SMJERNICE ZA USPOSTAVLJANJE BEZBJEDNOSNIH ZONA

PREPORUKE ODJELJENJA ZA INFORMACIONU BEZBJEDNOST (OIB-CERTRS)

AGENCIJA ZA INFORMACIONO DRUŠTVO REPUBLIKE SRPSKE

ODJELJENJE ZA INFORMACIONU BEZBJEDNOST

Autor: Ognjen Katić

Agencija za informaciono društvo Republike Srpske

Odjeljenje za informacionu bezbjednost

Publikacija **OIBRS-PUB-M1**

Serijal publikacija o bezbjednosti računarskih mreža

Autor: Ognjen Katić, ognjen.katic@aidrs.org

Urednik izdanja: mr Srđan Rajčević, srdjan.rajcevic@aidrs.org

http://oib.aidrs.org | http://www.aidrs.org

SADRŽAJ

LISTA DODATAKA

1. UVOD

Sa porastom stepena uvezanosti između informacionih sistema raste i njihova međusobna zavisnost te se greške i slabosti jednog sistema mogu propagirati u teritoriju drugog. Ovu činjenicu sve više koriste tvorci malicioznog softvera i eksploatišu slabosti mreža bez internih mjera bezbjednosti kako bi brzo širili svoj malver unutar mreže. Ovaj dokument pruža pregled osnovnih elemenata računarskih mreža, slabosti nemarno dizajniranih mreža i neke metode dizajna bezbjednih mreža.

Zaštita u slojevima predstavlja jaku odbranu od velikog broja napada jer omogućava granularizaciju metoda odbrane i uspostavljanje preciznijih odbrambenih mehanizama. Pored pojačanja odbrane ovakve metode olakšavaju održavanje i izmjene u odbrambenom sistemu.

1.1 AUTORITET

Odjeljenje za Informacionu bezbjednost je organizaciona jedinica u sastavu Agencije za informaciono društvo. Zadatak odjeljenja je koordinacija prevencije i zaštite od računarskih bezbjednosnih incidenta kao i zaštita kibernetičke infrastructure javnih organa, privatnih i fizičkih lica. Odjeljenje za informacionu bezbjednost vrši ulogu nacionalnog CERT-a.

Ovlaštenjima Odjeljenja za informacionu bezbjednost u daljem tekstu ćemo smatrati ona koja su mu data Uredbom o mjerama informacione bezbjednosti, član 36 i 37, kao i ovlašćenja koja su data CERT-u zakonom o informacionoj bezbjednosti, članovi 10, 11, 12, pošto Odjeljenje vrši ulogu nacionalnog CERT-a.

Zakon o informacionoj bezbjednosti predviđa da Odjeljenje za informacionu bezbjednost može da propisuje mjere i standarde za:

- Republičke organe,
- Organe jedinica lokalne samouprave,
- Pravna lica koja vrše javna ovlašćenja,
- Druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima u elektronskom obliku, republičkih organa, organa jedinica lokalne samouprave i pravnih lica koja vrše javna ovlašćenja,

1.2 NAMJENA I OBIM

Namjena ovog dokumenta je da upozna čitaoca sa tehnologijama i metodima dizajna bezbjednih računarskih mreža, te da pomogne arhitektama mreža i stručnjacima iz polja računarske bezbjednosti da korektno postave infrastrukturne servise u bezbjedne zone.

Metode navedene u ovom dokumentu su često zanemarene jer zahtjevaju dodatno planiranje u procesu postavljanja računarskih mreža, što je samo po sebi mukotrpan i dug proces. Velika porcija sadržaja je posvećena razmatranju metoda kako bi se bolje bolje shvatila njihova vrijednost.

Dokument pokriva i diskusije o uobičajnim prijetnjama računarskim mrežama koje potiču kako iz javnih mreža van posmatranog sistema tako i unutar samog sistema. Kako su računarske mreže u ovom dokumentu posmatrane na višem nivou apstrakcije, detalji zaštite individualnih računara, njihovih softverskih komponenti i mrežne opreme poput rutera, svičeva itd. je van njegovog domena i biće posmatrani u zasebnoj publikaciji OIB-a.

Smjernice pružene u ovom dokumentu nisu obavezujuće i predstavljaju samo savjete i dobre prakse.

1.3 PUBLIKA

Kako se dokument bavi specifičnostima dizajna računarskih mreža, on je primarno namjenjen stručnim licima u čije obaveze spadaju dizajn, obezbjeđivanje i održavanje računarskih mreža. U ova lica spadaju sistemski administratori, inženjeri i druga lica koja se bave projektovanjem i održavanjem računarskih mreža

Sekundarno, dokument je namjenjen licima koja su zainteresovana za sticanje dodatnog znanja iz oblasti zaštite računarskih mreža i kao takva sadrži neke teoretske osnovne neophodne za razumjevanje pomenutog sadržaja.

1.4 STRUKTURA DOKUMENTA

Ovaj dokument je podjeljen u nekoliko poglavlja. Prvo poglavlje pokriva informacije o samom dokumentu i instituciji koja ga je izdala. Analiza i prijedlozi za rješavanje problema izloženi su od drugo poglavlja pa nadalje.

Poglavlje broj dva bavi se upoznavanjem sa osnovnim pojmovima bezbjednosti računarskih mreža, dok se poglavlja nakon toga bave razmatranjem metoda segmentacije mreža.

Poglavlje broj tri sadrži konkretne smjernice i dobre prakse za dizajn bezbjedne računarske mreže. Smjernicu su sumirane u dodatnim poglavljima dokumenta, i uz njih su navedene skraćenice i pojmovi korišteni u njemu.

2. PREGLED

Ovo poglavlje sadrži informacije o osnovnim pojmovima i klasifikacijama mrežne bezbjednosti. Kako bi se dizajnirala otporna mreža potrebno je poznavati sastav sistema koji se pokušava obezbjediti. Poznavanje strukture i resursa koji se nalaze u sistemu omogućava korektnu klasifikaciju, a to je neophodno za uspostavljanje granularne zaštite.

2.1 UVOD U MREŽNU BEZBJEDNOSTI

Današnja sveopšta povezanost između mreža, naročito sa internetom, izlaže privatne mreže neprijateljskom okruženju sa prijetnjama koje se brzo razvijaju i šire. Povezivanje sa drugim mrežama obezbjeđuje zgodne kanale kroz koje spoljašnji entiteti mogu da ugroze računarske sisteme. Pored svega ovoga i korisnici internih mreža mogu da slučajno ili namjerno ugroze mreže i računarske sisteme svojim akcijama. Ukoliko neki uređaj sa interne mreže postane kompromitovan bezbjednost čitave mreže postaje ugrožena.

Mrežnu bezbjednost predstavljaju mjere koje su potrebne da se redukuje osjetljivost mreže na ove vrste prijetnji i ima tri osnovne direktive:

- Da zaštiti mrežne servise.
- Da smanji podložnost uređaja na mreži i računarskih aplikacija na prijetnje koje potiču sa mreže.
- Da zaštiti podatke prilikom prenosa preko mreže.

Mrežna zaštita obezbjeđuje sisteme od spoljašnjih i unutrašnjih prijetnji skupom mjera zaštite. Ove mjere uključuju:

- Fizička zaštita mrežnih komponenti i opreme
- Tehničke kontrole unutar mrežne infrastrukture koje redukuju osjetljivost na bezbjednosne prijetnje

- Kontrole koje se primjenjuju prilikom životnog ciklusa kako bi se ograničila ranjivost mrežne arhitekture na prijetnje
- Mjere informacione bezbjednosti za detekciju, zaustavljanje, odgovor na i oporavak od bezbjednosnih incidenata

Osnovni pojmovi bezbjednosne arhitekture mreža su:

- Bezbjednosni napad – svaka aktivnost koja ugrožava bezbjednost informacija u vlasništvu organizacije.
- Bezbjednosni mehanizam – proces projektovan za otkrivanje, sprječavanje ili oporavak od bezbjednosnog napada.
- Bezbjednosni servis – servis za obradu ili komunikaciju koji unaprjeđuje bezbjednost sistema za obradu podataka i prenos informacija jedne organizacije. Servisi su namjenjeni za suprotstavljanje bezbjednosnim napadima, a za pružanje te usluge koriste jedan ili više bezbjednosnih mehanizama.

2.2 KLASIFIKACIJE PODATAKA I ZONA U MREŽNOJ BEZBJEDNOSTI

Organizacije bi kao prvi korak u dizajnu arhitekture mreže i bezbjednosnih politika trebale da izvrše klasifikaciju svojih resursa kako bi ih grupisali na korektan način. Klasifikacije podataka i drugih informacionih resursa omogućavaju granularno djelovanje i projektovanje čime se olakšava obezbjeđivanje različitih resursa i eliminiše pretjerana ili nedovoljna zaštita.

Tri osnovna koncepta bezbjednosti podataka su:

- Povjerljivost podataka – podatak je dostupan samo licima koja su ovlašćena da ostvare pristup i dalje postupaju sa tim podatkom.
- Cjelovitost podataka – podrazumjeva očuvanje postojanja, tačnosti i kompletnosti podataka, kao i zaštitu procesa ili programa koji sprječavaju neovlašćeno mijenjanje podataka.
- Dostupnost podataka – podrazumjeva mogućnost da ovlašćeni korisnici mogu pristupiti podatku uvijek kada za tim imaju potrebu.

Mjere zaštite podataka i napor uložen pri obezbjeđivanju sistema koji sadrže te podatke biraju se prema klasifikaciji podataka na osnovu zahtjeva za njihovom povjerljivosti, cjelovitosti i dostupnosti.

Prema pravilniku o standardima informacione bezbjednosti ("Službeni glasnik Republike Srpske", broj 91/12) podaci se klasifikuju prema sledećim stepenima bezbjednosti:

- Prvi stepen bezbjednosti – Određuje se radi sprječavanja nastanka nepopravljive štete po interese subjekta.
- Drugi stepen bezbjednosti – Određuje se radi sprječavanja nastanka izuzetno štetne posljedice po interese subjekta.
- Treći stepen bezbjednosti – Određuje se radi sprječavanja nastanka štete po interese subjekta.
- Četvrti stepen bezbjednosti – Određuje se radi sprječavanja nastanka štete za rad, odnosno obavljanje zadataka I poslova subjekta koji ih je odredio.
- Peti stepen bezbjednosti (javni podaci) – Podaci za koje se smatra da ne mogu uzrokovai nastanak bilo kakve štete za subjekat koji ih je odredio.

Shodno resursima koji se u njima nalaze organizacije bi trebale da definišu kao sigurne administrativne zone prostore ili prostorije u kojima se čuvaju podaci i uređaji koji zahtjevaju odgovarajuću fizičku zaštitu. Ove zone klasifikovane su takođe na pet stepeni i shodno klasifikaciji resursa koje sadrže.

Koncept fizičkih zona bio je inspiracija i početna tačka za razvoj modela mrežnih bezbjednosnih zona. Pri fizičkom obezbjeđivanju identifikuju se resursi koji imaju iste bezbjednosne zahtjeve i postavljaju u zone se istim mjerama zaštite. Slično tome i zone mrežne bezbjednosti osmišlljene kao grupe u mrežnoj komunikaciji koje se obezbjeđuju istim mjerama mrežne zaštite. Zone su kreirane tako da se minimizuje kompleksnost mreže i osigura efektivan i efikasan način dostave mrežnih servisa.

Formiranje grupa uređaja na računarskoj mreži olakšava proces zaštite ovih uređaja. Proces odvajanja LAN grupa uređaja naziva se segmentacija i predstavlja jednu od osnovnih mjera zaštite računarskih mreža.

Prilikom segmentacije mreža organizacije bi trebale da izvrše klasifikaciju i organizaciju IP opsega kako bi se dodatno olakšalo kreiranje bezbjednosnih politika. Ova klasifikacija rezultuje IP shemom mrežnog prostora i vrši se prema funkcionalnim, bezbjednosnim ili nekim drugim klasifikacijama.

Primjenom segmentacije mreža, definisanjem IP shema, bezbjednih zona i adekvatnih kontrola zaštite uspostavlja se otporna i modularna mrežna arhitektura.

2.3 PRIJETNJE MREŽNOJ BEZBJEDNOSTI

Alati za izvođenje napada na računarske mreže postaju sve kompleksniji ali i pristupačniji. Maliciozni faktori, ali i istraživači doprinose užurbanom razvoju ovih alata. Iako su im konačni ciljevi različiti, i jedni i drugi nastoje razviti jednostavne i efektivne alate za otkrivanje ranjivosti i izvođenje napada. Istraživači ovo čine kako bi otklonili pronađene ranjivosti, a napadači kako bi ih eksploatisali. Bilo kako bilo alati za

sprovođenje napada su postali dovoljno jednostavni za koristiti i laki za pronaći, da i korisnici bez velikog stručnog znanja mogu predstavljati prijetnju bezbjednosti.

Napadi na mrežnu bezbjednost se mogu klasifikovati na nekoliko načina. Jedna od klasifikacija koja se koristi u RFC 4949 je na pasivne i aktivne napade. Pasivan napad pokušava da sazna ili iskoristi informaciju iz sistema, a da ne utiče na sistemske resurse. Aktivni napad pokušava da izmjeni sistemske resurse ili utiče na njihov rad.

2.3.1 PASIVNI NAPADI

Cilj protivnika koji izvodi pasivne napade je da nabavi informaciju koja se prenosi u nekoj komunikaciji. Dve vrste pasivnih napada su otkrivanje sadržaja poruke i analiza saobraćaja.

Otkrivanje sadržaja poruke ima za cilj da prilikom telefonskog razgovora, razmjene elektronske pošte ili datoteke koja se prenosi sazna informacije koje se prenose i koje sadrže povjerljive informacije. U svrhu zaštite od ovih napada sprovode se mjere mrežne bezbjednosti. Napadač će prilikom izvođenja ovog napada pokušati da dobije pristup komunikacionom mediju koji se koristi za prenos povjerljivih informacija. Pristup je moguće ostvariti na nekoliko načina i podrazumjevaju fizički pristup mrežnim uređajima ili vodovima. Nakon što dobije pristup napadač će prisluškivati komunikacione tokove i filtrirati ih kako bi izdvojio informacije koje su njemu od interesa, poput kredencijala za pristup nekom sistemu. U svrhu odbrane od ovakvih napada organizacije bi trebale da dobro osiguraju svoju komunikacionu opremu i vodove i ograniče pristup na samo autorizovana lica.

Analiza saobraćaja je suptilniji napad. Pretpostavimo da imamo način da maskiramo sadržaj poruka ili drugog toka informacija tako da protivnici, sve i da uhvate poruku, ne mogu da izvuku informaciju iz nje. Uobičajna tehnika za maskiranje podataka je šifrovanje. Ako smo uspostavili zaštitu šifrovanjem, protivnik ipak može da uoči šablon tih poruka. Protivnik bi mogao da odredi lokaciju i identitet računara u komunikaciji i mogao bi da uoči učestalost i dužinu razmjenjenih poruka. Te informacije bi mogle da mu budu korisne za određivanje prirode komunikacije koja se odvija. Kao i kod prošlog napada, preduslov za izvođenje ovog napada je mogućnost prisluškivanja komunikacionog medija. Nakon ostvarivanja pristupa napadač će nastojati da prikupi što veću količinu informacija kako bi mogao vršiti neka statistička ispitivanja. Dobra zaštita od ovakvog napada je dopunjavanje saobraćaja tako da ne postoje razlike u učestalosti ili dužini poruka koje se razmjenjuju. Iako ovaj metod prouzrokuje nepotrebna opterećenja na mreži, isplati se za slučajeve kada se radi sa osjetljivim podacima.

Pasivni napadi se veoma teško otkrivaju zato što ne dolazi ni do kakve izmjene podataka. Obično se saobraćaj poruka šalje na naizgled normalan način, pa ni

pošiljalac ni primalac nisu svjesni da je još neko pročitao poruku ili uočio šablon komunikacije. Međutim, izvodljivo je da se spriječi uspjeh takvih napada, obično pomoću šifrovanja.

2.3.2 AKTIVNI NAPADI

Aktivni napadi uključuju neku izmjenu toka podataka ili stvaranje lažnog toka i mogu da se podjele na četri kategorije – maskiranje, ponavljanje, izmjenu poruka i uskraćivanje usluga.

Maskiranje se dešava kada se jedan entitet pretvara da je neki drugi entitet. Napad maskiranjem obično uključuje i jedan od ostalih oblika aktivnog napada. Na primjer, moguće je uhvatiti sekvencu autentifikacije i ponoviti je nakon izvršenja važeće autentifikacije, pa ovlašćeni entitet sa manje privilegija može da pribavi dodatne privilegije tako što se predstavlja da je entitet sa većim privilegijama. Jedna vrsta ovog napada podrazumjeva lažno predstavljanje napadača kao neke usluge od povjerenja. Nakon uspostavljanja veze sa korisnikom napadač će pokušati da od njih izmami osjetljive informacije putem socijalnog inženjeringa, obično uz tvrdnju da je to u njihovom interesu.

Ponavljanje uključuje pasivno hvatanje jedinice podataka i njeno naknadno ponavljanje kako bi se postigao neovlašten efekat.

Izmjena poruka jednostavno znači da se promjeni neki dio legitimne poruke ili da se poruke odlože ili im se izmjeni redosljed kako bi se proizveo neovlašten efekat.

Uskraćivanje usluga se vrši u svrhu spječavanja ili kočenja normalnog korištenja komunikacionih sredstava ili njihovo upravljanje. Ovaj napad može da ima konkretan cilj. Na primjer jedan entitet može da obustavi sve poruke usmjerene na određeno odredište. Drugi oblik uskraćivanja usluge je poremećaj čitave mreže – bilo da se mreža onemogući ili da se preoptereti tako da se degradiraju performanse. Ovakva vrsta napada se obično izvodi slanjem ogromne količine saobraćaja korištenjem botnet-a. Zaštita od ove vrste napada je jako teška jer svako ograničenje koje se postavlja kako bi se sprječio ima uticaj i na dostupnost usluga legitimnim korisnicima.

Aktivni napadi imaju karakteristike suprotne pasivnim napadima. Dok se pasivni napadi teško otkrivaju, postoje mjere koje sprječavaju njihov uspjeh. Na drugoj strani, aktivne napade je teško potpuno spriječiti zbog velike raznovrsnosti potencijalnih fizičkih, softverskih i mrežnih ranjivosti. Umjesto toga, cilj je da se aktivni napadi otkriju i da se izvrši oporavak od štete izazvane promjenjenim ili odloženim podacima.

2.4 BEZBJEDNOSNI SERVISI

Bezbjednosni servis je u X.800 definisan kao servis koji pruža jedan sloj protokola komunikacionog sistema i koji obezbjeđuje adekvatnu bezbjednost sistema ili transfera podataka. Možda je jasnije definisan u dokumentu RFC 4949 u kojem se nalazi sledeća definicija: servis obrade ili komunikacije koji pruža sistem da bi sistemskim resursima proužio konkretnu vrstu zaštite. Bezbjednosni servisi imaju bezbjednosne politike i primjenjuju se pomoću bezbjednosnih mehanizama. Prema X.800 ovi servisi su podjeljeni u pet kategorija:

- Autentifikacija – servis autentifikacije se bavi obezbjeđivanjem da veza bude autentična. U slučaju pojedinačne poruke, funkcija servisa autentifikacije je da uvjeri primaoca da poruka potiče od izvora kako tvrdi da jeste. U slučaju interakcije u toku, kao što je veza terminala sa računarom, postoje dva aspekta. Najprije prilikom uspostavljanja veze, ovaj servis potvrđuje da su oba entiteta autentična. Drugo servis mora da obezbjedi da se veza ne ometa tako da se neko treći maskira u jednu od dve legitimne strane kako bi neovlašteno prenosio ili preuzimao poruke.
- Kontrola pristupa – u kontekstu mrežne bezbjednosti kontrola pristupa je mogućnost da se pristupanje računarskim sistemima i aplikacijama putem komunikacionih linkova ograniči i kontroliše. Da bi se to postiglo svaki entitet koji pokuša da dobije pristup mora najprije da se identifikuje ili autentifikuje da bi se prava pristupanja prilagodila pojedincu.
- Povjerljivost podataka – servisi čija je funkcija da zaštite podatke koji se prenose od pasivnih napada. Sa obzirom na sadržaj prenosa podataka, može se prepoznati nekoliko nivoa zaštite. Najširi servis štiti sve korisničke podatke koji se prenose između dva korisnika tokom jednog vremenskog perioda. Na primjer kada se između dva računara uspostavi SSL veza, ova široka zaštita sprječava otkrivanje bilo kojeg korisničkog podatka koji se prenosi preko SSL veze. Moguće je definisati uže oblike ovog servisa uključujući zaštitu jedne same poruke ili čak konkretnih polja unutar poruke. Drugi aspekt povjerljivosti je zaštita toka saobraćaja od analize. To zahtjeva da napadač ne bude u stanju da na sredstvu za komunikaciju opazi izvor ili odredište, frekvenciju, dužinu i druge karakteristike saobraćaja.
- Integritet podataka – kao povjerljivost, integritet podataka može da se primjeni i na tok poruka, na pojedinačnu poruku ili na odabrana polja unutar poruke. I ovdje najkorisniji i najjednostavniji pristup je potpuna zaštita toka. Servis integriteta orjentisan na vezu postupa sa tokom poruka i osigurava da se poruke šalju i primaju bez dupliciranja, dodavanja, mjenjanja, promjene redosljeda ili ponavljanja. Ovaj servis obuhvata i uništavanje podataka. Prema tome, servis integriteta orjentisan na vezu odnosi se kako na mjenjanja toka poruka, tako i na onemogućavanje usluga. Na drugoj strani, servis integriteta

bez direktnog uspostavljanja veze odnosi se na pojedinačne poruke bez obzira na širi kontekst i uglavnom obezbjeđuje samo zaštitu od mjenjanja poruke.

- Neporecivost – sprječava i pošiljaoca i primaoca da poreknu prenijetu poruku. Tako kada se poruka pošalje, primalac može da dokaže da je navodni pošiljalac poslao poruku. Slično tome, kada se poruka primi pošiljalac može da dokaže da je navodni primalac zaista primio poruku.

3. SMJERNICE

Ovo poglavlje se bavi razmatranjem konkretnih metoda zaštite mreža od unutrašnjih i spoljašnjih prijetnji, a koje se odnose na arhitekturu mreža. Metode koje se navode imaju za cilj uspostavljanje mreže u kojoj se komunikacija odvija na predvidljiv i kontrolisan način. Ovakva mreža omogućava definisanje preciznih politika i zaštitu od raznovrsnih prijetnji bez uvođenja pretjerane kompleksnosti koja redukuje upotrebljivost sistema.

3.1 NAMETANJE KONTROLE PRISTUPA

Organizacije bi trebale da uvedu mehanizme kontrole pristupa mreži u zonama sa visokim zahtjevima za povjerljivost. Kontrola pristupa se uvodi radi autentifikacije korisnika koji se prijavljuju na mrežu i utvrđivanja kojim podacima smeju da pristupaju i koje radnje smeju da obavljaju. Mehanizmi kontrole pristupa takođe ispituju zdravstvenu ispravnost korisnikovog računara ili mobilnog uređaja radi separacije uređaja koji bi mogle biti prijetnje sistemu.

Sistem za kontrolu pristupa ima tri kategorije komponenti :

- Tražilac pristupa – je uređaj koji pokušava da pristupi mreži, to može da bude radna stanica, server, štampač, kamera i drugi uređaji sposobni za IP komunikaciju. Entiteti ove kategorije se jos nazivaju i suplikanti.
- Server polise – na osnovu pozicije tražioca pristupa definisane u preduzeću, server polise utvrđuje kakav pristup treba odobriti. Server polise često se za pomoć u ocjenjivanju stanja računara oslanja na pozadinske sisteme, uključujući antiviruse ili direktorijume korisnika.
- Server za pristup mreži – funkcioniše kao tačka kontrole pristupa za korisnike na udaljenim lokacijama koji se povezuju sa unutrašnjom mrežom preduzeća. Zove se još mrežni prolaz za medij ili server za daljinski pristup. Ovaj server može da sadrži vlastite servise autentifikacije ili da se oslanja na servis autentifikacije servera polise.

Proces funkcioniše na način da raznovrsni suplikanti traže pristup mreži preduzeća tako što se prijavljuju nekoj vrsti sistema za pristup mreži. Prvi korak je obično autentifikacija molioca. Autentifikacija obično obuhvata neku vrstu bezbjednog protokola i korištenje kriptografskih ključeva. Autentifikaciju može da obavi sam sistem, a može i da posreduje procesu autentifikacije.

Pri procesu autentifikacije provjerava se navodni identitet molioca, čime se serveru polise omogućava da odredi koje privilegije pristupa može da ima, ukoliko ih uopšte ima. Razmjena autentifikacije može da završi uspostavljanjem ključeva sesije kako bi se omogućila bezbjedna komunikacija.

Obično server polise ili server za podršku provjerava molioca da se utvrdi da li mu treba dozvoliti interaktivno vezivanje daljinskim pristupom. Te provjere se ponekad zovu provjere zdravstvene ispravnosti, podobnosti, skrining, odnosno procjene i zahtjevaju da softver na korisnikovom sistemu dokaže usklađenost sa određenim osnovnim zahtjevima za bezbjednost u organizaciji.

Korištenje autentifikacije prilikom spajanja na mrežu predstavlja značajno povećanje bezbjednosti mreže. Bez ovih metoda zaštite u većini kompanija klijent koji se poveže na mrežu fizički dobija od DHCP servera IP adresu i postaje ravnopravan član LAN-a.

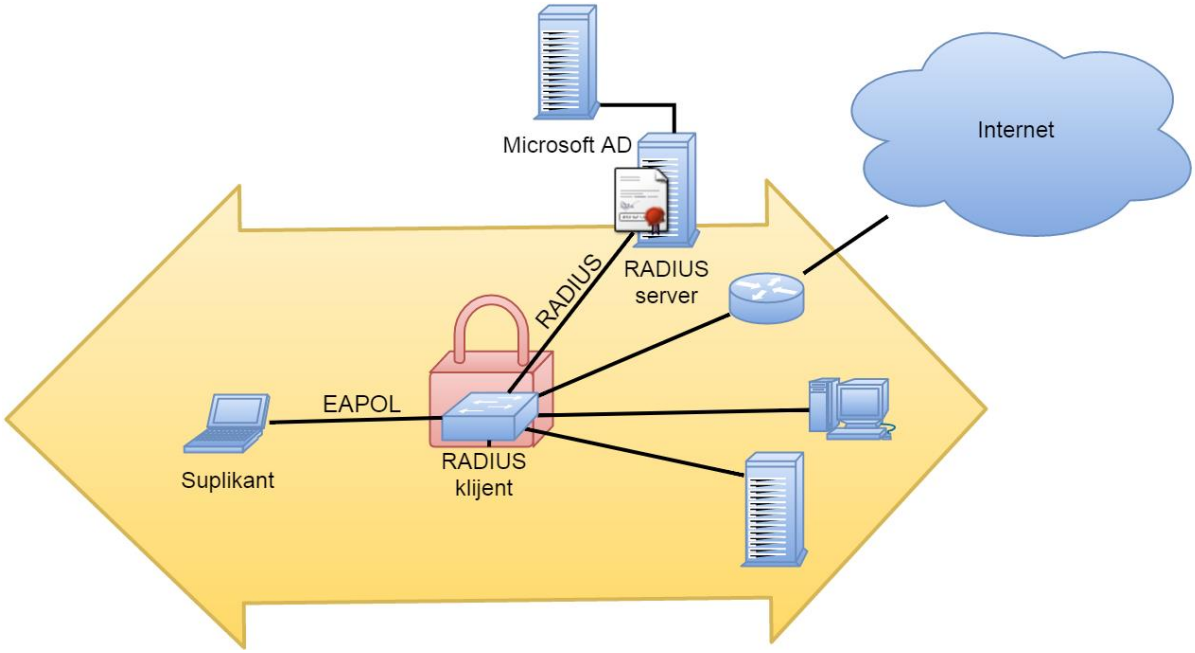
Standard IEEE 802.1X nameće autentifikaciju prije nego što se portu dodjeli IP adresa. Za proces komunikacije koristi proširivi EAP protokol. Ova kontrola pristupa spada u kategoriju port baziranih kontrola pristupa mreži. IEEE 802.1X projektovan je da bi se obezbjedile funkcije kontrole pristupa za LAN-ove. Dok servis za autentifikaciju ne autentifikuje molioca, on prosljeđuje samo kontrolne i autentifikacione poruke između molioca i servera za autentifikaciju. Pošto se molilac autentifikuje i pribave se ključevi, autentifikator može da prosljeđuje na mrežu podatke od molioca, podložne unapred definisanim ograničenjima pristupa molioca. Pod ovim uslovima, kanal podataka se deblokira.

Standard IEEE 802.1X koristi koncepte nekontrolisanih i kontrolisanih portova. Portovi su logički entiteti definisani unutar autentifikatora i odnose se na fizičke mrežne veze. Svaki logički port se preslikava u jednu od ove dve vrste fizičkih portova. Nekontrolisani port dozvoljava razmjenu jedinica podataka protokola između molioca i servera za autentifikaciju, bez obzira na stanje autentifikacije molioca. Kontrolisani port dozvoljava razmjenu PDU-ova između molioca i drugih sistema na mreži jedino ako trenutno stanje molioca dozvoljava takvu razmjenu. Bitan element definisan u IEEE 802.1X je protokol poznat kao EAPOL (EAP over LAN). Ovaj protokol funkcioniše u mrežnom sloju i koristi jedan LAN kao ethernet ili WiFi u sloju veze. Protokol EAPOL omogućava moliocu da komunicira sa autentifikatorom i podržava razmjenu EAP paketa za autentifikaciju.

Reprezentativan scenario predstavlja povezivanje klijentskog računara na switch koji će zatim putem RADIUS servera vršiti autentifikaciju klijenta. U ovom scenariju klijentski računar je suplikant, a switch ima ulogu posrednika između servera za

autentifikaciju i klijenta. Kako bi sve funkcionisalo korektno klijentski računar mora biti konfigurisan za IEEE 802.1X, switch mora biti konfigurisan kao RADIUS klijent, a radius mora imati pristup politikama za autentfikaciju klijenata.

U ovom scenariju postoji nekoliko ishoda, u zavisnosti od uspjeha autentifikacije klijenta. Moguće je definisati različite VLAN-ove kako bi se razdvojile grupe korisnika i obezbjedila fleksibilnost pri povezivanju različitih uređaja bez ugrožavanja bezbjednosti.



Slika 1.1 Primjer kontrole pristupa

3.2 IP SHEMA

Prilikom projektovanja računarskih mreža potrebno je rezervisati adresni prostor za postojeće i predviđene uređaje koji će učestvovati u mrežnoj komunikaciji. Dodjela adresa sama po sebi ne predstavlja mjeru zaštite ali olakšava sprovođenje konkretnih mjera. Prednosti korištenja dobre IP sheme se odražavaju u lakšoj implementaciji rutiranja i bezbjednosti.

Prednosti u rutiranju se odnose na optimizacije u vidu redukcije velikih tabela rutiranja i smanjenja ljudskih grešaka jer je moguće grupisati IP adrese uređaja srodnih funkcionalnosti u jedanu logičku mrežu.

Prednost u vidu bezbjednosti je takođe posljedica grupisanja uređaja u jednu grupu adresa čime se smanjuje set pravila za uređaje kontrole i omogućava se lakša primjena mehanizama za kontrolu pristupa.

Prilikom dizajna adresnog prostora potrebno je dobro razmisliti o potrebnom broju adresa uzimajući u obzir moguće ekspanzije kako bi se rezervisala prava količina adresa.

Particioniranje adresa moguće je vršiti na osnovu različitih kriterijuma. Neki česti kriterijumi za grupisanje adresa su: nivo zaštite, upotreba i lokacija. Nakon odabira kriterijuma za klasifikaciju resursa vrši se particioniranje adresnog prostora na način koji najbolje iskorištava adresni prostor. Particioniranje se može vršiti dodjeljivanjem brojne težine neke adrese resursu odgovarajuće težine (ovdje se pod težinom resursa misli na nivo bezbjednosti).

3.3 SEGMENTACIJA MREŽE

Mrežna infrastruktura napreduje i obezbjeđuje veće brzine kako bi zadovoljila potražnju, ali bezbjednosna infrastruktura ne uspjeva da pruži sigurne i kontrolisane servise. Timovi zaduženi za bezbjednost sistema ne posjeduju resurse za implementaciju svih neophodnih mjera, pa su prisiljeni da odaberu samo neke kada je u pitanju praćenje i kontrola novih mrežnih servisa.

Mrežna bezbjednost postaje nešto o čemu se misli nakon implementacije, a ne tokom, što dodatno otežava kokrektno funkcionisanje. Segmentacija mreže može da olakša pristup i osiguravanje infrastrukture i servisa mreža koje se često mjenjaju.

Segmentacija je proces grupisanja mrežnih resursa i aplikacija u odvojene sekcije IP opsega.

Prilikom segmentacije potrebno je izvršiti neka razmatranja:

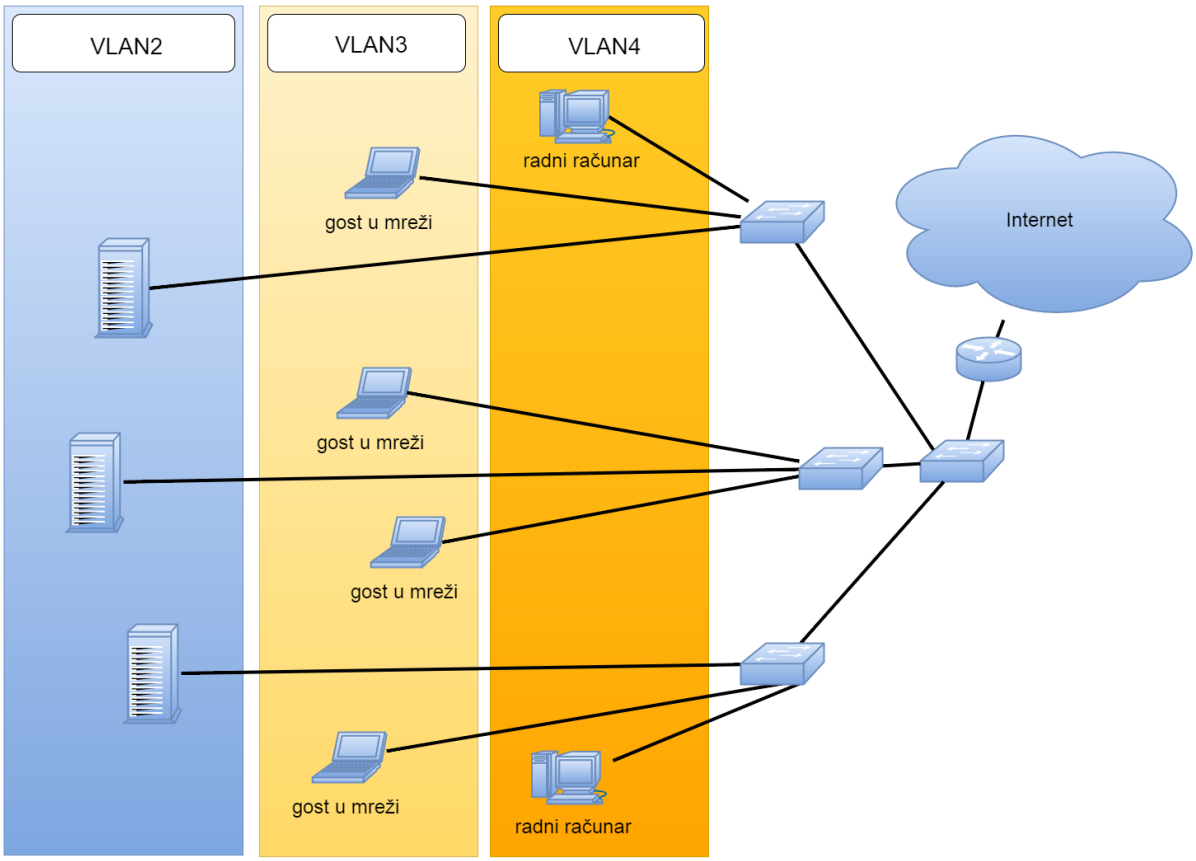
- Analizirati mrežni saobraćaj i uređaje na mreži
- Zaštititi komunikacije i resurse od dolaznog i odlaznog saobraćaja
- Implementirati granularne kontrole
- Postaviti podrazumjevano odbijanje (default deny) kao politiku za sve intersegmentne komunikacije

Prilikom implementacije mrežnog segmenta najbolje je početi sa jednostavnim segmentima i po potrebi proširivati logičku raspodjelu sa dodatnim kategorijama

Prilikom segmentacije treba se fokusirati na jedan po jedan segment i primjeniti naredne korake:

- Dobiti vidljivost – Ukoliko se ne poznaje profil saobraćaja za predloženi segment čitav proces nema smisla, te implementacija neće biti zadovoljavajuća. Mora se razumjeti kako se mreža koju segmentujemo koristi.
- Zaštititi komunikacije i resurse od dolaznih i odlaznih zahtjeva – Ukoliko nije moguće ostvariti zaštitu resursa unutar nekog segmenta sigurnost nije ostvariva. Jednostavna kontrola pristupa između segmenata nije dovoljna. Potrebna je sposobnost brže detekcije prijetnji i otklanjanja problema.
- Implementirati granularne kontrole – Svi podaci koji dolaze ili odlaze sa segmenta moraju biti kontrolisani. Kako je u prošlom koraku već uspostavljana zaštita, znamo da je sve što ulazi ili izlazi iz mreže osigurano određenim nivoom zaštitnih mjera, te je sada moguće implementirati komunikacionu politiku sa granularnim kontrolama pristupa. Ove kontrole trebaju biti implementirane u dva koraka, kao kontrole za detekciju i kontrole za prevenciju. Uspostavljanjem politike podrazumjevanog prihvatanja može se uspostaviti profil, te identifikovati i istražiti neočekivani saobraćaj.
- Postaviti politiku podrazumjevanog odbijanja na svim intersegmentnim komunikacijama – Sada kada su uspostavljeni zahtjevi iz prva tri koraka vrijeme je za pomjeranje prema politici podrazumjevanog odbijanja za sav intersegmentni saobraćaj. Tek kada je ova politika uspostavljena segment je uspješno odvojen od mreže i može da funkcioniše kao sopstvena logička jedinica.

U nekim slučajevima segmentacija razdvajanjem broadcast domena ruterima i postavljanje komunikacionih vodova skladno podjeli segmenata mreže nije moguća, možda zbog cijene, a možda zbog nepraktičnosti izmjene postojeće arhitekture. U tim slučajevima moguće je segmentovati mrežu putem VLAN-ova. Unutar svičevane mreže VLAN obezbjeđuje segmentaciju i organizacionu fleksibilnost. Kako je VLAN baziran na logičkim vezama, on omogućava administratoru da segmentuje mrežu na osnovu faktora poput funkcije, timova i aplikacija bez obzira na fizičku lokaciju korisnika ili uređaja. Uređaji unutar VLAN-a ponašaju se kao u zasebnom domenu umjesto u zajedničkoj infrastrukturi sa ostalim VLAN-ovima. Svaki od njih posmatra se kao zasebna logička mreža, i paketi namjenjeni za uređaje koji ne pripadaju tom lanu moraju ići kroz uređaj koji podržava rutiranje. Kreiranje VLAN-a kreira se logički broadcast domen koji se može protezati kroz više fizičkih lan segmenata. Korištenjem VLAN tehnologije postižu se bolje performanse i veća sigurnost uz manju cjenu.



Slika 1.2 VLAN segmentacija

Postoji nekoliko načina da se izvrši VLAN dodjela:

- Dodjela na osnovu porta – je podrazumjevani metod specifikovan u 802.1Q. Problem sa ovim pristupom je relativno lako zaobilaženje zabrane komunikacije ukoliko napadač ima fizički pristup. Za eksploataciju ove slabosti potrebno je samo da se napadač poveže na odgovarajući port i dobiće pristup mreži.
- Dodjela na osnovi MAC adrese – moguće je napraviti tabelu koja mapira MAC adrese sa odgovarajućim VLAN-om. Kada paket stigne parsira se tabela kako bi se dobavio odgovarajući MAC i uređaj dodjelio odgovarajućem VLAN-u. Iako ovo traži više napora pri konfiguraciji, omogućava održavanje sigurnosti i članstva VLAN-u za uređaje koji se kreću. Slabost ovoga pristupa je MAC spoofing, kojim se napadač predstavlja kao autentifikovani uređaj i tako dobija pristup.
- Dodjela po IP segmentu --- kako su VLAN-ovi mrežni segmenti moguće im je dodjeliti IP opseg.
- Dinamička dodjela – naročito korisno za WLAN mreže i remote uređaje. Bazira se na autentifikaciji sa grupom putem nekog servisa. Obično se sastoji od RADIUS servera i korisničkog direktorija. Kada se korisnik autentifikuje, paketi od njegovog uređaja se dodjeljuju odgovarajućem VLAN-u na osnovu pravila koja su propisana. Ovo je korisno za djeljene portove jer omogućava različito ponašanje i laku konfiguraciju za sisteme bazirane na ulogama.

- Dodjela po uređaju – većina endpoint uređaja nisu svjesni VLAN-a i nisu sposobni da procesiraju VLAN tagovane pakete, međutim neki proizvođači pružaju ekstenzije za NIC drajvere kako bi obezbjedili ovu funkcionalnost.
- Dodjela po protokolu – moguće je definisati VLAN grupe za specifične protokole, ovo je korisno za organizacije koje koriste više mrežnih protokola.
- Dodjela po aplikaciji – obezbjeđuje neku vrstu raspoređivanja tereta za ukoliko postoje aplikacije koje čine veliku porciju mrežnog saobraćaja.

Konceptualno segmentacija putem VLAN-ova ne razlikuje se od klasičnih metoda segmentacije. Isto je u smislu da su cilj i pristup isti - nastoji se ograničiti saobraćaj pri međusobnoj komunikaciji različitih djelova mreže. Razlikuju se samo u sloju na kome se segmentacija odvija. Sada se umjesto odvajanja segmenata putem rutera segmenti odvajaju dodjelama različitim VLAN-ovima, što olakšava prelazak sa flat mrežne arhitekture.

Postavljanje VLAN-ova povlači sa sobom i neke probleme i izlaže mrežu određenim prijetnjama poput VLAN hopping-a koji napadači koriste da pristupaju uređajima koji nisu na istom VLAN-u.

Kako se često komunikacija odvija preko nepovjerljivih mreža javlja se opasnost od kompromitacije. Implementacijom VPN tehnologija moguće je spriječiti neautentifikovan pristup kritičnim uređajima i sprječiti presretanje povjerljivih podataka prema i od ovih uređaja. VPN kreira obezbjeđene komunikacione veze između geografski udaljenih lokacija sa svrhom obezbjeđivanja istog nivoa povjerenja kao i u potpuno povjerljivoj mreži.

Postoje dve vrste VPN-ova:

- Trusted VPN – obezbjeđuje računarima na različitim lokacijama da budu članovi istog LAN-a sa pristupom mrežnim resursima lociranim unutar njega. Ova varijanta VPN-a ne pruža privatnost.
- Secured VPN – koristi protokole za kriptografsko tunelovanje kako bi obezbjedio privatnost. Unutar secured VPN-a povjerljivost, autentifikacija pošiljaoca i integritet poruke uspostavljaju privatnost.

U svim VPN-ovima moraju biti dve tačke na kojima se uklanja dodatna sigurnost VPN-a. Najvjerovatnije dve tačke terminacije su sami uređaji ili IPsec gateway-i locirani unutar fizičkog bezbjednosnog prostora uređaja. IPsec je najviše podržana varijanta VPN infrastrukture.

Individualno VLAN može pomoći segmentaciji saobraćaja a VPN zaštiti privatnosti saobraćaja. Međutim kada se koriste u kombinaciji ove tehnologije stvaraju višeslojni sistem bezbjednosti.

Kako flat mreže implementiraju model tvrđave sa jakom jednoslojnom odbranom, VLAN i VPN tehnologije omogućavaju prelaz na dubinsku odbranu i model u kome je potrebno probiti nekoliko slojeva za izvođenje uspješnog napada.

3.4 BEZBJEDNOSNE ZONE

Bezbjednosna zona je mrežni segment sa dobro definisanim tokom komunikacija sa drugim zonama i na kom se nalaze sistemi i komponente sa srodnim zahtjevima za zaštitu informacija i klasifikacijama dozvola pristupa. Kontrola toka informacija između zona vrši se interfejsnim tačkama koje se nalaze između zona i obično se implementiraju kombinacijom firewall-a, IDS i IPS uređaja i rutera. Sve interfejsne tačke moraju da zadovolje sledeće uslove:

- Svaka interfejsna tačka kontroliše dolazne informacije
- Interfejsne tačke implementiraju bezbjednosnu politiku zone na čijem se ulazu nalaze
- Sva komunikacija sa zonom se obavlja preko interfejsne tačke

Organizacije bi trebale da definišu bezbjednosne zone kako bi smanjili rizik otvorene mreže formiranjem logičkih grupa koje imaju iste bezbjednosne politike i zahtjeve. Iako je ovaj koncept sličan segmentaciji mreže, postoji potreba za separacijom ovih pojmova. Kreiranje zona je pristup logičkog dizajna za kontrolisanje i ograničenje pristupa i komunikacije podataka na samo one protoke i korisnike koji se slažu sa bezbjednosnom politikom. Velike mreže raspoređene preko udaljenih lokacija zahtjevaju pristup mrežnoj bezbjednosti koji je dosljedan. Nekada su unutrašnje mreže bile organizovane kao flat, odvojene od interneta samo jednim firewallom dok se unutar njih komunikacija odvijala ravnopravno između svih uređaja. Kako je situacija napredovala došlo je do porasta svjesti o važnosti informacione bezbjednosti i povjerljivosti podataka i o zavisnosti od elektronskih infrastruktura, što je rezultovalo nastankom novih bezbjednosnih metoda poput kontrole pristupa i mehanizama za autentifikaciju.

Flat ili ravne infrastrukture u današnje vrijeme predstavljaju jako ranjive sisteme, jer su osjetljivi na malver sa mogućnošću širenja putem korisničkih interakcija i replikacijom unutar sistema na mreži.

Sličnu prijetnju predstavljaju i ljudi, bilo kao zlonamjerni napadači sa vana ili iz unutrašnjosti mreže kao nezadovoljni zaposlenici. Sve ovo dovelo je do potrebe za zaštitom mreža i jednih od drugih. Dodatni faktor predstavljaju zastarjele aplikacije i sistemi čiji bezbjednosni problemi ne mogu biti zakrpljeni bilo to zbog prestanka podrške od strane prodavca ili jednostavno velike količine zaostatka u ažuriranju te predstavljaju slabu tačku u sistemu i prijetnju za čitavu mrežu.

Odvajanjem ovakvih aplikacija u zasebne mreže povećava se bezbjednost sistema. Bezbjednosna zona je mrežni segment sa dobro definisanim tokom komunikacija prema drugim zonama i na kom se nalaze sistemi i komponente sa srodnim zahtjevima za zaštitu informacija i klasifikacijama dozvola pristupa.

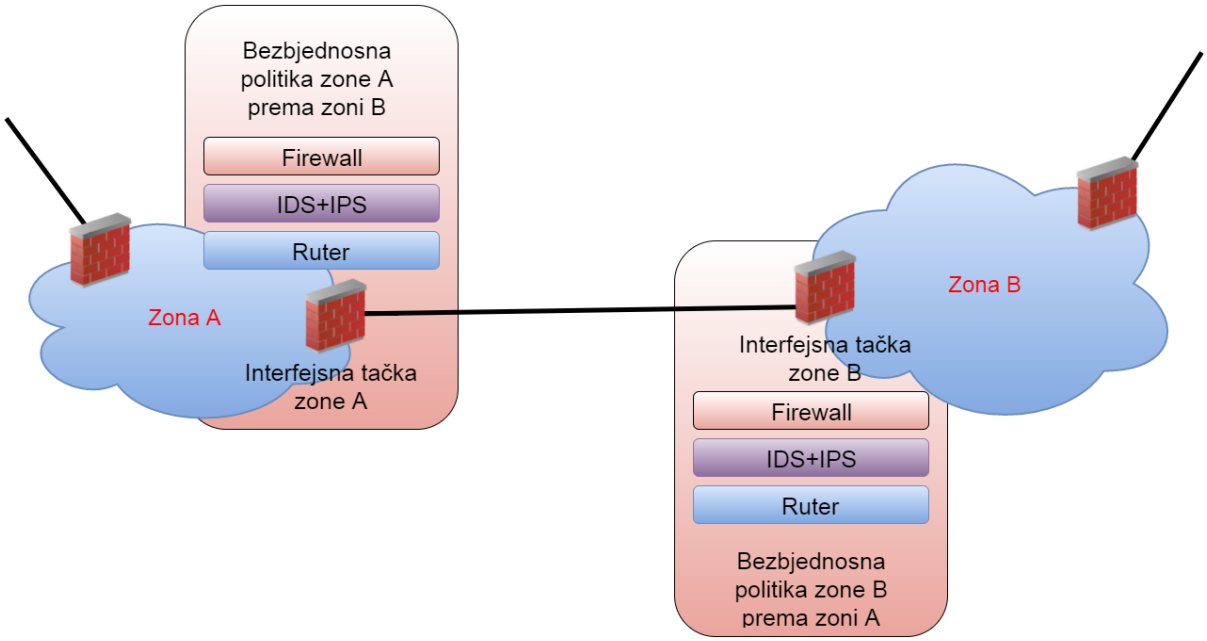
Ovi zahtjevi za elemente mrežnih bezbjednosnih zona su:

- Povjerljivost i integritet
- Kontrole pristupa
- Logovanje i monitoring

Ovakvi zahtjevi dovode do podjele ne samo između bezbjednosnih zona već i unutar njih dovode do slojevitih struktura. Ciljevi uspostavljanja bezbjednosnih zona su:

- Kontrola saobraćaja između zona
- Praćenje komunikacija između zona putem sistema za detekciju ili prevenciju napada
- Korelacija događaja putem SIEM-a
- Sprječavanje curenja informacija između zona
- Kontrola administratorskog pristupa
- Sprovođenje pravila za povjerljivost, cjelovitost i dostupnost podataka

Model bezbjednosnih zona obezbjeđuje sofisticiran i granularan pristup zaštiti sredstava i fokusira se na informacije kao najvrjedniji resurs. Naredna sekcija dokumenta bavi se opisom jedne moguće podjele na zone.



Slika 1.3 Interfejsne tačke između zona

3.4.1 SPOLJAŠNJA ZONA

Ova zona predstavlja komunikacione kanale koji nisu pod kontrolom projektanta. Ova zona obično predstavlja internet i iako nije moguće propisati pravila koja će se koristiti unutar nje, potrebno je njeno definisanje zbog cjelovitosti modela bezbjednosti. Kako se radi o saobraćaju koji nije pod kontrolom preduzeća za koje se projektuju bezbjednosne zone, potrebno je posmatrati sav saobraćaj koji dolazi sa ove mreže kao potencijalne prijetnje.

3.4.2 ZONA JAVNOG PRISTUPA

Ova zona sadrži uređaje i servise koji su namjenjeni da ih spoljašnji korisnici direktno koriste. Takođe se koristi kao međusloj za zaštitu interne mreže od prijetnji sa vana. Ova zona se pozorno prati i kontroliše, jer štiti interne uređaje i aplikacije od neprijateljskog okruženja spoljašnje zone. Takođe služi kao zavjesa koja krije interne resurse od javne zone i ograničava njihovu izloženost. Interfejsi za sve eksterne servise su implementirani kroz ovu zonu. Servisi koje ova zona može da pruža su proxy serveri za email i drugih gateway-a za poruke, remote access, extranet access itd. Osjetljive informacije ne trebaju biti skladištene u ovoj zoni. One mogu prolaziti ili biti prikupljane u njoj ali trebaju biti skladištene u baze podataka u operativnim ili zabranjenim zonama. Zona javnog pristupa pored filtriranja dolaznog saobraća filtrira i odlazni jer saobraćaj spoljašnje zone po definiciji nije pod kontrolom organizacije.

U komunikaciji sa spoljašnjom zonom bi trebalo da važi sledeća politika:

- Sav dolazni saobraćaj terminira se u proxy servisima unutar zone javnog pristupa nakon filtriranja od strane interfejsne tačke – U uslovima kada ovo nije moguće potrebno je razmotriti bezbjednosne prijetnje i osmisliti alternativno rješenje.
- Sav dolazni i odlazni saobraćaj sa spoljašnjom zonom treba biti ograničen na osnovu blacklist-a. Blacklist sadrži listu mrežnih adresa spoljašnje zone koje se pridružene prošlim malicioznim aktivnostima.
- Sav odlazni saobraćaj treba biti filtriran tako da samo adrese iz definisanog internog opsega mogu da komuniciraju sa spoljašnjom zonom.

Prilikom komunikacije sa operativnom i zonom sa ograničenim pristupom treba da važi sledeća politika:

- Sav saobraćaj između zone javnog pristupa i navedene dvije zone mora bit whitelist-ovan.
- Desktopi moraju koristiti proxy servise za pristup spoljašnjoj mreži.

Prilikom pristupa sa ostalim zonama saobraćaj mora biti whitelist-ovan.

3.4.3 OPERATIVNA ZONA

Ovo je standardna zona za svakodnevne operacije zaposlenika. Sa korektnim kontrolama na konkretnim uređajima ova zona može biti pogodna za rad sa osjetljivim podacima ili kritičnim aplikacijama. Unutar ove zone saobraćaj obično nije ograničen i može da potiče od autorizovanih eksternih resursa. Primjer eksternog saobraćaja su remote access i extranet.

Prilikom komunikacije sa spoljašnjom zonom sledeća politika treba da važi:

- Sva komunikacija sa spoljašnjom zonom se odvija preko proxy servisa zone javnog pristupa. Za specijalne slučajeve kada ovo nije moguće potrebno je izvršiti whitelist-ovanje ili odbiti komunikaciju.

U komunikaciji sa zonom javnog pristupa i zonom sa ograničenim pristupom treba da važi sledeća politika:

- Sva komunikacija sa navedenim zonama mora da bude whitelist-ovana i filtrirana od strane interfejsne tačke.

3.4.4 ZONA SA OGRANIČENIM PRISTUPOM

Obezbjeđuje kontrolisano mrežno okruženje generalno namjenjeno za poslovno kritične IT servise (gdje bi gubitak servisa značio prekid usluge) ili velike repozitorijume osjetljivih informacija. Dozvoljava povezivanje sa sistemima u javnoj spoljašnjoj zoni putem zone javnog pristupa. Svi mrežni entiteti u ovoj zoni su autentifikovani na neki način, putem mehanizama autentifikacije ili fizički i putem konfiguracionih kontrola. Ova zona smanjuje prijetnje sa vana ograničavajućo pristup i kroz administrativno praćenje (monitoring). Usluge za povjerljivost podataka su implementirane da se zaštiti saobraćaj zone od prisluškivanja.

U komunikaciji sa spoljašnjom zonom važi sledeća politika :

- Zona sa ograničenim pristupom ne komunicira sa spoljašnjom zonom.

Pri komunikaciji sa operativnom i zonom javnog pristupa važi:

- Sve komunikacije između ove zone i ostalih zona će biti procesirane u interfejsnoj tači i whitelist-ovane.
- Zona sa ograničenim pristupom komunicira direktno samo sa operativnom zonom i drugim zonama sa ograničenim pristupom.

3.4.5 ZONA ZA MENADŽMENT

Obezbjeđuje visoko kontrolisano mrežno okruženje generalno pogodno za aplikacije kojima je kritična sigurnost (one sa visokim zahtjevima za pouzdanost, čije se narušavanje odražava opasnošću za stabilnost sistema). Samo druge zone koje su

pod kontrolom kompanije mogu pristupati ovim zonama. Svi entiteti sa mreže su autentifikovani. Ova zona ima strožije zahtjeve za uređaje od zone ograničenog pristupa. Takođe postavlja strožija pravila i kontrole nad internim korisnicima kako bi se osigurala od te prijetnje. Servisi za povjerljivost podataka su postavljeni da sprječe prisluškivanje. U ovu zonu se obično smještaju servisi za administraciju sistema.

Pri komunikaciji sa spoljašnjom zonom važi sledeća politika:

- Servisi unutar zone za menadžment komuniciraju sa spoljašnjom zonom samo putem zone javnog pristupa u svrhu ažuriranja softvera verifikovanih prodavaca putem bezbjedne komunikacije.

U komunikaciji sa operativnom, zonom za javni pristup i zonom sa ograničenim pristupom važi:

- Sav saobraćaj sa navedenim zonama je whitelist-ovan, a prati se i filtrira u interfejsnoj tački.
- Zona za menadžment komunicira sa svim zonama koje su pod kontrolom ogranizacije.

3.4.6 ZONA SA SPECIJALNIM PRISTUPOM

Jako kontrolisano mrežno okruženje pogodno za specijalne potrebe procesiranja. Zahtjevi za ovu zonu bi se razvijali po potrebi, u skladu sa konkretnom situacijom.

3.4.7 ZONA ZA EKSTRANET

Specijalna zona koja omogućava pristup povjerljivim eksternim entitetima i pravila se razvijaju u zavisnosti od konkretne situacije. Česte upotrebe ove zone su u svrhu integracije finansijskih institucija, državno-provincijski interfejsi, interfejsi sa drugim vladama itd. Politike ove zone se razvijaju u skladu sa potrebama.

3.4.8 INTERNA KONFIGURACIJA ZONA

Za uspostavljanje korektne arhitekture bezbjednosnih zona organizacije bi trebale ispoštovati neke kritične zahtjeve navedene u sledećim grupama:

- Zahtjevi za mrežne interfejse – skup pravila koji definišu bezbjednosne zahtjeve za tipove interfejsa koji su dozvoljeni prema drugim zonama, korištenju zajedničke infrastrukture i djeljenje uređaja sa drugim zonama.
- Zahtjevi za kontrolu saobraćaja – skup pravila koja se odnose na protok mrežnog saobraćaja kroz zonu i između zona. Ova pravila definišu tipove saobraćaja, pravila o uvezivanju ili sprječavanju uvezivanja sa drugim zonama itd.
- Zahtjevi mrežne konfiguracije – skup bezbjednosnih zahtjeva koji upravljaju vezama upređaja na zone. Ovi zahtjevi se odnose na upravljanje asocijacijama

između mrežnih entiteta, fizičkih interfejsa i upravljanje i kontrolu nad fizičkim prenosom. Zahtjevi mrežne konfiguracije specifikuju zaštite i neophodne za kontrolu dodavanja i uklanjanja uređaja vezanih za jednu zonu. Ograničenjem fizičkog pristupa značajno se redukuje vjerovatnoća napada na mrežu.

- Zahtjevi vezani za zaštitu podataka – zahtjevi za uspostavljanje servisa za zaštitu podataka.

Zone izoluju bezbjednosne aspekte mrežne infrastrukture od poslovnih procesa i nude aplikacijama predvidljiv nivo bezbjednosti dok osiguravaju da je funkcionalnost bezbjednosti relativno transparentna. Bezbjednosne zone daju objektivnu mjeru za procjenu mrežne bezbjednosti.

Prilikom implementacije zona i klasifikacije servisa prema bezbjednosnim zahtjevima može se doći do tabele slične tabeli 1.1.

Zona javnog pristupa	Operativna zona	Zona ograničenog pristupa	Zona za menadžment
Eksterni DNS Email Proxy Reverse Proxy Web Aplikacije Udaljeni Pristup	Servis Autentifikacije Desktop Email Interni DNS VOIP Servisi za podatke	Servisi za kritične podatke	Servisi za logove Backup servisi Administrativni servisi Sevisi za administraciju bezbjednosti

Tabela 1.1 Raspored servisa prema zonama

DODATAK A – SAŽETAK SMJERNICA

- Organizacije bi prije bilo kakve tehničke segmentacije mreže i dizajna politika trebale da izvrše klasifikaciju svojih resursa kako bi ih grupisali na korektan način.
- Shodno resursima koji se u njima nalaze organizacije bi trebale da definišu sigurne administrativne zone kao prostore ili prostorije u kojima se čuvaju podaci i uređaji koji zahtjevaju odgovarajuću fizičku zaštitu.
- Prilikom segmentacije mreže organizacije bi trebalo da izvrše organizaciju IP opsega kako bi se dodatno olakšalo kreiranje bezbjednosnih politika.
- Organizacije bi trebalo da definišu bezbjednosne zone, kako bi smanjile rizik otvorene mreže formiranjem logičkih gripa koje imaju iste bezbjednosne politike i zahtjeve.

- Nakon definisanja zona, organizacije bi trebalo da izvrše uspostavljanje interfejsnih tačaka zona na granicama između zona.
- Bezbjednosne zone trebaju da komuniciraju samo preko definisanih interfejsnih tačaka.
- Fokus interfejsne tačke pri kontroli saobraćaja treba da bude na saobraćaju koji ulazi u nju.
- Ukoliko se interfejsna tačka povezuje na zonu višeg nivoa nije potrebno filtriranje dolaznog saobraćaja, ali jeste potreban nadzor.
- Interfejsne tačne trebaju sadržavati mehanizme za nadzor saobraćaja, detekciju i prevenciju napada, te mehanizme za logovanje.
- Svaka odvojena mreža treba da se nalazi samo unutar jedne zone.
- Za zone višeg nivoa privatnosti, potrebno je vršiti autentifikaciju pri ulasku u zonu.
- Za uspostavljanje korektne arhitekture bezbjednosnih zona organizacije bi trebalo da uspostave zahtjeve za mrežne interfejse, kontrolu saobraćaja, mrežne konfiguracije i zahtjeve vezane za zaštitu podataka.
- Sav dolazni saobraćaj zoni javnog pristupa iz spoljašnje zone terminira se u proxy servisima unutar zone javnog pristupa nakon filtriranja od strane interfejsne tačke – U nekim uslovima ovo nije moguće, tada je potrebno razmotriti bezbjednosne prijetnje i osmisliti alternativno rješenje.
- Sav dolazni i odlazni saobraćaj za zonu javnog pristupa iz spoljašnje zone treba biti ograničen na osnovu blacklist-a. Blacklist sadrži listu mrežnih adresa spoljašnje zone koje su pridružene prošlim malicioznim aktivnostima.
- Sav odlazni saobraćaj iz zone javnog pristupa treba biti filtriran tako da samo adrese iz definisanog internog opsega mogu da komuniciraju sa spoljašnjom zonom.
- Desktopi moraju koristiti proxy servise zone javnog pristupa za pristup spoljašnjoj mreži.
- Sva komunikacija operativne zone sa spoljašnjom zonom se odvija preko proxy servisa zone javnog pristupa. Za specijalne slučajeve kada ovo nije moguće potrebno je izvršiti whitelist-ovanje ili odbiti komunikaciju.
- Zona sa ograničenim pristupom ne komunicira sa spoljašnjom zonom.
- Zona sa ograničenim pristupom komunicira direktno samo sa operativnom zonom i drugim zonama sa ograničenim pristupom.
- Servisi unutar zone za menadžment komuniciraju sa spoljašnjom zonom samo putem zone javnog pristupa u svrhu ažuriranja softvera verifikovanih prodavaca putem bezbjedne komunikacije.
- Zona za menadžment komunicira sa svim zonama koje su pod kontrolom ogranizacije.

DODATAK B – POJMOVI I DEFINICIJE

Bezbjednosni napad – svaka aktivnost koja ugrožava bezbjednost informacija u vlasništvu organizacije.

Bezbjednosni mehanizam – proces projektovan za otkrivanje, sprječavanje ili oporavak od bezbjednosnog napada.

Bezbjednosni servis – servis za obradu ili komunikaciju koji unaprjeđuje bezbjednost sistema za obradu podataka i prenos informacija jedne organizacije. Servisi su namjenjeni za suprotstavljanje bezbjednosnim napadima, a za pružanje te usluge koriste jedan ili više bezbjednosnih mehanizama.

Povjerljivost podataka – definiše da li je podatak dostupan samo licima koja su ovlašćena da ostvare pristup i dalje postupaju sa tim podatkom.

Cjelovitost podataka – podrazumjeva očuvanje postojanja, tačnosti i kompletnosti podataka, kao i zaštitu procesa ili programa koji sprječavaju neovlašćeno mijenjanje podataka.

Dostupnost podataka – podrazumjeva mogućnost da ovlašćeni korisnici mogu pristupiti podatku uvijek kada za tim imaju potrebu.

Sigurne administrativne zone - prostori ili prostorije u kojima se čuvaju podaci i uređaji koji zahtjevaju odgovarajuću fizičku zaštitu

Segmentacija – proces odvajanja LAN grupa uređaja, predstavlja jednu od osnovnih mjera zaštite računarskih mreža.

Bezbjednosna zona – mrežni segment sa dobro definisanim tokom komunikacija prema drugim zonama i na kom se nalaze sistemi i komponente sa srodnim zahtjevima za zaštitu informacija i klasifikacijama dozvola pristupa.

IP shema – funkcionalna organizacija IP opsega kako bi se dodatno olakšalo kreiranje bezbjednosnih politika.

Aktivni napad – napad na mrežu koji pokušava da izmjeni sistemske resurse ili utiče na njihov rad.

Pasivni napad – napad na mrežu sa ciljem dobavljanja neke informacije koja se prenosi u komunikaciji.

Tražilac pristupa –uređaj koji pokušava da pristupi mreži.

Server polise – na osnovu pozicije tražioca pristupa definisane u preduzeću, server polise utvrđuje kakav pristup treba odobriti.

Server za pristup mreži – funkcioniše kao tačka kontrole pristupa za korisnike na udaljenim lokacijama koji se povezuju sa unutrašnjom mrežom preduzeća.

Flat mreža – računarska mreža koja je od spoljašnjih prijetnji odvojena jednom barijerom, a saobraćaj unutar nje se kreće bez jakih kontrola.

Socijalni inženjering – skup metoda socijalne manipulacije koje napadači koriste kako bi naveli korisnike da urede nešto u korist napadača.

Botnet – veći skup računara pod kontrolom napadača, koristi se za izvođenje masivnih koordinisanih napada.

802.1Q – mrežni standard koji podržava VLAN na ethernet mreži.

IEEE 802.1X – standard za port baziranu kontrolu pristupa mreži.

DODATAK C – AKRONIMI

CERT – Computer Emergency Response Team

OIB – Odjeljenje za Informacionu Bezbjednost

LAN – Local Area Network

IP – Internet Protocol

IEEE - Institute of Electrical and Electronics Engineers

EAP – Extensible Authentication Protocol

EAPOL – EAP Over LAN

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

IPsec – Internet Protocol Security

SIEM – Security Information and Event Management

MAC – Media Access Control

WLAN – Wireless Local Area Network

RADIUS – Remote Authtentication Dial-In User Service

NIC – Network Interface Controller

DHCP – Dynamic Host Configuration Protocol

RFC – Request For Comments

DODATAK D – LITERATURA

1) Daniel Oxenhandler GSEC – ver. 1.4b, “Designing a Secure Local Area Network” https://www.sans.org/reading-room/whitepapers/bestprac/designing-secure-local-area-network-853

2) Keith Stouffer Joe Falco Karen Scarfone, “Guide to Industrial Control Systems (ICS) Security” http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

3) Garrett Leischner and Cody Tews, Schweitzer Engineering Laboratories, Inc. , “Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability” http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.125.5869&rep=rep1&type=pdf

4) “Network Security Zoning Design Considerations for Placement of Services within Zones” https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg38-eng_0.pdf

5) “Baseline Security Requirements for Network Security Zones in the Government of Canada” https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg22-eng_0.pdf

6) Peter Kai Wimmer, “Secure Network Zones” https://www.atsec.com/downloads/pdf/ISSE_2009-Secure_network_zones-Peter_Wimmer.pdf

7) William Stallings, “Network Security Essentials: Applications and Standards, Fifth Edition”

8) Zakon o informacionoj bezbjednosti http://oib.aidrs.local/sites/default/files/Zakon_o_informacionoj_bezbjednosti.pdf

9) Uredba o mjerama informacione bezbjednosti
http://oib.aidrs.local/sites/default/files/Uredba_o_mjerama_informacione_bezbjednosti.pdf