Sigurnost IT sustava smještenih u višeoblačnom okruženju

Ardalić, Jelena

Professional thesis / Završni specijalistički

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:168:671836

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-25**

Repository / Repozitorij:

FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repozitory

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Jelena Ardalić

SIGURNOST IT SUSTAVA SMJEŠTENIH U VIŠEOBLAČNOM OKRUŽENJU

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Jelena Ardalić

SECURITY OF IT SYSTEMS IN MULTI-CLOUD ENVIRONMENT

SIGURNOST IT SUSTAVA SMJEŠTENIH U VIŠEOBLAČNOM OKRUŽENJU

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2023.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija Informacijska sigurnost.
Mentor(i): izv. prof. dr. sc. Miljenko Mikuc

Specijalistički rad ima: 64 stranice

Specijalistički rad br.:_____.

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Marin Vuković – predsjednik
2. izv. prof. dr. sc. Miljenko Mikuc – mentor
3. izv. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek - član

Povjerenstvo za obranu u sastavu:

1. izv. prof. dr. sc. Marin Vuković – predsjednik
2. izv. prof. dr. sc. Miljenko Mikuc – mentor
3. izv. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek - član

Datum obrane: 23. listopada 2023.

Sažetak

Cilj rada je prikazati primjenu sigurnosnih direktiva, koncepata i mehanizama na modelu sve prisutnijeg višeoblačnog sustava. Naime, pojava pandemije Covid-19 promijenila je način rada za mnoge organizacije kada je veliki broj zaposlenika zamijenio urede organizacija s vlastitim domom. To je dovelo i do sve veće potrebe za udaljenim pristupom resursima organizacije, i sve većim migracijama aplikacija i usluga u oblačne sustave. Takav pristup je pak potaknuo organizacije da sve više razmišljaju o sigurnosnim rizicima, te uspostavljanju vlastitih sigurnosnih strategija, kako ostvariti identifikaciju, provjeru autentičnosti i nadzor korisnika i uređaja te koje još dodatne mehanizme zaštite trebaju kako bi osigurali svoju infrastrukturu i informacije. Uzevši o obzir potrebe koje se nameću ubrzanom digitalnom transformacijom, ovaj rad prikazuje okvir NIS direktive s dostupnim alatima za uspostavljanje sigurnosne strategije i upravljanje njenim životnim ciklusom. Osim što je za organizaciju bitno da ima uspostavljenu sigurnosnu strategiju bitno je i da je implementirano rješenje u skladu s najboljim sigurnosnim praksama, koje su u skladu s najpoznatijim standardima u području kibernetičke sigurnosti, te na koje se oslanjaju i dostupna tehnička rješenja opisana u ovom radu – softverski definirane mreže i mehanizmi zaštite na aplikativnom nivou.

Summary

The aim of this paper is to show how security directives, concepts and mechanisms can be applied on increasingly present multi-cloud system. The emergence of Covid-19 pandemic changed the way of working for many organizations when a large number of employees replaced the organizations' offices with their own homes. That has led to an increasing need for remote access to the organization's resources, and increasing migrations of apllications and services to cloud systems. Such an approach has encouraged organizations to think more and more about security risks, about establishing their own security strategies, how to achieve identification, authentication and monitoring of users and devices, and what additional protection mechanisms they need to secure their infrastructure and information. Taking into account the needs imposed by the accelerated digital transformation, this paper presents the framework of the NIS directive with available tools for establishing a security strategy and managing its life cycle. In addition to the fact that it is important for the organization to have an established security strategy, it is also important that the implemented solution is in accordance with the best security practices, which are in accordance with the most well-known standards in the field of cyber security. Moreover, the available technical solutions described in this paper, software-defined networks and protection mechanisms at the application level, also rely on those standards.

Sadržaj

1 Uvod

Scenariji koje smo prije viđali na filmovima vezano uz hakere koji probijaju velike i kritične sustave postaju stvarni izazovi u današnje doba digitalne transformacije. Kako bi se osigurala minimalna razina sigurnosti mrežnih i informacijskih sustava za sve države članice Europske Unije (EU), Agencija Europske unije za kibersigurnost (engl. European Union Agency for Cybersecurity, ENISA) 2016. godine donosi direktivu o mrežnoj i informacijskoj sigurnosti (engl. Network and Information Security, NIS). Početkom 2023.godine usvojena je revidirana NIS 2 direktiva koja proširuje opseg primjene, definira jače zahtjeve za upravljanje rizikom kibernetičke sigurnosti kojih se organizacije moraju pridržavati, te pojednostavljuje obveze izvješćivanja o incidentima s preciznijim odredbama o izvješćivanju, sadržaju i vremenskom okviru. Temeljni cilj NIS direktive je uvođenje zajedničkih minimalnih sigurnosnih zahtjeva za operatore ključnih usluga i pružatelje digitalnih usluga, te minimalne zahtjeve za planiranje i izgradnju potrebnog kapaciteta, međusobnu suradnju i razmjenu informacija. Kako bi NIS direktiva trebala podići svijest o sigurnosti i kao takva stvoriti podlogu za razvoj i rast digitalne transformacije, preporuka je za sve organizacije voditi se načelima i mjerama propisanima NIS/NIS2 direktivom neovisno jesu li zakonski obvezne slijediti ju ili ne.

Digitalna transformacija donosi i povećani broj korisnika, uređaja, vrsta uređaja što dovodi do potreba za sve većom, bržom i pouzdanijom komunikacijom s raznih udaljenih lokacija. Sve navedeno dovodi do izazova i promjena u računalnim i mrežnim paradigmama. Iz perspektive mreža dolazi do promjene obrazaca prometa, povećanoj raznolikosti pristupa, rastućim potrebama za kapacitetima što sve skupa povlači i dodatne sigurnosne izazove. U podatkovnim centrima je sve više zahtijeva i za komunikaciju i prometom između pojedinih komponenata, a ne samo komunikacijom i prometom između klijenata i poslužitelja. Raste i potreba za povezivanje korporativne mreže s infrastrukturom pružatelja usluga u oblaku, što rezultira i dodatnim prometom iz podatkovnih centara i/ili pristupnih mreža preko mreže širokog područja do privatnih ili javnih oblaka. Nadalje, korisnici sve više koriste osobne mobilne uređaje za pristup korporativnim mrežama. Uz udaljene i/ ili mobilne pojedince i usluge u oblaku, kompleksnost dodatno povećavaju i višestruke interne mreže, te udaljene lokacije s vlastitom infrastrukturom. Ta raznolikost infrastrukture dovela je i do otežanog upravljana istom te ugrožavanja mrežne sigurnosti koja se temeljila na perimetru. Budući da više ne postoji jedinstveni perimetar, koji se lako identificira za pojedinu organizaciju, samim time i površina napada je veća. To je olakotna okolnost za napadače, lakše im je zaobići perimetar te kada ga

probiju, nesmetano im je daljnje lateralno kretanje. Sve to dovodi do potreba za novom mrežnom paradigmom, koja bi bila u stanju suprotstaviti se prijetnjama izvan i unutar organizacije, odnosno pružiti obranu i unutar perimetra. Model sigurnosti *bez povjerenja*, poznat i kao arhitektura *nultog povjerenja* (engl. zero trust), opisuje pristup dizajnu i implementaciji IT sustava gdje je inherentno povjerenje u mrežu uklonjeno. Glavni koncept koji stoji iza sigurnosnog modela s nultim povjerenjem je "nikad ne vjeruj, uvijek provjeravaj", što znači da se uređajima i korisnicima ne bi trebalo neopozivo vjerovati, čak i ako su povezani na dopuštenu mrežu kao što je lokalna korporativna mreža. Umjesto toga, svaki zahtjev za pristup provjerava se na temelju politike pristupa. Za svaki zahtjev za pristup gradi se kontekst, koji se oslanja na jaku autentifikaciju i autorizaciju, ispravnost pristupnog uređaja te vrijednost podataka kojima se pristupa. Provjera konteksta je zapravo provjera sigurnosnog položaja subjekta koji je uputio zahtjev za pristup.

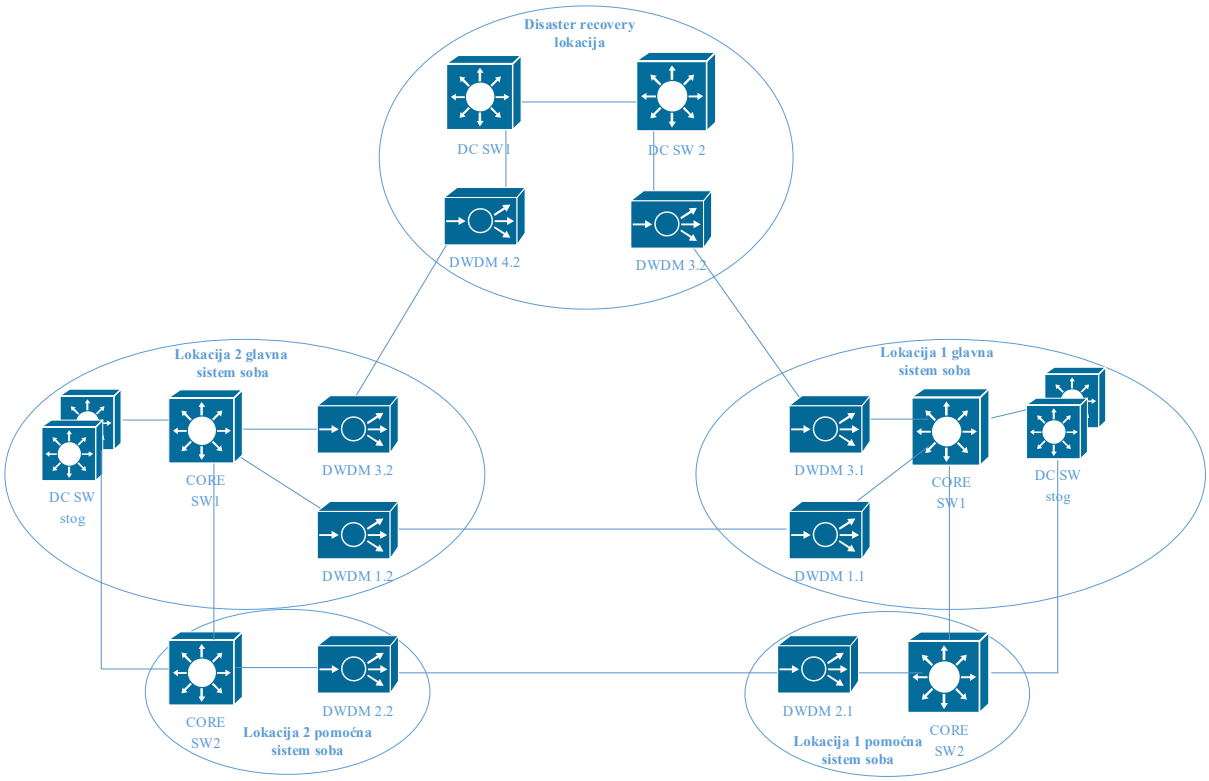
U takvim modernim okruženjima, u kojima su aplikacije te koje pokreću poslovanje, potrebno je osim mrežne sigurnosti ugraditi i dodatne mehanizme zaštite na aplikativnom nivou. Dodavanjem novih funkcionalnosti u aplikacije, upotrebom aplikacijskih programskih sučelja, raznim točkama integracije i smještajem istih u javne oblake dolazi do potrebe za naprednim sigurnosnim kontrolama aplikacija. Kako bi organizacije osigurale svoje poslovno kritične aplikacije koje su izložene Internetu, u opseg implementiranih sigurnosnih rješenja uvode se i dodatna sigurnosna rješenja na aplikativnom nivou, kao što su vatrozid web aplikacija (engl. Web Application Firewall, WAF), rješenja za balansiranje i zaštitu web prometa, za zaštitu elektroničke pošte, za zaštitu od DDoS napada.

Rad je strukturiran na način da se u prvom poglavlju predstavi model višeoblačnog sustava na kojem će se kroz rad razrađivati primjena sigurnosnih rješenja. Drugo poglavlje se osvrće na NIS direktivu, te alate, ciljeve i sigurnosne mjere koje ona definira s ciljem uvida kako se isti mogu primijeniti na opisanom modelu. Treće poglavlje daje pregled modela nultog povjerenja i skupa tehničkih rješenja koji su implementirani na opisanom modelu. Četvrto poglavlje prikazuje dodatne mehanizme zaštite na aplikativnom nivou koji su implementirani na opisanom modelu s ciljem postizanja zaštite u dubinu. Zaključak donosi osvrt na prednosti i izazove koje donose obrađeni koncepti i implementirana rješenja.

2 Model višeoblačnog sustava

Model višeoblačnog sustava koji će se obrađivati u ovom specijalističkom radu sastoji se od dva podatkovna centra smještena na dvije odvojene fizičke lokacije organizacije, koji čine privatni oblak, trećeg podatkovnog centra koji je smješten u drugoj potresnoj zoni u iznajmljenom prostoru javnog oblaka te dodatnog poslužitelja, koji je smješten u drugom javnom oblaku u drugoj zoni dostupnosti. Taj dodatni poslužitelj služi kao svjedok (engl. witness server), koji osigurava kvorum u slučaju nekonzistentnosti podataka u podatkovnim centrima koja može nastati zbog pogrešaka na linkovima preko kojih se odvija sinkronizacija podataka između poslužitelja ili pogrešaka u radu poslužitelja. Svi podatkovni centri i poslužitelji su dio jednog logičkog rastegnutog klastera. S dva podatkovna centra na lokacijama organizacije se postiže visoka dostupnost svih servisa i pristupa Internetu. Dodatno se na lokacijama podatkovnih centara nalazi po jedna glavna sistem soba i po jedna pomoćna sistem soba kako bi se osigurala povezanost mikrolokacija do podatkovnog centra na udaljenoj lokaciji u slučaju bilo kakvog ispada ili katastrofe u lokalnoj glavnoj sistem sobi. Treći podatkovni centar u iznajmljenom prostoru javnog oblaka služi kao lokacija za oporavak od katastrofe (engl. disaster recovery, DR) kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe. Poslužitelj svjedok smješten u drugom javnom oblaku kako bi u slučaju raspada klastera dvije virtualne mašine odnosno klastera aplikacije odlučio koja je mjerodavna i koja bi trebala nastavljati obavljati aktivne funkcije do popravka stanja tog klastera.

Sva tri podatkovna centra su međusobno povezani iznajmljenim optičkim linkovima (engl. dark fiber) zakupljenima od telekom pružatelja usluga korištenjem optičkog prijenosnog sustava, kako prikazuje *Slika 1.* Optički prijenosni sustav služi za prijenos više signala na različitim valnim duljinama kroz jedno optičko vlakno. Sustav je namijenjen za multipleksiranje s gustom valnom podjelom (engl. Dense Wavelength Division Multiplexing, DWDM).



Slika 1 *Međupovezanost podatkovnih centara*

Podatkovni centri na lokacijama organizacije s mrežne strane predstavljaju jedan rastegnuti klaster (engl. streched cluster), što znači da se koristi jedan IP adresni plan za oba podatkovna centra, te u slučaju bilo kakvog ispada jednog od podatkovnih centara nije potrebna ručna promjena IP adresa. Poslužitelji se mogu seliti iz jednog podatkovnog centra u drugi bez potrebe promjene konfiguracije poslužitelja. U podatkovnim centrima nalazi se dio zajedničkih servisa, kao što su DHCP (engl. Dynamic Host Configuration Protocol), NTP (engl. Network Time Protocol), DNS (engl. Domain Name System), dok je dio servisa zakupljen kao usluga u javnim oblacima, kao što su usluga elektroničke pošte i zaštita elektroničke pošte, usluga zajedničkog mjesta za pohranu i dijeljenje datoteka i dokumenata.

Komponente podatkovnog centra i njihova međupovezanost su simetrična u sva tri podatkovna centra. Svi poslužitelji u podatkovnom centru su povezani 10G ili 25G linkovima, ovisno o mogućnostima poslužitelja, na dva preklopnika podatkovnog centra (DC SW stog) složenih u stog (engl. stack) kako bi se postigla visoka dostupnost poslužitelja odnosno servisa koji se nalaze na njima. Preko tih preklopnika poslužitelji ostvaruju vezu na vatrozid za promet unutar podatkovnog centra. Preklopnici podatkovnog centra su 100G vezama povezani na dva jezgrena preklopnika složena u stog kako bi krajnjim korisnicima pružila brza veza prema

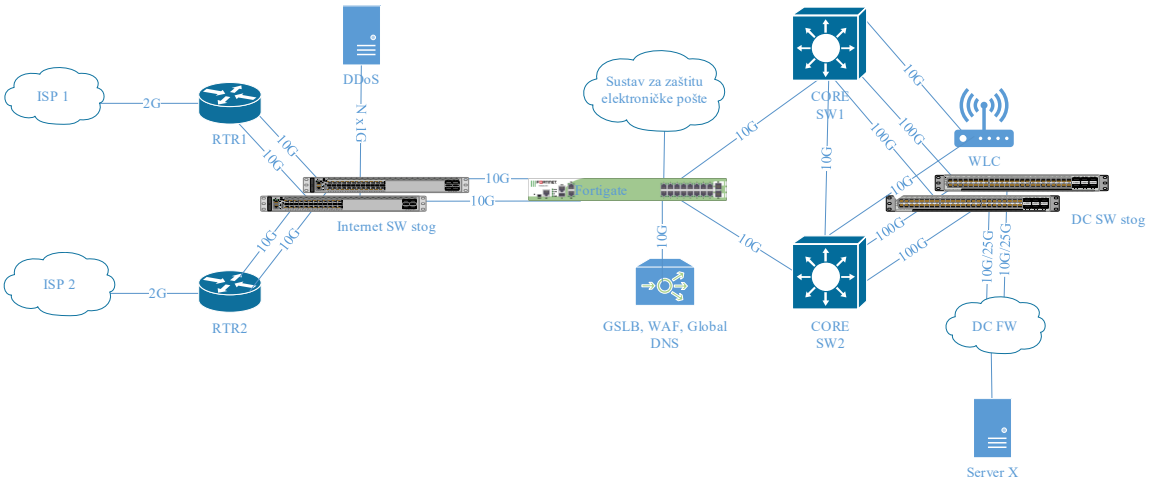
podatkovnim centrima. Jezgreni preklopnici, smješteni po jedan u glavnoj sistem sobi i po jedan u pomoćnoj sistem sobi na svakoj lokaciji, služe kao agregacijski čvor za pristupne preklopnike na koje su spojeni krajnji uređaji i korisnici. Po jedan kontroler za centralno upravljanje i nadzor bežičnih pristupnih točaka (engl. Wireless Controller, WLC) spojen je na svakoj lokaciji na jezgrene preklopnike 10G linkovima. Jezgreni preklopnici su drugim krajem spojeni 10G linkovima na perimetarski vatrozid, kroz koji prolazi sav promet sa Interneta. Perimetarski vatrozidi nove generacije su složeni za način rada visoke dostupnosti s jednim aktivnim uređajem a drugim u stanju pripravnosti koji preuzima aktivnu ulogu u slučaju ispada primarnog aktivnog uređaja i nema gubitka funkcije perimetarskog vatrozida. Ti vatrozidi pružaju kontrolu pristupa sadržaju na Internetu, zaštitu od prijetnji s Interneta, URL filtriranje web prometa, sigurnost sadržaja i uređaja na lokalnoj mreži, te služe za terminaciju VPN sesija. Dodatno imaju i komponentu za upravljanje te prikupljanje logova i izvještavanje o događajima. Perimetarski vatrozidi su preko Internet preklopnika 10G linkovima spojeni na Internet usmjernike na koji su spojeni Internet linkovi pružatelja internet usluga. Za ostvarivanje visoke dostupnosti Internet linkova, između usmjernika i vatrozida je implementiran protokol koji podržava konfiguraciju s dva podrazumijevana poveznika, jednim aktivnim i drugim u stanju pripravnosti.

Prema sigurnosnim preporukama o zaštiti u dubinu, odnosno zaštiti na više razina osim perimetarskog vatrozida i vatrozida za podatkovni centar, model ima implementiran i vatrozid web aplikacija sa sustavom za balansiranje opterećenja web prometa, sustav za zaštitu od DDoS napada i sustav za zaštitu elektroničke pošte. Za potrebe servisa koji su dostupni s Interneta, kao i za interne servise dostupne korisnicima, koristi se globalni DNS sustav za balansiranje web prometa (engl. Global Service Load Balancer, GSLB) koji osigurava preusmjeravanje upita na ispravnu IP adresu neovisno o pružatelju internet usluga. Tim sustavom se izbjegava ručno mijenjanje DNS zapisa na višestrukim uređajima u mreži u slučaju ispada nekog servisa te smanjuje vrijeme propagacije istoga.

Veza na Internet je ostvarena preko dva različita pružatelja Internet usluga koji se spajaju na dva usmjernika na svakoj lokaciji podatkovnog centra kako bi se osiguralo da ispad bilo kojeg Internet linka ne utječe na dostupnost servisa i pristup Internetu iz lokalne mreže. U tu svrhu se između usmjernika, na istoj lokaciji, koristi protokol za usmjeravanje unutar autonomnih sustava (*internal Border Gateway Protocol, iBGP*). Za razmjenu staza prema pružateljima usluga se koristi protokol za usmjeravanje između autonomnih sustava (*external Border*

Gateway Protocol, eBGP). Promet između mrežnih komponenti usmjerava se preko protokola stanja veze (*Open Shortest Path First, OSPF*).

Shematski prikaz svih opisanih komponenti i njihova povezanost u jednom podatkovnom centru prikazan je na *Slika 2*.



Slika 2 *Shematski prikaz svih komponenti i njihova povezanost u jednom podatkovnom centru*

Za spajanje udaljenih lokacija ugovoreni su *dark fiber* linkovi od udaljene lokacije prema lokacijama podatkovnih centara, koji su preduvjet za implementaciju softverski definiranih širokopojasnih mreža. *Dark fiber* linkovi terminiraju na agregacijskim preklopnicima na udaljenim lokacijama i na jezgrenim preklopnicima na lokacijama podatkovnih centara s podignutim *MACSec* tunelom. *MACSec* rješenje se koristi za enkripciju podatkovnog sloja modela OSI preko linkova pružatelja usluga kako bi se osigurao integritet i povjerljivost prijenosa podataka. Dodatna prednost *MACSec* rješenja je podržana brzina medija, bez gubitka performansi prilikom šifriranja i dešifriranja podataka.

3 Sigurnosna strategija usklađena s NIS direktivom

S ciljem sprječavanja kibernetičkih napada, te poboljšanja statusa kibernetičke sigurnosti kroz osiguranje integriteta i kontinuiteta poslovanja operatera ključnih i digitalnih usluga, direktiva NIS propisuje da tvrtke iz definiranih sektora moraju implementirati mjere za sprječavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava. Definirane mjere su tehničke i organizacijske mjere za upravljanje rizicima, koje moraju uzeti u obzir najnovija tehnička dostignuća i najbolje sigurnosne prakse, kako bi se postigla što veća i sigurnija zaštita.

Kako bi se osigurala veća kibernetička sigurnost na nivou EU-a te uklonile razlike u zahtjevima kibernetičke sigurnosti i u provedbi mjera kibernetičke sigurnosti u različitim državama članicama, donesena je revidirana NIS2 direktiva. NIS2 direktiva utvrđuje minimalne regulatorne okvire i mehanizme za učinkovitu suradnju među relevantnim tijelima u svakoj državi članici, strože nadzorne mjere za nacionalna tijela, strože zahtjeve za provedbu i ima za cilj uskladiti režime sankcija u svim državama članicama EU-a. Dodatno, proširuje područje primjene na opskrbne lance, na pružatelje javnih elektroničkih komunikacijskih mreža i usluga, usluga podatkovnih centara, gospodarenje otpadnim vodama i otpadom, proizvodnju kritičnih proizvoda, poštanske i kurirske usluge te subjekte javne uprave, kao i zdravstveni sektor. Područje primjene nije nužno ograničeno na spomenuta područja/industrije te je preporuka slijediti spomenutu direktivu za svaku organizaciju koja želi podići svoj nivo kibernetičke sigurnosti. NIS direktiva, i njena nasljednica NIS2 direktiva, pruža alate za upravljanje životnim ciklusom sigurnosne strategije, te ciljeve i minimalne sigurnosne mjere koje moraju biti implementirane. U nastavku će biti prikazani dostupni alati koje organizacija implementiranog rješenja može koristiti, dok pregled sigurnosnih tehničkih mjera je uvršten u dizajn implementiranog rješenja.

3.1 Upravljanje životnim ciklusom sigurnosne strategije

ENISA je izdala okvir za upravljanje životnim ciklusom razvoja nacionalnih strategija kibernetičke sigurnosti koji se na temelji na Demingovom modelu „Planiraj-Napravi-Provjeri-Djeluj/Prilagodi“ (engl. Plan-Do-Check-Act, PDCA). Demingov model opisuje četiri koraka i koristi se za kontrolu i kontinuirano poboljšanje politika, procesa, proizvoda i u konačnici strategija. Okvir definira uloge i odgovornosti svih sudionika te pruža okosnicu za koordinaciju različitih aktivnosti tijekom životnog ciklusa strategije. Pristup za upravljanje životnim ciklusom koristi rezultate faze evaluacije za održavanje i prilagođavanje strategije kako bi što brže mogle reagirati i prilagoditi svoje akcije novim prijetnjama i problemima koje donose.

Trenutno izdanje okvira obrađuje prva dva koraka, planiraj i napravi, a drugo izdanje će se usredotočiti na faze provjere i djelovanja tj. prilagodbe. Okvir te faze naziva:

- razvoj i provedba strategije - planiranje
- ocjenjivanje i prilagođavanje strategije – izvedba

Prvo izdanje popraćeno je i alatima za samoprocjenu trenutnog stanja kibernetičke sigurnosti te unapređenje i izgradnju strategije kibernetičke sigurnosti – okvir za procjenu nacionalnih sposobnosti (engl. National Capabilities Assessment Framework, NCAF), te skupom alata za rješavanje problema interoperabilnosti različitih metoda za upravljanje rizika informacijske sigurnosti (engl. EU RM toolbox) koji su prikazani u nastavku.

Predloženi okvir za upravljanje životnim ciklusom sigurnosne strategije je okvir koji je primjenjiv i na upravljanje životnim ciklusom sigurnosne strategije svake organizacije. Preporuka je koristiti predloženi okvir i dostupne alate kao dio digitalne strategije pojedine organizacije.

NCAF okvir osmišljen je za sudionike uključene u dizajniranje, implementaciju i evaluaciju nacionalnih strategija za kibernetičku sigurnost. Cilj NCAF okvira je pomoći državama članicama ili organizacijama poboljšati i izgraditi strateške i operativne sposobnosti kibernetičke sigurnosti te podići svijest o razini zrelosti države članice ili organizacije. NCAF okvir pruža državama članicama ili organizacijama samoprocjenu njihove razine kibernetičke zrelosti procjenom ciljeva i sposobnosti nacionalne ili organizacijske kibernetičke sigurnosti.

Kroz okvir se procjenjuje:

- sposobnost države članice ili organizacije za uspostavom odgovarajućih načina upravljanja, provedbom standarda i dobrih praksi u području kibernetičke sigurnosti,
- sposobnost države članice ili organizacije da kontinuirano gradi sposobnosti kibernetičke sigurnosti i povećava razinu znanja i vještina u tom području,
- sposobnost države članice ili organizacije za uspostavom pravnog okvira, potrebnih zakonskih i regulatornih instrumenata za rješavanje i suzbijanje porasta kibernetičkog kriminala, za zaštitu kritične informacijske infrastrukture, građana i organizacija,
- suradnja i razmjena informacija između različitih skupina na nacionalnoj i međunarodnoj razini.

Cilj EU RM paketa alata je zaduženim sudionicima za upravljanje rizicima pružiti referentni okvir kako bi se postiglo zajedničko razumijevanje rizika i povezanih razina rizika, te moglo procijeniti interoperabilne rizike. EU RM paket alata pruža referentni okvir za tumačenje, usporedbu i združivanje rezultata dobivenih različitim metodama procjene rizika. EU RM paket alata poštuje osobitosti odgovarajućih metoda za upravljanje rizikom i ne mijenja način na koji pojedine organizacije ili dijelovi organizacije rade na upravljanju svojim rizicima informacijske sigurnosti.

EU RM paket alata omogućuje zaduženim sudionicima rad na zajedničkim prijetnjama i scenarijima rizika te usporedbu njihovih razina rizika koristeći različite alate i metode. Nadalje daje upute kako tumačiti te rezultate i dobiti širi pogled na kibernetičku sigurnost organizacije, te kako se pojedini sektori i zemlje članice nose sa specifičnim prijetnjama što može pružiti podlogu za popunjavanje praznina i manjkavosti alata i metoda koje se trenutno koriste. Sastoji se od nekoliko komponenti koje se dijele na:

- funkcionalne – pridonose usklađivanju aktivnosti upravljanja rizikom te premošćuju praznine između različitih metoda procjene rizika usklađivanjem funkcija upravljanja rizikom sa alatima unutar paketa. Odnosno pružaju preslikavanje između baze znanja alata i odgovarajućih komponenti koje su usvojile različite metodologije upravljanja rizikom. Funkcionalne komponente su:
    - terminološko mapiranje,
    - mapiranje imovine,
    - mapiranje prijetnji,
    - mapiranje razina rizika,
- bazu znanja alata – pruža sve potrebne informacije funkcionalnim komponentama za preslikavanje scenarija rizika u metode upravljanja rizikom te načinima izvještavanja o razinama rizika, te se sastoji od:
    - terminologije,
    - klasifikacije imovine,
    - taksonomije prijetnji,
    - referentne ljestvice rizika.

Tablica 1 *Uloga EU RM alata i njegovo pozicioniranje u RM procesu [1]*

Područje	Terminologija	Imovina		Prijetnje -> Scenarij rizika	Utjecaj i nivoi rizika	
EU RM paket alata	Terminološko mapiranje/ terminologija	Mapiranje imovine/ klasifikacija imovine		Mapiranje/ taksonomija prijetnji	Mapiranje razine rizika sa referentnom ljestvicom rizika	
Alati organizacije	Interna procjena rizika					
Referentni okvir	Sigurnosne karakteristike sustava	Imovina	Modeliranje sustava	Identifikacija rizika	Analiza rizika	Upravljanje rizikom

Tablica 1 prikazuje pozicioniranje EU RM paketa alata kao srednjeg apstraktnog sloja između sloja scenarija rizika i sloja metodologije i alata za upravljanje rizikom koje koristi pojedina organizacija. Paket alata EU RM olakšava usklađivanje aktivnosti upravljanja rizikom korištenjem funkcija baze znanja kako prikazuje *Tablica 1*:

- terminologije – uspostaviti zajednički dogovor o aktivnostima tijekom procesa upravljanja rizikom koji omogućuje nedvosmisleno razumijevanje svake aktivnosti bez obzira na korištene alate i metodologiju za upravljanje rizikom,
- klasifikacije imovine – definirati opseg procjene rizika te zajedničku klasifikaciju i kategorizaciju imovine u definiranom opsegu i okruženju za razvoj nedvosmislenih scenarija rizika,
- taksonomije prijetnji – nakon odabira scenarij rizika za procjenu, koristiti zajedničku taksonomiju prijetnji (prirodne, industrijske prijetnje, namjerni napadi, prijetnje povezane sa uslugama, pogreške i nenamjerni kvarovi) za pojedini scenariji rizika kako bi ga se preslikalo na odgovarajuću internu metodu upravljanja rizikom što omogućuje organizacijama jednostavnu procjenu svojih razina rizika i sigurnosnog stanja svoje organizacije te paralelno normalizaciju izračunatih rezultata,

- referentne ljestvice rizika – služi za normalizaciju rezultata procjene rizika u zajedničku ljestvicu rizika odnosno preslikavanje izračunatih vrijednosti rizika, korištenjem interne metode upravljanja rizikom, na zajedničku referentnu ljestvicu rizika EU RM skupa alata, kako prikazuje *Tablica 2.* Izračun rizika informacijske sigurnosti prema EU RM paketu alata uzima u obzir razine utjecaja i vjerojatnosti prema sljedećoj jednadžbi,

$$R = (\text{vjerojatnost pojave prijetnje}) \times (\text{utjecaj prijetnje})$$

iz koje se definira pet diskretnih razina za vjerojatnost pojave prijetnje (*Tablica 2*).

Tablica 2 *Referentna ljestvica rizika EU RM alata [1]*

Referentna ljestvica rizika		**Vjerojatnost pojave prijetnje**				
		Vrlo visoka	**Visoka**	**Srednja**	**Niska**	**Zanemariva**
Utjecaj prijetnje	**Vrlo visok**	Vrlo visok	Vrlo visok	Visok	Srednji	Srednji
	Visok	Vrlo visok	Visok	Visok	Srednji	Nizak
	Srednji	Visok	Visok	Srednji	Srednji	Nizak
	Nizak	Srednji	Srednji	Srednji	Nizak	Zanemariv
	Zanemariv	Srednji	Nizak	Nizak	Zanemariv	Zanemariv

Prilikom definiranja funkcija oslanjalo se na standarde ISO 27005:2018 i ITSRM2.

Skup funkcija koje pruža EU RM paket alata je zamišljen kao proširiv skup koji bi unaprijedio i pružio jedinstven tretman rizika za sve države članice i organizacije, a uključivao bi nove kategorije imovine koje su izvan početne kategorizacije, prijetnje u nastajanju ili prijetnje koje su povezane s određenim okruženjima te popise sigurnosnih mjera.
Korištenje referentnog okvira i zajedničkih metrika za razine rizike pomaže regulatornim i nadzornim tijelima da dobiju bolji pregled i usporedbu razina rizika i sigurnosnog položaja organizacija u određenom sektoru te lakše praćenje aktivnosti po pitanju specifičnih prijetnji i scenarija rizika.

3.2 Ciljevi i sigurnosne mjere

NIS direktiva je služila kao prva zakonska podloga o kibernetičkoj sigurnosti na razini cijele EU s ciljem promicanja sigurnosnih mjera i povećanja razine sigurnosti mrežnih i informacijskih sustava kritične infrastrukture. Stavlja se naglasak na klasifikaciju rizika na sustave s nepredviđenim utjecajem i akcijske planove za poboljšanje otpornosti na napade. Pri tome se uzimaju u obzir ljudi, procesi i tehnologije kako bi se osigurao integritet, cjelovitost i dostupnost ključnih usluga za društvo i gospodarstvo.

Uzevši u obzir povećanu digitalizaciju i sve veći opseg kibernetičkih prijetnji, ENISA je donijela ažuriranu verziju, NIS2 direktivu koja poboljšava postojeći status kibernetičke sigurnosti u cijeloj EU na sljedeće načine:

- proširuje se opseg pravila na nove sektore i subjekte,
- poboljšava se otpornost i kapaciteti odgovora na incidente javnih i privatnih subjekata, nadležnih tijela i EU-a u cjelini kroz:
    - stvaranje potrebne strukture za upravljanje kibernetičkom sigurnošću,
    - povećanje razine usklađenosti sigurnosnih zahtjeva i obveza izvještavanja,
    - razmjenu znanja među državama članicama.

NIS direktiva daje i pregled zajedničkih strateških ciljeva koji bi trebali biti pokriveni strategijama nacionalne ili organizacijske kibernetičke sigurnosti, kako je prikazano u *Tablica 3*.

Tablica 3 *Strateški ciljevi NIS direktive* [2] *i način implementacije u opisanom modelu*

ID	NCSS strateški cilj	Detaljni opis cilja	Način implementacije
1	Razviti nacionalne ili organizacijske planove za nepredviđene situacije vezane uz kibernetičku sigurnost	- Predstaviti i objasniti kriterije za definiranje krizne situacije, - Definirati ključne procese i radnje za rješavanje kibernetičke krize, - Jasno definirati uloge i odgovornosti različitih dionika tijekom kibernetičke krize, - Predstaviti i objasniti kriterije za proglašenje kraja krize i/ili tko ima ovlasti proglasiti kraj krize,	Uspostavljeni Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji Treći podatkovni centar koji služi kao *DR* lokacija kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe uz popratni Plan organizacije za oporavka od katastrofe (engl. Disaster Recovery, DR)
2	Uspostaviti osnovne sigurnosne mjere	- Uskladiti različite prakse koje slijede organizacije u javnom i privatnom sektoru, - Stvoriti zajednički jezik između nadležnih javnih tijela i organizacija te stvoriti zaštićene komunikacijske kanale između istih za međusobnu komunikaciju, - Omogućiti različitim dionicima da provjere i usporede svoje sposobnosti kibernetičke sigurnosti, - Podijeliti informacije o dobrim praksama kibernetičke sigurnosti u svakom sektoru industrije, - Pomoći dionicima u prioritizaciji ulaganja u kibernetičku sigurnost,	Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga [3] Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti [4] Uspostavljen Program informacijske sigurnosti u organizaciji
3	Organizirati vježbe kibernetičke sigurnosti	- Utvrditi što treba testirati (planovi i procesi, ljudi, infrastruktura, sposobnosti odgovora, sposobnosti suradnje, komunikacija itd.), - Uspostaviti nacionalni tim za planiranje kibernetičkih vježbi,	Simulirane vježbe kibernetičke sigurnosti

		- Integrirati kibernetičke vježbe unutar životnog ciklusa nacionalne ili organizacijske strategije kibernetičke sigurnosti ili nacionalnog ili organizacijskog plana za kibernetičke situacije,	
4	Uspostaviti sposobnost odgovora na incident	- Definirati ovlasti, uloge i odgovornosti koje dotična vlada ili organizacijska upravljačka jedinica treba dodijeliti timu za upravljanje i rješavanje sigurnosnih incidenata, - Definirati portfelj usluga koje tim za upravljanje i rješavanje sigurnosnih incidenata pruža svojim korisnicima ili ih koristi za vlastito interno funkcioniranje, - Definirati operativne sposobnosti odnosno tehničke i operativne zahtjeve koje tim za upravljanje i rješavanje sigurnosnih incidenata mora ispuniti, - Definirati opseg suradnje odnosno zahtjeve u vezi s razmjenom informacija s drugim timovima koji nisu obuhvaćeni u prethodne tri kategorije, npr. kreatori politike, vojska, regulatori, operateri (kritične informacijske infrastrukture), tijela za provedbu zakona,	Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji
5	Podići svijest korisnika	- Identificirati nedostatke u znanju o problemima kibernetičke sigurnosti ili sigurnosti informacija, - Riješiti nedostatke podizanjem svijesti ili razvojem/jačanjem temeljnih znanja,	Edukacija korisnika organizacije Simulirane vježbe kibernetičke sigurnosti
6	Ojačati programe obuke i obrazovanja	- Poboljšati operativne sposobnosti postojeće radne snage za informacijsku sigurnost, - Potaknuti sudionike da se pridruže pripremljenim obukama za upoznavanje s kibernetičkom sigurnošću, - Promicati i poticati odnose između akademskih okruženja informacijske sigurnosti i industrije informacijske sigurnosti, - Uskladiti obuku o kibernetičkoj sigurnosti s poslovnim potrebama,	Edukacija korisnika organizacije Sudjelovanje korisnika organizacije na konferencijama o kibernetičkoj sigurnosti Simulirane vježbe kibernetičke sigurnosti

7	Poticati kulturu istraživanja i razvoja	- Utvrditi prave uzroke ranjivosti umjesto da se popravlja njihov utjecaj, - Okupiti znanstvenike iz različitih disciplina kako bi mogli pružiti rješenja za višedimenzionalne i složene probleme kao što su fizičke kibernetičke prijetnje, - Spojiti potrebe industrije i nalaze istraživanja, čime se olakšava prijelaz s teorije na praksu, - Pronaći načine za održavanje i povećanje razine kibernetičke sigurnosti proizvoda i usluga koje podržava implementirana kibernetička infrastruktura,	Uspostava SOC tima u organizaciji Implementacija SIEM rješenja u organizaciji Simulirane vježbe kibernetičke sigurnosti
8	Osigurati poticaje privatnom sektoru za ulaganje u sigurnosne mjere	- Identificirati moguće poticaje za privatne tvrtke da ulažu u sigurnosne mjere, - Osigurati tvrtkama poticaje za ulaganja u kibernetičku sigurnost,	Razne vrste financijskih i edukacijskih potpora za organizaciju
9	Zaštititi kritičnu informacijsku infrastrukturu, u koju se ubrajaju operateri bitnih usluga i pružatelji digitalnih usluga (zajednički naziv kritična informatička infrastruktura)	- Identificirati kritičnu informacijsku infrastrukturu, - Prepoznati i ublažiti relevantne rizike za kritičnu informacijsku infrastrukturu,	Analiza utjecaja na poslovanje (engl. Business Impact Analysis, BIA) organizacije Uspostavljen program Upravljanja rizicima (engl. Risk management, RM) u organizaciji
10	Donijeti zakone za područje kibernetičkog kriminala	- Donijeti zakone za područje kibernetičkog kriminala, - Povećati učinkovitosti agencija za provođenje zakona,	Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga [3]
11	Uspostaviti mehanizme za prijavu incidenata	- Steći znanje o cjelokupnom okruženju prijetnji, - Procijeniti utjecaj incidenata (npr. proboji sigurnosti, kvarovi mreže, prekidi usluge), - Steći znanje o postojećim i novim ranjivostima i vrstama napada, - U skladu sa stečenim saznanjima ažurirati sigurnosne mjere,	Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji

		- Provesti odredbe NIS Direktive o izvješćivanju o incidentima,	
12	Pojačati privatnost i zaštitu podataka	- Poraditi na jačanju temeljnih prava na privatnost i zaštitu podataka,	Uskladiti poslovanje organizacije sa općom uredbom o zaštiti podataka (engl. General Data Protection Regulation, GDPR)
13	Uspostaviti javno-privatno partnerstvo	- Raditi na zajedničkom odvraćanju napadača, - Raditi na zajedničkoj zaštiti koristeći istraživanje novih sigurnosnih prijetnji, - Raditi na zajedničkom otkrivanju koristeći dijeljenje informacija za rješavanje novih prijetnji, - Raditi na zajedničkom reagiranju kako bi se osigurala sposobnost suočavanja s početnim učinkom incidenta, - Raditi na zajedničkom oporavku kako bi se osigurala sposobnost popravljanja konačnog utjecaja incidenta,	Suradnja između organizacija, nadležnih tijela i timovima za odgovore na računalne sigurnosne incidente
14	Institucionalizirati suradnju između javnih agencija	- Povećati suradnju između javnih agencija s odgovornostima i nadležnostima povezanim s kibernetičkom sigurnošću, - Izbjegavati preklapanje nadležnosti i resursa između javnih agencija, - Poboljšati i institucionalizirati suradnju između javnih agencija u različitim područjima kibernetičke sigurnosti,	Dio nacionalne strategije o kibernetičkoj sigurnosti koju organizacija treba usvojiti i aktivno sudjelovati u dopuštenim granicama
15	Uključiti se u međunarodnu suradnju (ne samo s državama članicama EU)	- Iskoristiti stvaranje zajedničke baze znanja između država članica EU-a, - Stvoriti sinergijske učinke između nacionalnih tijela za kibernetičku sigurnost, - Omogućiti i pojačati borbu protiv transnacionalnog kriminala,	Dio nacionalne strategije o kibernetičkoj sigurnosti koju organizacija treba usvojiti i aktivno sudjelovati u dopuštenim granicama

ENISA je donijela i minimalni skup sigurnosnih mjera koje trebaju biti implementirane u mrežnim i informacijskim sustavima na razini EU-a. Te mjere nisu zamjena za postojeće standarde, okvire ili dobre prakse koje trenutno koriste operatori ključnih usluga i pružatelji digitalnih usluga ili druge organizacije koje se vode tim principima, već su mapirane s međunarodnim standardima. Sigurnosne mjere grupirane su u 4 domene: obrana (*Tablica 4*) , upravljanje i ekosustav (*Tablica 5)*, zaštita (*Tablica 6*) i otpornost (*Tablica 7*) koje su dalje podijeljene u pod domene [5].

Minimalni skup sigurnosnih mjera bi trebao služiti kao vodič za implementaciju svim organizacijama, posebno onima koje moderniziraju svoja poslovanja i prolaze kroz procese digitalne transformacije.

Tablica 4 *Minimalni skup sigurnosnih mjera prema NIS Direktivi* [5] *i način implementacije u opisanom modelu za domenu Obrana*

Pod domena	**Sigurnosna mjera**	**Opis**	**Mapiranje sa ISO 27001:2013 kontrolnim mjerama / zahtjevima**	**Mapiranje s NIST SP800-53 Rev5 CSF kategorijama kontrolnih mjera**	**Način implementacije**
Upravljanje računalnim sigurnosnim incidentima	Izvješće o incidentu	Operater ili organizacija kreira, ažurira i provodi procedure za prijavu incidenata	A.16 Upravljanje sigurnosnim incidentom 7.5 Dokumentirane informacije	IR – Odgovor na incidente AU- Revizija i odgovornost	Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji
Upravljanje računalnim sigurnosnim incidentima	Komunikacija s nadležnim tijelima	Operater ili organizacija implementira uslugu koja mu omogućuje da bez nepotrebnog odgađanja primi na znanje informacije koje je poslalo njegovo nacionalno nadležno tijelo u vezi s incidentima, ranjivostima, prijetnjama i relevantnim preslikavanjima	A.6 Organizacija informacijske sigurnosti 7.4 Komunikacije 7.5 Dokumentirane informacije	PM – Upravljanje programom informacijske sigurnosti IR - Odgovor na incidente SI - Zaštita integriteta sustava i informacija	Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji

Detekcija	Bilježenje	Operater ili organizacija postavlja sustav bilježenja za svaki kritični sustav kako bi se zabilježili događaji koji se odnose barem na autentifikaciju korisnika, upravljanje računima i pravima pristupa, izmjene sigurnosnih pravila i funkcioniranje samog sustava	A.12 Upravljanje operacijama A.15 Upravljanje odnosima s dobavljačima A.18 Sukladnost 9.1 Nadzor, mjerenje, analiza i evaluacija	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor CM – Upravljanje konfiguracijom AC – Kontrola pristupa SC- Zaštita sustava i komunikacija AU – Revizija i odgovornost	Komponente softverski definiranih mreža zadužene za automatizaciju upravljanja mrežom i uvid u stanje mreže i svih komponenti koje su spojene na istu
Detekcija	Korelacija i analiza zapisa	Operater ili organizacija radi korelaciju i analizu zapisa koji analizira događaje koje bilježi sustav za evidentiranje instaliran za svaki implementirani kritični sustav kako bi otkrio događaje koji utječu na sigurnost sustava	A.16 Upravljanje sigurnosnim incidentima 9.1 Nadzor, mjerenje, analiza i evaluacija	CA – Promjena, autorizacija i nadzor PM – Upravljanje programom informacijske sigurnosti IR – Odgovor na incidente AU - Revizija i odgovornost	Komponente softverski definiranih mreža zadužene za automatizaciju upravljanja mrežom i uvid u stanje mreže i svih komponenti koje su spojene na istu

Upravljanje računalnim sigurnosnim incidentima	Komunikacija s nadležnim tijelima i timovima za odgovore na računalne sigurnosne incidente (CSIRT)		A.6 Organizacija informacijske sigurnosti 7.4 Komunikacije 7.5 Dokumentirane informacije	PM – Upravljanje programom informacijske sigurnosti IR - Odgovor na incidente SI - Zaštita integriteta sustava i informacija MP - Zaštita medija	Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji
Detekcija	Detekcija	Operater ili organizacija postavlja sustav detekcije sigurnosnih incidenata tipa "analitičke sonde za datoteke i protokole". Te sonde analiziraju tokove podataka koji prolaze kroz njih kako bi se potražili događaji koji bi mogli utjecati na sigurnost sustava	A.12 Upravljanje operacijama A.15 Upravljanje odnosima s dobavljačima 9.1 Nadzor, mjerenje, analiza i evaluacija	CA – Promjena, autorizacija i nadzor PM – Upravljanje programom informacijske sigurnosti CM – Upravljanje konfiguracijom RA - Procjena rizika SA – Nabava sustava i usluga SR- Upravljanje dobavnim lancem	Komponente softverski definiranih mreža zadužene za automatizaciju upravljanja mrežom i uvid u stanje mreže i svih komponenti koje su spojene na istu
Upravljanje računalnim sigurnosnim incidentima	Odgovor na incidente sigurnosti informacijskog sustava	Operater ili organizacija izrađuje, ažurira i provodi proceduru za rukovanje, odgovor i analizu incidenata koji utječu na funkcioniranje ili sigurnost sustava, u skladu s definiranim sigurnosnim politikama za svoj informacijski sustav (ISSP)	A.16 Upravljanje sigurnosnim incidentom	IR – Odgovor na incidente AU – Revizija i odgovornost	Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji

Tablica 5 *Minimalni skup sigurnosnih mjera prema NIS Direktivi* [5] *i način implementacije u opisanom modelu za domenu Upravljanje i ekosustav*

Pod domena	**Sigurnosna mjera**	**Opis**	**Mapiranje sa ISO 27001:2013 kontrolnim mjerama / zahtjevima**	**Mapiranje s NIST SP800-53 Rev5 CSF kategorijama kontrolnih mjera**	**Način implementacije**
Upravljanje sigurnošću informacijskog sustava i upravljanje rizicima	Sigurnost ljudskih resursa	Uspostavljene sigurnosne politike informacijskog sustava postavljaju program podizanja svijesti o sigurnosti implementiranih kritičnih sustava za svo osoblje te program sigurnosne obuke zaposlenika kako bi ih se upoznalo s njihovim odgovornostima kao dio tog programa	A.6 Organizacija informacijske sigurnosti A.7 Sigurnost ljudskog potencijala A.9 Kontrole pristupa 4.1 Razumijevanje organizacije i njenog konteksta 4.2 Razumijevanje potreba i očekivanja zainteresiranih strana 5.3 Organizacijske uloge, odgovornosti i ovlasti 6.2 Ciljevi informacijske sigurnosti i planiranje za njihovo postizanje 7 Podrška 9.1 Nadzor, mjerenje, analiza i evaluacija	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor IA – Identifikacija i autentifikacija AC- Kontrola pristupa	Uspostavljen Program informacijske sigurnosti u organizaciji Edukacija korisnika organizacije

Upravljanje sigurnošću informacijskog sustava i upravljanje rizicima	Pokazatelji sigurnosti informacijskog sustava	Operater ili organizacija ocjenjuje svoju usklađenost s definiranim sigurnosnim politikama za svoj informacijski sustav (ISSP) za svaki implementirani kritični sustav prema nizu pokazatelja i metoda ocjenjivanja. Pokazatelji se mogu odnositi na izvedbu organizacije za upravljanje rizikom, održavanje resursa u sigurnim uvjetima, prava pristupa korisnika, provjeru autentičnosti pristupa resursima i administraciju resursa	A.12 Upravljanje operacijama 6.2 Ciljevi informacijske sigurnosti i planiranje za njihovo postizanje 7.1 Resursi 7.2 Kompetencije 9 Evaluacija performansi	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor	Uspostavljen Program informacijske sigurnosti u organizaciji Upravljanje sigurnosnim politikama temeljenim na identitetima u softverski definiranim mrežama
Upravljanje sigurnošću informacijskog sustava i upravljanje rizicima	Analiza rizika sigurnosti informacijskog sustava	Operater ili organizacija provodi i redovito ažurira analizu rizika, utvrđujući svoje kritične informacijske sustave koji podupiru pružanje osnovnih usluga i identificira glavne rizike za iste	A.8 Upravljanje imovinom A.12 Upravljanje operacijama A.18 Sukladnost 6 Planiranje 8 Operacije 9.3 Ocjena menadžmenta 10 Poboljšanja	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor RA - Procjena rizika CM - Upravljanje konfiguracijom SI - Zaštita integriteta sustava i informacija	Uspostavljen program Upravljanja rizicima (engl. Risk management, RM) u organizaciji

Upravljanje sigurnošću informacijskog sustava i upravljanje rizicima	Revizija sigurnosti informacijskog sustava	Operater ili organizacija uspostavlja i ažurira politiku i procedure za provođenje procjena sigurnosti informacijskog sustava i revizija kritične imovine i kritičnih informacijskih sustava, uzimajući u obzir redovito ažuriranu analizu rizika	A.5 Politika sigurnosti A.12 Upravljanje operacijama A.18 Sukladnost 6 Planiranje 8 Operacije 9.2 Interna revizija 9.3 Pregled uprave 10 Poboljšanja	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor RA - Procjena rizika SA - Nabava sustava i usluga AU- Revizija i odgovornost	Uspostavljen program Upravljanja rizicima (engl. Risk management, RM) u organizaciji
Upravljanje ekosustavom	Mapiranje ekosustava	Operater ili organizacija uspostavlja mapiranje svog ekosustava, uključujući unutarnje i vanjske dionike kao što su dobavljači, posebno one koji imaju pristup ili upravljaju kritičnom imovinom operatera	4.1 Razumijevanje organizacije i njenog konteksta 4.2 Razumijevanje potreba i očekivanja zainteresiranih strana 4.3 Određivanje opsega sustava upravljanja informacijskom sigurnošću 5.2 Politika 8.1 Operativno planiranje i kontrola	PM – Upravljanje programom informacijske sigurnosti CM – Upravljanje konfiguracijom SA – Nabava sustava i usluga PL- Planiranje	Uspostavljen Program informacijske sigurnosti u organizaciji Upravljanje konfiguracijom i sigurnosnim politikama sustava kroz centralne komponente softverski definiranih mreža

Upravljanje sigurnošću informacijskog sustava i upravljanje rizicima	Akreditacija sigurnosti informacijskog sustava	Na temelju analize rizika i u skladu s postupkom akreditacije definiranim u sigurnosnoj politici informacijskih sustava, operater ili organizacija akreditira identificirane kritične sustave u analizi rizika informacijskog sustava, uključujući, između ostalog, inventar i arhitekturu administrativnih komponenti tih sustava	A.12 Upravljanje operacijama 6.1 Aktivnosti za rješavanje rizika i prilika 8 Rad 9.2 Interna revizija 10.1 Nesukladnost i korektivne mjere	PM – Upravljanje programom informacijske sigurnosti CM- Upravljanje konfiguracijom SA – Nabava sustava i usluga PL - Planiranje RA - Procjena rizika	Uspostavljen Program informacijske sigurnosti u organizaciji Uspostavljen program Upravljanja rizicima (engl. Risk management, RM) u organizaciji

Upravljanje sigurnošću informacijskog sustava i upravljanje rizicima	Politika sigurnosti informacijskog sustava	Nadovezujući se na analizu rizika, operater ili organizacija uspostavlja, održava ažurnom i provodi politiku sigurnosti informacijskog sustava koju je odobrilo više rukovodstvo, jamčeći visoku razinu odobravanja politike	A.5 Politika sigurnosti A.6 Organizacija informacijske sigurnosti A.7 Sigurnost ljudskog potencijala A.18 Sukladnost 4.3 Određivanje opsega sustava upravljanja informacijskom sigurnošću 4.4 Sustav upravljanja informacijskom sigurnošću 5.1 Vodstvo i predanost 5.2 Politika 5.3 Organizacijske uloge, odgovornosti i ovlasti 6.2 Ciljevi informacijske sigurnosti i planiranje za njihovo postizanje 9.3 Pregled uprave	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor CM - Upravljanje konfiguracijom PS – Sigurnost osoblja SA – Nabava sustava i usluga	Uspostavljen Program informacijske sigurnosti u organizaciji Upravljanje konfiguracijom i sigurnosnim politikama sustava kroz centralne komponente softverski definiranih mreža

Upravljanje ekosustavom	Odnosi ekosustava	Operater ili organizacija uspostavlja politiku prema svojim odnosima sa svojim ekosustavom kako bi ublažio potencijalne identificirane rizike. Ovo posebno uključuje, ali nije ograničeno na sučelja između kritičnih sustava i trećih strana	A.5 Politika sigurnosti A.7 Sigurnost ljudskog potencijala A.12 Upravljanje operacijama A.13 Upravljanje komunikacijama A.14 Nabava, razvoj i održavanje informacijskih sustava A.15 Odnosi s dobavljačima A.18 Sukladnost 4.2 Razumijevanje potreba i očekivanja zainteresiranih strana 5.2 Politika 7.4 Komunikacija 7.5 Dokumentirane informacije 8.1 Operativno planiranje i kontrola 9.3 Pregled uprave	PM – Upravljanje programom informacijske sigurnosti CM - Upravljanje konfiguracijom PL- Planiranje SA – Nabava sustava i usluga CA – Promjena, autorizacija i nadzor PS – Sigurnost osoblja SR – Upravljanje dobavnim lancem	Uspostavljen Program informacijske sigurnosti u organizaciji Upravljanje konfiguracijom i sigurnosnim politikama sustava, za sve korisnike uključujući i treće strane, kroz centralne komponente softverski definiranih mreža

Tablica 6 *Minimalni skup sigurnosnih mjera prema NIS Direktivi* [5] *i način implementacije u opisanom modelu za domenu Zaštita*

Pod domena	**Sigurnosna mjera**	**Opis**	**Mapiranje sa ISO 27001:2013 kontrolnim mjerama / zahtjevima**	**Mapiranje s NIST SP800-53 Rev5 CSF kategorijama kontrolnih mjera**	**Način implementacije**
Upravljanje identitetom i pristupom	Autentifikacija i identifikacija	Za identifikaciju, operater ili organizacija postavlja jedinstvene račune za korisnike ili za automatizirane procese koji trebaju pristup resursima kritičnih sustava. Nekorišteni ili više nepotrebni računi moraju se deaktivirati. Treba uspostaviti redoviti proces pregleda	A.9 Kontrola pristupa	IA – Identifikacija i autentifikacija AC - Kontrola pristupa	Kontrola pristupa implementirana kroz sigurnosne politike temeljene na identitetima u softverski definiranim mrežama
Održavanje IT sigurnosti	Procedure za održavanje IT sigurnosti	Operater ili organizacija razvija i provodi postupak za održavanje sigurnosti u skladu sa definiranom sigurnosnom politikom informacijskog sustava. U tu svrhu, procedura definira uvjete koji omogućuju održavanje minimalne razine sigurnosti za resurse kritičnih sustava	A.11 Fizička sigurnost i sigurnost okruženja A.12 Upravljanje operacijama A.14 Nabava, razvoj i održavanje informacijskih sustava A.15 Odnosi s dobavljačima 7.5 Dokumentiranje informacije 8.1 Operativno planiranje i kontrola 10.1 Nesukladnost i korektivne mjere	CP – Planiranje kontinuiteta poslovanja IR – Odgovor na incidente PL - Planiranje PM - Upravljanje programom informacijske sigurnosti SA – Nabava sustava i usluga CM- Upravljanje konfiguracijom RA – Procjena rizika MA - Održavanje	Uspostavljen Program informacijske sigurnosti u organizaciji Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji Kontinuirano ažuriran i nadgledan treći podatkovni centar koji služi kao *DR* lokacija kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe uz popratni Plan organizacije za oporavka od katastrofe (engl. Disaster Recovery, DR)

				SR – Upravljanje dobavnim lancem	
Arhitektura IT sigurnosti	Odvajanje sustava	Operater ili organizacija odvaja svoje sustave kako bi ograničio širenje IT sigurnosnih incidenata unutar svojih sustava ili podsustava	A.12 Upravljanje operacijama A.13 Upravljanje komunikacijama	CM- Upravljanje konfiguracijom AC- Kontrola pristupa SC – Zaštita sustava i komunikacija SA – Nabava sustava i usluga	Segmentacija mreže i sigurnosne politike temeljene na identitetima u softverski definiranim mrežama

Arhitektura IT sigurnosti	Kriptografija	U svojoj sigurnosnoj politici informacijskih sustava, operater ili organizacija uspostavlja i provodi politiku i postupke koji se odnose na kriptografiju, s ciljem osiguranja odgovarajuće i učinkovite upotrebe kriptografije za zaštitu povjerljivosti, autentičnosti i/ili cjelovitosti informacija svojih kritičnih sustava	A.10 Kriptografija A.18 Sukladnost	SC – Zaštita sustava i komunikacija IA – Identifikacija i autentifikacija	Segmentacija mreže, sigurnosni tuneli i sigurnosne politike temeljene na identitetima u softverski definiranim mrežama

Održavanje IT sigurnosti	Sustavi industrijske kontrole		A.6 Organizacija informacijske sigurnosti A.8 Upravljanje imovinom A.9 Kontrola pristupa A.11 Fizička sigurnost i sigurnost okruženja A.12 Upravljanje operacijama A.14 Nabava, razvoj i održavanje informacijskih sustava A.15 Odnosi s dobavljačima A.17 Upravljanje kontinuitetom poslovanja 4 Kontekst organizacije 5.2 Politika 5.3 Organizacijske uloge, odgovornosti i ovlasti 7 Podrška 8 Operacije 9.1 Nadzor, mjerenje, analiza i evaluacija	PM - Upravljanje programom informacijske sigurnosti CM- Upravljanje konfiguracijom CP – Planiranje kontinuiteta poslovanja MP – Zaštita medija MA – Održavanje AC- Kontrola pristupa SC – Zaštita sustava i komunikacija SA – Nabava sustava i usluga SR – Upravljanje dobavnim lancem PE – Fizička zaštita i zaštita okoliša	Uspostavljen Program informacijske sigurnosti u organizaciji Upravljanje konfiguracijom i sigurnosnim politikama sustava, za sve korisnike uključujući i treće strane, kroz centralne komponente softverski definiranih mreža Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji

Administracija IT sigurnosti	Administrativni korisnički računi	Operater ili organizacija postavlja posebne račune za administraciju, koji će se koristiti samo za administratore koji provode administrativne operacije (instalacija, konfiguracija, upravljanje, održavanje itd.) na kritičnim sustavima. Ti se računi vode na ažurnom popisu.	A.9 Kontrola pristupa A.12 Upravljanje operacijama	AC- Kontrola pristupa CM – Upravljanje konfiguracijom AU - Revizija i odgovornost	Kontrola pristupa implementirana kroz sigurnosne politike temeljene na identitetima u softverski definiranim mrežama
Fizička i ekološka sigurnost	Fizička i ekološka sigurnost	Operater ili organizacija sprječava neovlašteni fizički pristup, štetu i potencijalno narušavanje sigurnosti podatkovnim centrima i informacijama u njima	A.8 Upravljanje imovinom A.11 Fizička sigurnost i sigurnost okruženja	CM – Upravljanje konfiguracijom PL - Planiranje PS - Sigurnost osoblja PE - Fizička zaštita i zaštita okoliša MA - Održavanje MP – Zaštita medija CP – Planiranje kontinuiteta poslovanja AC – Kontrola pristupa	Fizička sigurnost Upravljanje konfiguracijom i sigurnosnim politikama sustava, za sve korisnike uključujući i treće strane, kroz centralne komponente softverski definiranih mreža Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji

Upravljanje identitetom i pristupom	Prava pristupa	Među pravilima definiranim u sigurnosnoj politici informacijskih sustava, operater ili organizacija dodjeljuje prava pristupa korisniku ili automatiziranom procesu samo kada je taj pristup strogo neophodan da korisnik izvrši svoju misiju ili da automatizirani proces izvrši svoje tehničke operacije.	A.9 Kontrola pristupa	IA – Identifikacija i autentifikacija AC – Kontrola pristupa CM – Upravljanje konfiguracijom	Kontrola pristupa implementirana kroz sigurnosne politike temeljene na identitetima u softverski definiranim mrežama
Arhitektura IT sigurnosti	Filtriranje prometa	Operater ili organizacija filtrira tokove prometa koji kruže kritičnim informacijskim sustavima. Zabranjuju se prometni tokovi koji nisu potrebni za funkcioniranje sustava i koji bi mogli olakšati napad.	A.13 Upravljanje komunikacijama 8.1 Operativno planiranje i kontrola	CM – Upravljanje konfiguracijom AC – Kontrola pristupa SC – Zaštita sustava i komunikacija CA – Promjena, autorizacija i nadzor PL - Planiranje	Segmentacija mreže i sigurnosne politike temeljene na identitetima u softverski definiranim mrežama
Administracija IT sigurnosti	Administracija informacijskih sustava	Hardverskim i softverskim resursima koji se koriste u administrativne svrhe upravlja i konfigurira operater ili organizacija ili, prema potrebi, davatelj usluga kojeg je operater ili organizacija ovlastio za obavljanje administrativnih operacija.	A.9 Kontrola pristupa A.12 Upravljanje operacijama	IA – Identifikacija I autentifikacija AC – Kontrola pristupa CM – Upravljanje konfiguracijom AU – Revizija i odgovornost	Upravljanje konfiguracijom i sigurnosnim politikama sustava, za sve korisnike uključujući i treće strane, kroz centralne komponente softverski definiranih mreža

Arhitektura IT sigurnosti	Konfiguracija sustava	Operater ili organizacija samo instalira usluge i funkcionalnosti ili povezuje opremu koja je neophodna za funkcioniranje i sigurnost sustava	A.6 Organizacija informacijske sigurnosti A.8 Upravljanje imovinom A.12 Upravljanje operacijama A.13 Upravljanje komunikacijama A.14 Nabava, razvoj i održavanje informacijskih sustava 4.3 Određivanje opsega sustava upravljanja informacijskom sigurnošću	PM – Upravljanje programom informacijske sigurnosti AC – Kontrola pristupa MP – Zaštita medija CM – Upravljanje konfiguracijom CA – Promjena, autorizacija i nadzor SA – Nabava sustava i usluga SC – Zaštita sustava i komunikacija SI - Zaštita integriteta sustava i informacija	Uspostavljen Program informacijske sigurnosti u organizaciji Upravljanje imovinom, konfiguracijom i sigurnosnim politikama sustava, za sve korisnike uključujući i treće strane, kroz centralne komponente softverski definiranih mreža

***Tablica** 7 Minimalni skup sigurnosnih mjera prema NIS Direktivi* [5] *i način implementacije u opisanom modelu za domenu Otpornost*

Pod domena	**Sigurnosna mjera**	**Opis**	**Mapiranje sa ISO 27001:2013 kontrolnim mjerama / zahtjevima**	**Mapiranje s NIST SP800-53 Rev5 CSF kategorijama kontrolnih mjera**	**Način implementacije**
Kontinuitet poslovanja	Upravljanje oporavkom od katastrofe	U skladu sa sigurnosnom politikom informacijskih sustava, operater ili organizacija definira ciljeve i strateške smjernice u vezi s upravljanjem oporavkom od katastrofe, u slučaju ozbiljnog IT sigurnosnog incidenta.	A.17 Upravljanje kontinuitetom poslovanja	CP – Planiranje kontinuiteta poslovanja	Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji Kontinuirano ažuriran i nadgledan treći podatkovni centar koji služi kao *DR* lokacija kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe uz popratni Plan organizacije za oporavka od katastrofe (engl. Disaster Recovery, DR)

Upravljanje krizama	Organizacija upravljanja krizama	U sigurnosnoj politici informacijskih sustava operater ili organizacija definira organizaciju za upravljanje krizama u slučaju IT sigurnosnih incidenata i kontinuitet aktivnosti organizacije.	A.6 Organizacija informacijske sigurnosti A.11 Fizička sigurnost i sigurnost okruženja A.17 Upravljanje kontinuitetom poslovanja 5.3 Organizacijske uloge, odgovornosti i ovlasti	PM – Upravljanje programom informacijske sigurnosti CP – Planiranje kontinuiteta poslovanja PS - Sigurnost osoblja MA - Održavanje SA - Nabava sustava i usluga	Uspostavljen Program informacijske sigurnosti u organizaciji Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji Kontinuirano ažuriran i nadgledan treći podatkovni centar koji služi kao *DR* lokacija kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe uz popratni Plan organizacije za oporavka od katastrofe (engl. Disaster Recovery, DR) Fizička sigurnost

Kontinuitet poslovanja	Upravljanje kontinuitetom poslovanja	U skladu sa sigurnosnom politikom informacijskih sustava, operator ili organizacija definira ciljeve i strateške smjernice u pogledu upravljanja kontinuitetom poslovanja, u slučaju IT sigurnosnog incidenta.	A.5 Politika sigurnosti A.11 Fizička sigurnost i sigurnost okruženja A.17 Upravljanje kontinuitetom poslovanja 9.3 Pregled uprave 10.2 Stalno poboljšanje	PM – Upravljanje programom informacijske sigurnosti CP – Planiranje kontinuiteta poslovanja MA - Održavanje CA – Promjena, autorizacija i nadzor	Uspostavljen Program informacijske sigurnosti u organizaciji Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji Kontinuirano ažuriran i nadgledan treći podatkovni centar koji služi kao *DR* lokacija kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe uz popratni Plan organizacije za oporavka od katastrofe (engl. Disaster Recovery, DR) Fizička sigurnost Sigurnosne politike temeljene na identitetima u softverski definiranim mrežama

Upravljanje krizama	Proces upravljanja krizom	U sigurnosnoj politici informacijskih sustava operater ili organizacija definira procese za upravljanje kriznim situacijama koje će organizacija za upravljanje kriznim situacijama implementirati u slučaju IT sigurnosnih incidenata i kontinuiteta aktivnosti organizacije.	A.5 Politika sigurnosti A.6 Organizacija informacijske sigurnosti A.11 Fizička sigurnost i sigurnost okruženja A.17 Upravljanje kontinuitetom poslovanja 7.4 Komunikacija 9.3 Pregled uprave	PM – Upravljanje programom informacijske sigurnosti CA – Promjena, autorizacija i nadzor CP – Planiranje kontinuiteta poslovanja MA - Održavanje IR – Odgovor na incident	Uspostavljen Program informacijske sigurnosti u organizaciji Uspostavljeni i redovito ažurirani Planovi kontinuiteta poslovanja (engl. Business Continuity Plans, BCP) u organizaciji Kontinuirano ažuriran i nadgledan treći podatkovni centar koji služi kao *DR* lokacija kako bi se osigurao kontinuitet poslovanja u slučaju bilo kakve katastrofe uz popratni Plan organizacije za oporavka od katastrofe (engl. Disaster Recovery, DR) Uspostavljen program Upravljanja sigurnosnim incidentima (engl. Information security incident management) u organizaciji Sigurnosne politike temeljene na identitetima u softverski definiranim mrežama

4 Koncepti i implementacija arhitekture nultog povjerenja

Jedan od implementiranih sigurnosnih mehanizama u opisanom modelu višeoblačnog sustava je arhitektura nultog povjerenja kroz softverski definiranu mrežu (engl. Software Defined Network, SDN). U nastavku su predstavljeni osnovni koncepti tog modela, te implementacija takve arhitekture i njenih gradivnih elemenata.

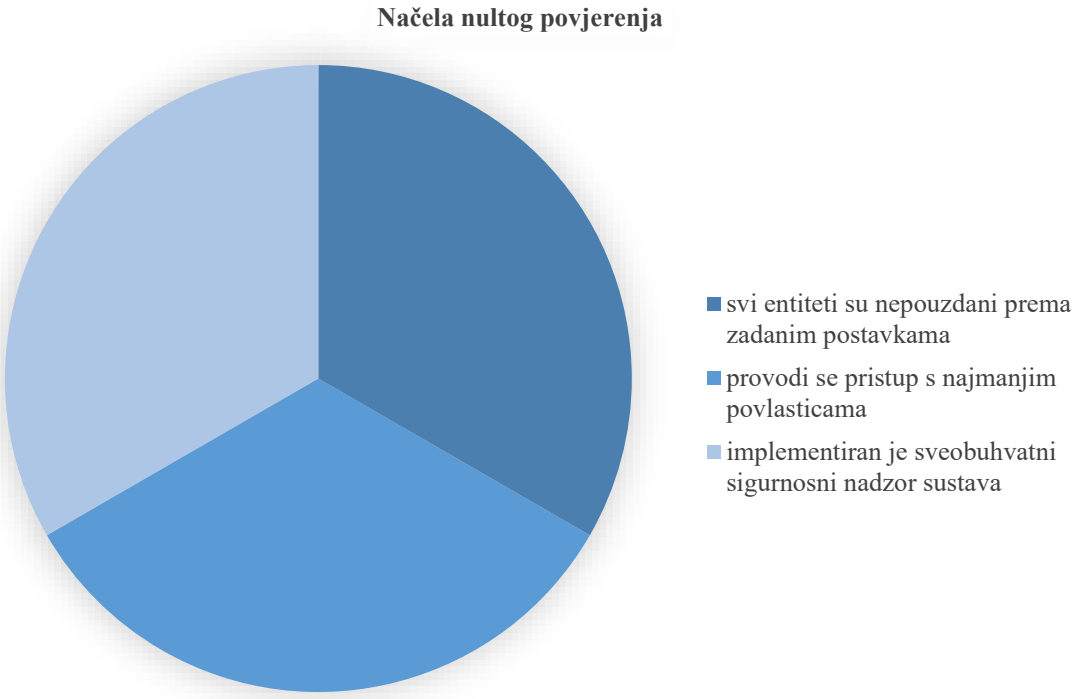
Model sigurnosti nultog povjerenja značajno je odstupanje od tradicionalne mrežne sigurnosti koja je slijedila metodu "vjeruj, ali provjeri". Tradicionalni pristup automatski je vjerovao korisnicima i krajnjim točkama unutar perimetra organizacije, a štitio se vanjski perimetar. Na taj način se vatrozidima provjeravao pristup resursima organizacije izvana i promet koji dolazi s Interneta te blokiralo sve sumnjivo, a unutarnje okruženje organizacije je i dalje bilo izloženo riziku od zlonamjernih ili kompromitiranih internih aktera koji su imali pristup resursima organizacije. Migracijom dijela ili cijelog poslovanja u oblak te povećanim trendom rada na daljinu, tradicionalni pristup mrežne sigurnosti više nije primjenjiv. Spektar krajnjih točaka se širi, od mobitela, tableta i privatnih računala koja se spajaju na mreže organizacije ili organizacijske resurse smještene u oblacima gdje razmjena informacija nije uvijek obavljena na pouzdan način. Model nultog povjerenja donosi drukčiji pristup sigurnosti koji se bazira na nepovjerenju prema svima i svemu, unutar i izvan perimetra organizacije, te zagovara kontinuiranu reevaluaciju korisnika i krajnjih točaka.

Za razliku od tradicionalne mrežne sigurnosti, arhitektura nultog povjerenja zahtijeva da svi korisnici, bilo unutar ili izvan mreže organizacije, budu autentificirani, autorizirani i da im se kontinuirano provjerava sigurnosni položaj prije nego im se odobri pristup zahtijevanim resursima. Jednokratna provjera nije dovoljna jer može doći do promjene u sigurnosnom položaju pojedinog subjekta koji može dovesti do potencijalne prijetnje sustavu. Zbog toga sustav mora osigurati autentičnost subjekta i valjanost zahtjeva u svakom trenutku.

Prema Forrester istraživanju [6], model sigurnosti nultog povjerenja se bazira na zadanim postavkama zabrane pristupa resursima. Kako prikazuje *Slika 3,* taj model zagovara tri osnovna načela:

- prema zadanim postavkama svi entiteti su nepouzdani – prava pristupa pojedinim entitetima se dodjeljuju sukladno definiranim poslovnim potrebama,

- postaviti pristup s najmanjim povlasticama – svakom entitetu dodijeljena su minimalna prava nužna za obavljanje poslovnih funkcija,
- implementiran je sveobuhvatan sigurnosni nadzor – sve radnje na sustavu se bilježe te za svako uočeno odstupanje treba provjeriti i odraditi potrebne akcije kako bi se spriječili ili ublažile prijetnje.

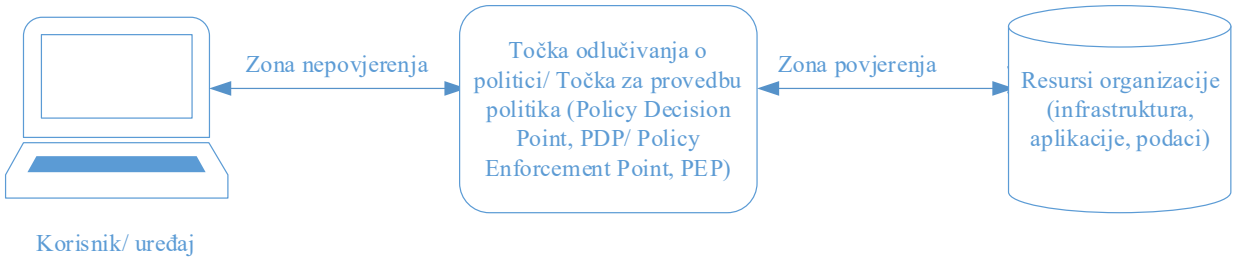


Slika 3 *Osnovna načela nultog povjerenja prema Forrester istraživanju* [7]

NIST publikacija, *NIST SP 800-207 Zero Trust Architecture* [8], formalizirala je arhitekturu nultog povjerenja koju je kao takvu predstavio i popularizirao istraživač John Kindervag u Forrester istraživanju iz 2010 [6], definira nulto povjerenje kao skup koncepata i ideja osmišljenih da se uspostave detaljno definirane kontrole ili politike pristupa koja onemogućuju neovlašten pristup bilo kojem resursu, od uređaja pa do usluga i podataka. Apstraktni model nultog povjerenja i osnovna načela nultog povjerenja, opisan u NIST publikaciji [8] su tehnološki agnostička te služe kao smjernice pri implementaciji tog modela u praksi. Rješenja raznih proizvođača se oslanjaju na isti model kako bi osigurali da ponuđena rješenja pružaju sve nužne komponente koje bi omogućile implementaciju modela nultog povjerenja.

Slika 4 prikazuje apstraktni model [8] temeljen na činjenici da subjekt, koji se smatra nepouzdanim, traži pristup resursu organizacije. Subjekt šalje zahtjev za pristup točci odlučivanja o politici (engl. Policy Decision Point, PDP), koja verificira zahtjev te odobrava ili

zabranjuje pristup, čiju odluku dalje provodi odgovarajuća točka za provedbu politike (engl. Policy Enforcement Point, PEP). Komponente prikazanog modela, točke odlučivanja o politici i provedbe politike, su granica između *zone nepovjerenja*, u kojoj se svi entiteti smatraju nepouzdanima i njihov sigurnosni položaj treba provjeriti prije nego im se odobri pristup resursima organizacije, i *implicitne zone povjerenja*, u kojoj je entitetu odobren pristup kroz PEP točku nakon što je uspješno autentificiran i autoriziran od strane PDP točke. Ovaj model zagovara smještaj PDP/PEP točke što bliže resursima kojima subjekt pristupa, kako bi implicitna zona povjerenja bila što manja i na taj način što lakše ju se kontroliralo.



Slika 4 *Apstraktni model nultog povjerenja* [8]

Glavna načela modela nultog povjerenja prema NIST publikaciji [8] su:

- resursima se smatraju svi podaci, usluge, softver i hardver koji je u vlasništvu organizacije ili ima pristup resursima koji su u vlasništvu organizacije,

- sva komunikacija prema resursima organizacije mora biti zaštićena bez obzira je li se radi o zahtjevu entiteta koji je unutar ili izvan mreže organizacije,

- svaki zahtjev entiteta prema resursu organizacije, za svaku uspostavljenu sesiju, se mora posebno odobriti s najmanjim potrebnim privilegijama,

- zahtjev za pristup pojedinim resursima se odobrava dinamičkim politikama na temelju provjere sigurnosnog položaja subjekta, koji osim korisničkog računa mogu uključivati i vrijeme i datum zahtjeva, mrežnu lokaciju s koje je zahtjev upućen, uređaj s kojeg je zahtjev upućen uključujući instalirane verzije softvera i dodatnih instaliranih vjerodajnica, te dodatne automatizirane analitike subjekta i pristupnog uređaja kako bi se provjerilo je li postoje kakva odstupanja od uobičajenih obrazaca korištenja,

- organizacija bi trebala stalno nadzirati svu svoju imovinu i njen sigurnosni položaj te primjenjivati potrebne zakrpe u slučaju uočenog narušenog sigurnosnog položaja,

- organizacija bi trebala imati implementiran sustav za kontinuirani nadzor svih komunikacija, koji nudi i mogućnost provjere sigurnosnog položaja subjekta kroz korisničke transakcije te ako se ustanovi da je potrebno pokrenuti ponovni proces autentifikacije i autorizacije,

- organizacija bi sve prikupljene podatke o imovini, zahtjevima za pristupom i prometu trebala obraditi i iskoristiti za unapređenje implementiranih politika pristupa.

Na temelju gornjih načela, proizvođači mrežne opreme osmislili su sigurnosna rješenja za mrežu nultog povjerenja koja definiraju kao rješenja za softverski definirane mreže. Tri su osnovna podskupa takve mreže,

- Softverski definirani pristup mreži,
- Softverski definirana mreža širokog pristupa,
- Softverski definirani podatkovni centar.

Ovisno od proizvođača do proizvođača, svaki podskup je implementiran kao jedinstveno rješenje ili u nekim slučajevima su dva ili sva tri podskupa implementirana kao dio jednog rješenja. Više o svakom podskupu implementiranom u prikazanom modelu u narednim poglavljima.

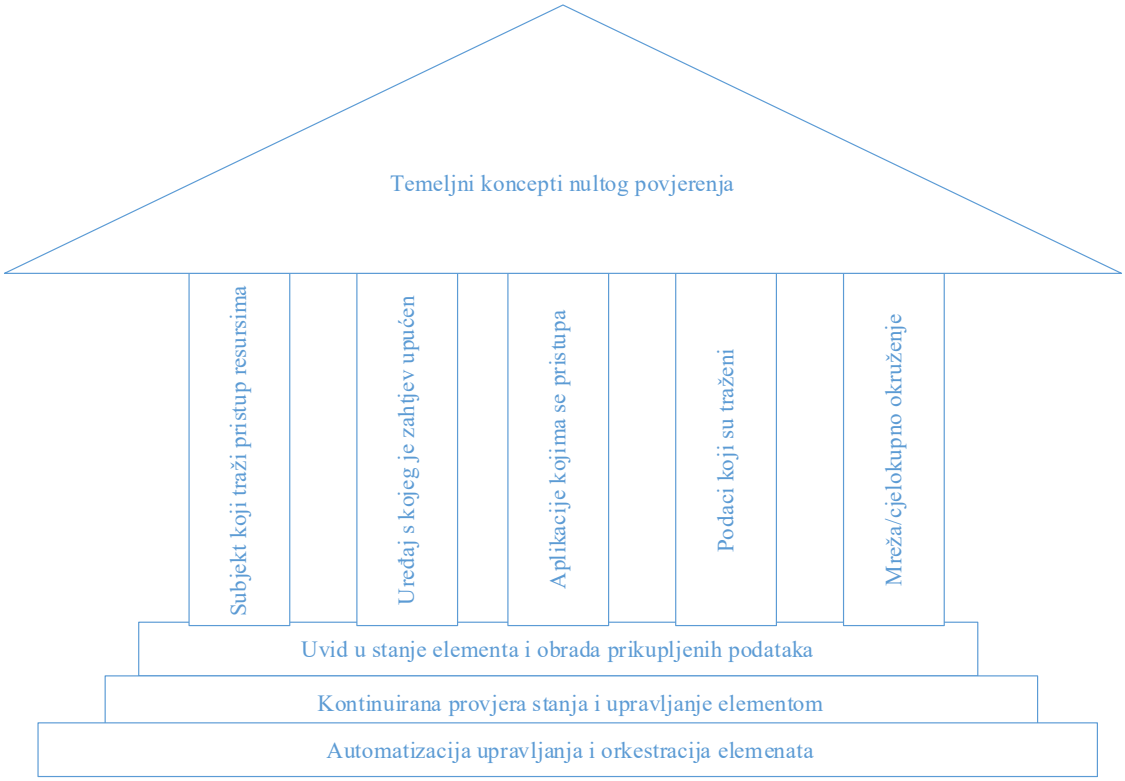
Kako prikazuje *Slika 5*, subjekt koji traži pristup resursima, uređaj s kojeg je zahtjev upućen, aplikacije kojima se pristupa, podaci koji su traženi te mreža i cjelokupno okruženje koje povezuje prethodno navedeno tvore temeljne stupove nultog povjerenja. Na tim stupovima počivaju temeljni koncepti nultog povjerenja:

- uvid u stanje prikazanih stupova koji sudjeluju u izgradnji konteksta odnosno sigurnosnog položaja, te obrada prikupljenih podataka kako bi se uspostavilo povjerenje potrebno za pristup resursima,
- automatizacija upravljanja i orkestracija prikazanim stupovima,
- mehanizmi kontinuirane provjere stanja i mogućnosti upravljanja stupovima.

Implementacija tih koncepata je ostvarena kroz:

- automatizaciju upravljanja mrežom i uvid u stanje mreže i svih komponenti koje su spojene na istu,

- segmentaciju mreže kako bi se smanjila potencijalna površina napada,
- sigurnosne politike temeljene na identitetima i dostupnim atributima vezanima uz identitet.



Slika 5 *Temeljni koncepti modela nultog povjerenja* [9]

4.1 Sigurnosne politike temeljene na identitetima

Promjenom paradigme mrežne sigurnosti dolazi i do promjene u načinu implementacije. Sigurnosne politike se više ne temelje na IP adresama nego na identitetima i dodatnim atributima, npr. uređaj s kojeg je poslan zahtjev za pristup, mrežna lokacija tog uređaja, koji svi zajedno tvore kontekst odnosno dio su sigurnosnog položaja pojedinog entiteta. Pri obradi zahtjeva za pristup u obzir se uzima cijeli kontekst te se dodjeljuju samo nužna prava pristupa. Iz toga razloga je bitno automatizirati prikupljanje podataka koji čine kontekst kako bi konačna odluka o autorizaciji pristupa bila što točnija. Pri tome je potrebno uključiti podatke o ponašanju iz cijelog ekosustava koji su dostupni za obradu u stvarnom vremenu, kao što su: korisničke vjerodajnice, radna opterećenja uređaja, status mreže, status krajnje točke, informacije dostupne u alatima za mrežni i sigurnosni nadzor, informacije koje pruža davatelj identiteta, obavještajni podaci o prijetnjama i slično.

Ovakav pristup omogućava definiranje sigurnosne politike za pojedinog korisnika koja uvijek vrijedi za tog korisnika bez obzira na mjesto i način spajanja. Takav pristup utječe i na bolje

iskustvo krajnjeg korisnika, a s druge strane pojednostavljuje se i dodavanje novih korisnika i uređaja na mrežu prilikom proširenja organizacije. Mrežni uređaji nisu unaprijed konfigurirani po pristupnim sučeljima već se konfiguracija određuje na temelju uspješne autentifikacije i autorizacije, odnosno nakon određivanja identiteta i konteksta za svakog korisnika/uređaj.

4.2 Segmentacija mreže

Koncept segmentacije mreže znači postavljanje pojedinačnih ili grupa resursa na jedinstveni mrežni segment koji je zaštićen od ostalih mrežnih segmenata. Prednosti segmentacije po pitanju sigurnosti su višestruke:

- mrežni problem na pojedinom segmentu ne širi se na ostale mrežne segmente odnosno smanjuje se utjecaj ako dođe do vanjskog ili unutarnjeg sigurnosnog proboja,
- smanjuje se razina pristupa osjetljivim informacijama, čime se i napadaču otežava lociranje i pristup osjetljivim informacijama,
- kontroliranje pristupa posjetitelja,
- povećanje performansi.

Neka rješenja nude samo model mikrosegmentacije, segmentacija temeljena na identitetu, dok neka nude i model makrosegmentacije, segmentacija temeljena na mrežnom segmentu. Pozivajući se na model dan u NIST publikaciji [8], mikrosegmentacija se u načelu temelji na stalnoj zaštiti svakog resursa. Takva zaštita se postiže kroz PEP točke koje obrađuju svaki pojedinačni zahtjev za pristup resursima organizacije. Uobičajeno se kao PEP točke koriste:

- inteligentni preklopnici ili usmjernici, koji imaju mogućnost upravljanja i konfiguriranja naprednijih mrežnih i sigurnosnih funkcija, npr. odvajanje prometa u zasebne podmreže, te nadzor samog uređaja i prometa koji ide kroz njega,
- noviji vatrozidi (engl. Next-Generation Firewall, NGFW) koji pored standardnih funkcija podržavaju i napredne funkcije kao dubinska provjera na razini paketa (engl. deep packet inspection), otkrivanje i prevencije upada (engl. intrusion prevention), osnovne funkcije vatrozida web aplikacija,
- softverski agenti na krajnjim točkama.

Uređajima u svojstvu PEP točke je potrebno upravljati kako bi bili u stanju reagirati i odgovoriti na uočene prijetnje ili promjene u radu. PEP točke se za obradu zahtjeva oslanjanju na PDP točke koje su zapravo komponente za upravljanje identitetom (engl. identity governance program, IGP) i koje štite resurse od neovlaštenog pristupa. U opisanom modelu koristi se i mikrosegmentacija i makrosegmentacija.

Preporuka je segmentirati mreže u što manje segmente, gdje je moguće primijeniti dodatne sigurnosne kontrole, što specifičnije ograničiti pristup te pomno pratiti mrežni promet na temelju osjetljivosti sustava i podataka unutar takvog manjeg segmenta. Ovakvim pristup se napadačima smanjuje pristup u slučaju proboja tradicionalnog perimetra.

4.3 Automatizacija i uvid u stanje mreže

Kako bi kontinuirana provjera povjerenja bila moguća, potrebno je cijelo vrijeme imati uvid u stanje mreže, krajnje točke i korisnike spojene na mrežu, sa svim njihovim atributima koji tvore kontekst, i na temelju svih prikupljenih informacija donositi odluke o pristupu pojedinim resursima. U slučaju da se utvrdi da stanje pristupnog uređaja ili aplikacije nije zadovoljavajuće, npr. zbog nedostatka zakrpa za poznate ranjivosti, automatski bi se trebala primijeniti odgovarajuća zakrpa. Automatizacija provjere usklađenosti i primjene odgovarajućih mjera uz kontinuirani uvid u stanje mreže i resursa spojenih na istu su dio rješenja za softverski definirani pristup mreži.

Kontinuirana provjera povjerenja znači da je cijelo vrijeme i za sve resurse potrebno provjeravati povjerenje na temelju kojega se dozvoljava ili brani pristup određenom resursu.

4.4 Implementacija arhitekture nultog povjerenja u višeoblačnom sustavu

Implementirano rješenje, u skladu sa svim načelima nultog povjerenja i bazirano na tehnologiji softverski definiranih mreža, sadrži slijedeće elemente:

- napredno upravljanje identitetom i kontrolama pristupa temeljenih na pravilima,
- korištenje mikrosegmentacije,
- korištenje prekrivajućih mreža (overlay *network*), odnosno logičkih mreža izgrađenih na fizičkim mrežama podlogama (*underlay network*), i softverski definiranih perimetara.

Navedeni elementi kombiniraju više naprednih tehnologija kao što su više faktorska provjera autentičnosti, provjera i zaštita identiteta subjekta, odluka o odobrenju pojedinog zahtjeva za pristup određenom resursu na temelju sigurnosnog položaja subjekta i cjelokupnog sustava u tom trenutku. Kroz dodatne mehanizme zaštite na aplikativnom nivou, vodi se briga i o zaštiti podataka koji se razmjenjuju, zaštiti elektroničke pošte te zaštiti svih resursa bez obzira na njihov smještaj.

Osnovni koncept SDN arhitekture je odvajanje funkcije prosljeđivanja mrežnih paketa, podatkovna ravnina, od razine mrežne kontrole i upravljanja, kontrolna ravnina koja se smatra mozgom SDN mreže. Takav koncept omogućuje veću automatizaciju mreže, pojednostavljuje operativni rad, daje bolji nadzor mreže te omogućava brže rješavanje problema. Osnovne komponente SDN arhitekture su:

- SDN aplikacijski sloj – sloj aplikacije putem kojeg korisnik upravlja mrežom i dobiva uvid u stanje mreže. Ovaj sloj putem sučelja koje se uobičajeno naziva *northbound* sučelje*, (engl. Northbound Interface, NBI*) ostvaruje komunikaciju prema SDN kontroleru,

- SDN *northbound* sučelje (*SDN NBI*) – sučelje koje omogućuje komunikaciju zahtjeva i apstraktnih mrežnih prikaza između SDN aplikacijskog sloja i SDN kontrolera. SDN NBI sučelja bi trebala biti pisana na način da su neovisna o proizvođaču i pružati mogućnosti integracije s rješenjima drugih proizvođača,

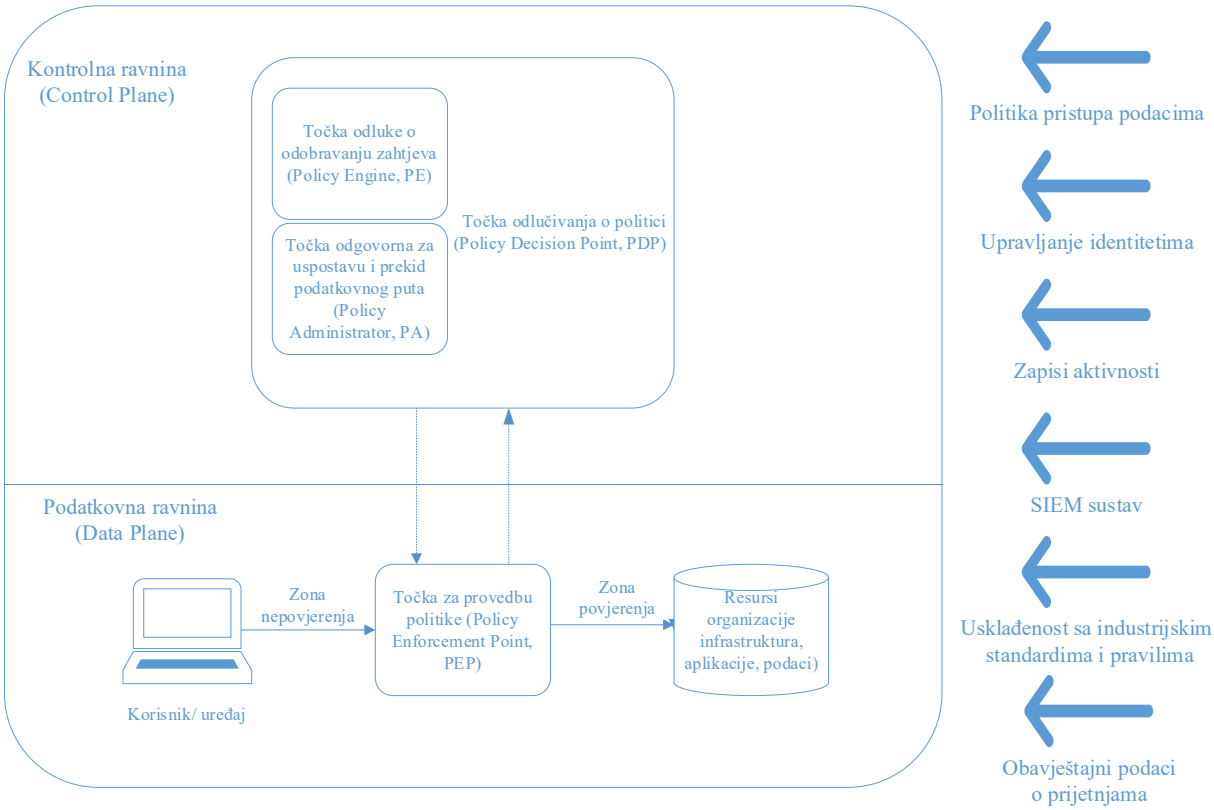
- SDN kontroler – centralna komponenta koja je zadužena za prevođenje zahtjeva SDN aplikacijskog sloja na SDN sloj podatkovnog puta i za pružanje apstraktnog prikaza mreže SDN aplikacijskom sloju. Sastoji se od jednog ili više NBI sučelja, upravljačke logike i kontrolnog sučelja prema podatkovnoj ravnini,

- SDN kontrolno sučelje prema podatkovnoj ravnini – sučelje koje omogućuje komunikaciju zahtjeva, oglašavanje mogućnosti mrežnih uređaja, izvještavanje o statistikama i događajima između kontrolera i sloja podatkovnog puta. Ova sučelja bi također trebala biti pisana na način da su neovisna o proizvođaču i pružati mogućnosti integracije s rješenjima drugih proizvođača,

- SDN sloj podatkovnog puta - mrežni uređaji kojima se upravlja te koji oglašavaju svoje mogućnosti, statistike i događaje višim slojevima putem SDN kontrolnog sučelja. Imaju ugrađene mehanizme za obradu i prosljeđivanje prometa.

Prema apstraktnom modelu [8], rješenja za implementaciju nultog povjerenja se temelje na prethodno opisanoj SDN arhitekturi odvajanja kontrolne i podatkovne ravnine, kako prikazuje *Slika 6.* PDP točka je dio kontrolne ravnine koja ima dvije sastavnice, jednu odgovornu za konačnu odluku o odobravanju zahtjeva subjekta za pristup određenom resursu (engl. Policy

Engine, PE), i drugu odgovornu za uspostavu i prekid podatkovnog puta između subjekta i resursa (engl. Policy Administrator, PA). PA sastavnica komunicira odluke PE sastavnice prema PEP točci, koja je dio podatkovne ravnine, te je odgovorna za izvršavanje naredbi koje dobije od PA sastavnice.



Slika 6 *Osnovne logičke komponente arhitekture nultog povjerenja* [8]

Slijedeći koncepte SDN arhitekture i zahtijevanih komponenti, proizvođači su rješenja podijelili u tri osnovne skupine, ovisno koji dio mreže pokrivaju:

- lokalna mreža - softverski definirana pristupna mreža
    - proizvođači ovaj segment nazivaju *Software Defined Access - SDA, Zero Trust Network Access - ZTNA* ili *Software Defined Local Area Network - SD LAN*,
- širokopojasna mreža - softverski definirana širokopojasna mreža
    - proizvođači ovaj segment mreža nazivaju i *Software Defined Wide Area Network - SD WAN*,
- mreža u podatkovnom centru - softverski definirana mreža podatkovnog centra
    - proizvođači ovaj segment nazivaju *Software Defined Data Center - SDDC*, koji osim mrežnih i sigurnosnih funkcija obuhvaća i ostale komponente infrastrukture podatkovnog centra kao što su sustavi za pohranu podataka,

procesorske, memorijske, diskovne jedinice. Ovaj rad se bavi mrežnim i sigurnosnim funkcijama SDDC rješenja.

Rješenja se temelje na mreži podlozi, koja služi za fizičko povezivanje komponenti, te prekrivajućoj mreži kojom se ostvaruje logička povezanost na implementiranim načelima nultog povjerenja. U nastavku više o implementaciji prekrivajuće mreže za gore navedene skupine.

4.5 Softverski definirana pristupna mreža

Softverski definirana pristupna mreža izgrađena je na načelima softverski definiranih mreža odvajanjem kontrolne i podatkovne razine koja omogućuju istovjetne politike za žične i bežične lokalne mreže. Dodatno načelo je sigurnost kao integralni dio rješenja što dovodi do interoperabilnosti sigurnosnih i mrežnih rješenja. Rješenja se baziraju na načelu da postoji nadzor svih korisnika i uređaja na mreži te njihovih aktivnosti. Centralna komponenta za upravljanje i nadzor mrežnih uređaja prvo otkriva i identificira sve spojene uređaje. Na temelju tih podataka se gradi baza podataka kontrolne razine. Ta baza podataka je ažurna tablica svih krajnjih uređaja u danom trenutku, s preklopnicima ili bežičnim pristupnim točkama na koje su ti uređaji povezani, koja omogućuje uspostavu komunikacije između krajnjih uređaja. Stjecanje uvida o spojenim korisnicima i uređajima potrebno je kako bi se uspostavila odgovarajuća kontrola pristupa. Cijeli proces započinje sa subjektom, koji preko krajnjeg uređaja, spojenog na pristupni preklopnik ili bežičnu pristupnu točku, želi pristupiti određenom resursu. Subjekt šalje zahtjev za pristupom, odnosno zahtjev za autentifikacijom i autorizacijom centralnoj točki za sigurnosne politike koja prvo provjerava identitet subjekta kao ključan korak u identifikaciji subjekta. Za konačnu odluku se osim provjere politika i kontrola pristupa, radi i provjera sigurnosnog položaja krajnje uređaja i subjekta. Nakon odobrenja ili odbijanja zahtjeva, centralna točka za sigurnosne politike odluku komunicira krajnjem uređaju i centralnoj točki za upravljanje i nadzor mrežnim uređajima. Centralna točka za upravljanje i nadzor mrežnim uređajima shodno odluci konfigurira sučelje pristupnog preklopnika kako bi krajnji uređaj dobio pristup odobrenim resursima, odnosno mogućnost za uspostavu sesije. Dodatno se za uspostavu i tijek odobrene sesije između krajnjeg uređaja i traženih resursa dodjeljuju jedinstveni mrežni atributi preko kojih se uspostavlja podatkovni put te putem kojih se odvija kontinuirana provjera povjerenja. Ovakav način segmentacije naziva se segmentacija bazirana na identitetu korisnika ili mikrosegmentacija. Jednom odobren pristup se kontinuirano evaluira na način da se kontinuirano nadgledaju i provjeravaju svi uređaji i aktivnosti korisnika. Kako

bi krajnji uređaj mogao uopće pristupiti centralnoj točci za sigurnosne politike, potrebno je postaviti podrazumijevanu L3 točku na pristupnom preklopniku ili bežičnoj pristupnoj točci. Shodno najboljim praksama u opisanom modelu implementirana je i makrosegmentacije odnosno centralni mrežni i poslovni servisi odvojeni su u različite segmente od segmenata krajnjih uređaja. U predstavljenom modelu centralna točka za upravljanje i nadzor mrežnim uređajima i centralna točka za sigurnosne politike su zasebne komponente koje su integrirane kako bi omogućile da iste politike i kontrole pristupa vrijede neovisno o mjestu i načinu spajanja krajnjeg korisnika. Ovakvim pristupom dobiva se tranzicija s prikaza korisnika baziranog na IP adresi na prikaz korisnika baziran na korisnikovim identitetu.

4.6 Softverski definirana širokopojasna mreža

Namjena softverski definirane širokopojasne mreže je logičko povezivanje udaljenih lokacija neovisno o ostvarenom fizičkom načinu povezivanja istih. Takvom mrežom se upravlja uz pomoć središnjih kontrolera preko kojih se vrši kontrola i upravljanje mrežom. Za razliku od softverski definirane pristupne mreže, osim kontrolne i podatkovne razine, postoji i dodatna razina upravljanja i orkestracije kao centralno mjesto svih kontrolera te orkestracije cjelokupnog rješenja.

Implementirano rješenje se bazira na preklopnoj mreži između kontrolera i usmjernika koji se nalaze na rubovima pristupnih mreža svake udaljene lokacije. Kontroleri uspostavljaju IPSec tunele između udaljenih lokacija. Svaki usmjernik, preko uspostavljenog sigurnog tunela, oglašava svoje mreže, sljedeći skok, sigurnosne ključeve i informacije o politikama. Dodatno oglašava i atribute o mogućnostima prijenosa svoje lokacije. U tablicu preklapanja se instaliraju samo informacije o aktivnim točkama u mreži, te služe za odluke kontrolne ravnine na razini mreže preklapanja. Uspostavljenim sigurnim tunelima prenose se i atributi definirani makrosegentacijom i mikrosegmentacijom u softverski definiranoj pristupnoj mreži udaljene lokacije. Za svaki zahtjev subjekta za pristup resursima, nakon uspješne autentifikacije i autorizacije, uspostavlja se dinamički sigurni tunel za tu komunikaciju i ne koristi se za vezu između subjekta i drugih resursa. Za vezu prema drugom resursu šalje se novi zahtjev za pristupom, radi se nova provjera subjekta i sigurnosnog položaja prije uspostave novog sigurnog tunela. To predstavlja razliku od tradicionalnog pristupa gdje je jedan subjekt koristio jedan tunel prema udaljenoj lokaciji za komunikaciju prema svim resursima koji se nalaze na toj lokaciji.

Drugo bitno načelo rješenja je prioritiziranje i usmjeravanje prometa s obzirom na predefinirane mrežne parametre po pojedinoj aplikaciji. Rješenje na temelju uvida u stanje mreže i analize mrežnog prometa, dobiva uvid u aplikacije odnosno otkriva položaj pojedinih aplikacija. Na temelju te informacije, omogućava se prioritizacija i odabir najbolje veze, te nije nužno usmjeravati sav promet prema centralnoj lokaciji ako se aplikacija nalazi u oblaku. U svrhu određivanja najboljeg puta, odnosno performansi pojedinih linkova, koriste se *Bidirectional Forwarding Detection (BFD*) sonde koje daju informacije o kašnjenju, varijaciji kašnjenja i gubitku paketa na pojedinom linku. Kako bi se osigurala što veća pouzdanost rješenja, koriste se i mehanizmi za ublažavanje posljedice gubitaka podataka na linkovima, što je od posebnog značaja za poslovno kritične aplikacije. U tu svrhu se koriste *Forward Error Correction (FEC)* mehanizam i mehanizam slanja istih paketa po odvojenim linkovima, kako bi se u slučaju gubitka pojedinog paketa, paket na odredištu mogao nadomjestiti iz toka podataka s drugog linka. *FEC* mehanizam služi za oporavak do jednog izgubljenog paketa u grupi. Temelji se na načelu slanja dodatnog paketa pariteta za svaku grupu od N paketa te sve dok na odredište stigne podskup od N-1 paketa u grupi i paket pariteta, izgubljeni paket se može vratiti.

Baza i ovog rješenja je integracija sigurnosnih značajki u mrežne funkcionalnosti što omogućuje centraliziranu mrežnu zaštitu i dosljednu provedbu politika kroz cijelo okruženje.

4.7 Softverski definirani podatkovni centri

Softverski definirani podatkovni centri počivaju na načelima virtualnih mreža koje služe za povezivanje virtualiziranih aplikacija koje se nalaze na poslužiteljima unutar podatkovnih centara. U prikazanom modelu, poslužitelji se nalaze unutar više fizičkih podatkovnih centara, koji su djelomično udaljeni od krajnjih korisnika, čineći jedan logički podatkovni centar. Tako smještene aplikacije zahtijevaju pouzdanu dostavu repliciranih podataka, otpornost na pogreške, što manje kašnjenje u dostavi podataka i usluga krajnjim korisnicima te uravnoteženu raspodjelu opterećenja. Shodno tome rješenje se bazira na sigurnosti, automatizaciji i kontinuitetu aplikacija objedinjujući sigurnosne i mrežne funkcije. Implementirano rješenje osim funkcija usmjeravanja i prosljeđivanja paketa između komponenti podatkovnog centra i prema krajnjim korisnicima, obavlja i funkcije provjere sigurnosnog položaja, prioritizacije prometa, upravljanja opterećenjem i funkcije vatrozida unutar logičkog podatkovnog centra. U softverski definiranim podatkovnim centrima, sigurnosni položaj se može temeljiti na MAC adresama, IP adresama, portovima, objektima virtualnih mašina na kojima se nalaze aplikacije i atributima domenskih grupa.

Prema načelima softverski definiranih mreža, rješenje se sastoji od podatkovne, kontrolne i upravljačke ravnine, koje su implementirane kroz krajnju transportnu točku, kontroler i upravljačku komponentu. Podatkovna ravnina implementirana kroz krajnju transportnu komponentu, virtualni preklopnik na poslužitelju, pruža funkcije preklapanja, usmjeravanja, omogućuje povezivanje virtualne okoline s fizičkom infrastrukturom, te funkcije vatrozida na razini pojedinog poslužitelja. Podatkovna razina prosljeđuje pakete na temelju informacija koje dobije od kontrolne ravnine. Usmjeravanje paketa postiže se pomoću dvije vrste usmjernika:

- usmjernika zaduženog za usmjeravanja paketa između logičke i fizičke mreže,
- usmjernika zaduženog za usmjeravanje paketa unutar segmenata virtualne okoline.

Poslužitelj pruža vezu prema vanjskoj fizičkoj infrastrukturi no da bi mogao s njom komunicirati, uspostavlja prvo komunikaciju s kontrolerom kao centralnom točkom koja je svjesna ostalih poslužitelja i mreža na njima. Kontrolna ravnina implementirana kroz kontroler kao centralnu komponentu za distribuirano usmjeravanje između više poslužitelja i virtualnih mreža na njima. Dodatno, kontroler pruža informacije upravljačkoj komponenti o topologiji mreže i statistikama prometa. Ravnina upravljana implementirana kroz upravljačku komponentu koja je zadužena za upravljanje konfiguracijama i orkestracijom cijelog okruženja, uključujući i sigurnosne politike i uspostavu sigurnih kanala komunikacije između poslužitelja i kontrolera. Sigurna komunikacija ostvaruje se šifriranjem prometa razmjenom javnih i privatnih ključeva.

5 Dodatni mehanizmi zaštite na aplikativnom nivou

Kako je uvodno opisano, u opisanom modelu koriste se i dodatni mehanizmi zaštite na aplikativnom nivou kako bi se postigla zaštita u dubinu, odnosno zaštita na više razina. Model koristi vatrozid web aplikacija sa sustavom za balansiranje opterećenja web prometa, sustav za zaštitu elektroničke pošte i sustav za zaštitu od DDoS napada. Sve navedene komponente opisane su u nastavku.

5.1 Vatrozid web aplikacija

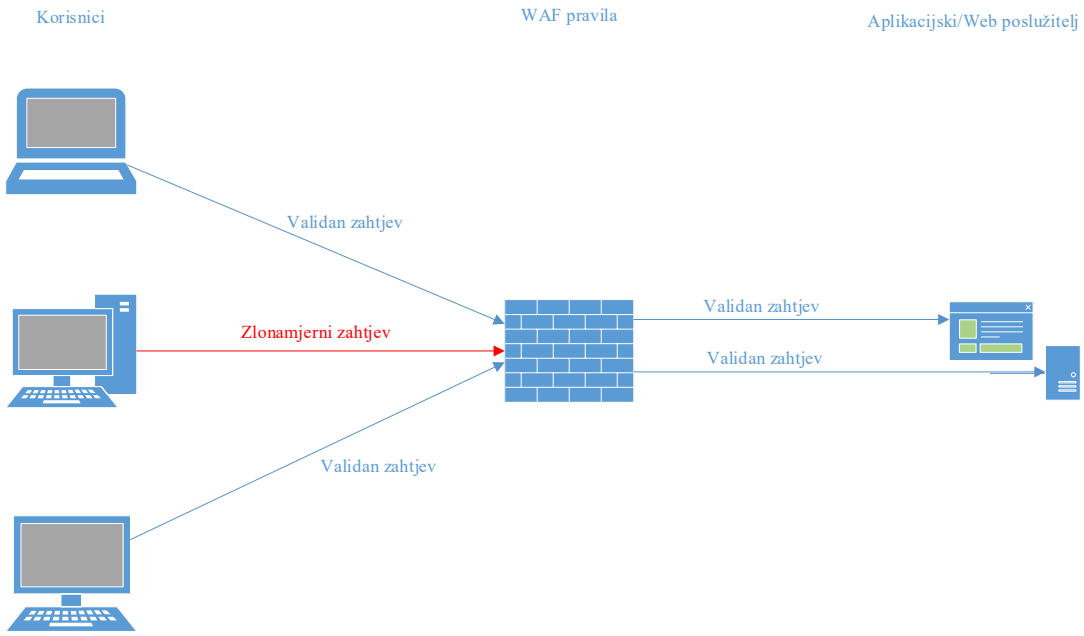
Vatrozid web aplikacija (*Web Application Firewall, WAF*) pruža dodatni sloj sigurnosti koji pruža zaštitu web aplikacija od širokog spektra napada, uključujući napade uskraćivanjem usluga, blokiranje sumnjivih korisničkih zahtjeva i neovlaštene korisnike, sprječavanjem pristupa osjetljivim datotekama i još mnogo toga. WAF funkcionira putem politika koje su zapravo skup pravila koja vatrozidu web aplikacije govore što treba učiniti s određenim vrstama zahtjeva s ciljem zaštite web aplikacija od ranjivosti. Većinom se WAF pravila koriste za blokiranje zlonamjernih zahtjeva, npr. ubacivanje SQL koda SQL injekcijom, za blokiranje određenih IP adresa, web stranica, određenih korisnika ili za blokiranje određenih ključnih riječi ili fraza.

Druga važna uloga WAF rješenja je poboljšana sigurnost aplikacijskih programskih sučelja (engl. Application Programming Interface, API). API su vezivno tkivo današnjih aplikacija a time i srž modernog poslovanja te je broj napada povezanih s API-jima u stalnom porastu, no njihova sigurnost se često zanemaruje. Neadekvatna sigurnost autentifikacije i autorizacije za API je jedna od najčešćih prijetnji prema OWASP Top 10 popisu sigurnosti za web aplikacije [11].

WAF rješenje analizira zahtjeve protokola za prijenos hiperteksta (HTTP) i primjenjuje skup pravila koja definiraju koji su dijelovi tog razgovora benigni, a koji su zlonamjerni. Zlonamjerni zahtjevi se smatraju zahtjevi sumnjive domene koji se namjerno koriste za iskorištavanje sustava, npr. krivotvorenje zahtjeva, DDoS napad i slični. Glavni dijelovi HTTP razgovora koje WAF analizira su GET i POST zahtjevi. GET zahtjevi koriste se za dohvaćanje podataka s poslužitelja, a POST zahtjevi koriste se za slanje podataka poslužitelju radi promjene stanja.

WAF rješenje štiti web aplikacije filtriranjem, nadzorom i blokiranjem bilo kakvog zlonamjernog HTTP/S prometa koji putuje do web aplikacije i sprječavanjem curenja podataka.

Kako je prikazano na *Slika 7*, to se postiže kroz skup pravila koja pomažu odrediti koji je promet zlonamjeran, a koji je siguran. Pravila se prilagođavaju kako bi zadovoljila jedinstvene potrebe web aplikacija pojedine organizacije. Što se modificirana politika može brže i lakše implementirati, to je odgovor na različite vektore napada brži te vrijednost WAF rješenja veća, npr. tijekom DDoS napada, ograničenje brzine može se brzo implementirati modificiranjem WAF politika. Tu veliku ulogu doprinosi i napredak u strojnom učenju koji omogućuje automatsko ažuriranje WAF politika.



Slika 7 *Način rada WAF rješenja*

Vatrozid web aplikacija uz pomoć svojih zaštitnih mehanizama, može spriječiti napade na aplikacijskom sloju koji inače zaobilaze tradicionalne mrežne vatrozide, uključujući sljedeće:

- zaštita od napada grubom silom – ovim napadom pokušava se dobiti pristup sustavu pokušajem prijave s velikim brojem mogućih lozinki,

- zaštita osjetljivih podataka od ubacivanja podataka – ovim napadom ubacuje se zlonamjerni kod u legitiman zahtjev za podacima kako bi se dobili osjetljivi podaci poput korisničkih imena, lozinki ili podataka o kreditnoj kartici. Ubacivanje podataka također se može koristiti za izmjenu podataka ili ometanje normalnog rada web stranice,

- zaštita od uskraćivanja usluge – ovim napadom se preplavljuje web stranicu brojnim zahtjevima sve dok ne bude u stanju opsluživati svoje korisnike i na taj način uzrokuje

pad ili nedostupnost usluge. Primjeri (D)DoS napada usmjerenih na aplikacijski sloj su HTTP/S poplave, SSL napadi, napadi grubom silom,

- zaštita od zlonamjernog URL-a (engl. Uniform Resource Locator) – ovima napadom se zlonamjerni softver postavlja na URL koji je sličan dobronamjernom URL-u s drugim znakovima,

- zaštita od krađe web sesije – ovim napadom se omogućuje napadačima da otmu ID sesije i maskiraju se u ovlaštenog korisnika. ID sesije obično se pohranjuje unutar kolačića ili URL-a,

- zaštita od ubacivanja SQL koda (engl. SQL injection) – ovim napadom se napadačima omogućuje da unesu SQL kod u podatkovno polje gdje to ne bi trebalo biti dopušteno. To napadačima omogućuje izvlačenje, promjenu ili brisanje informacija,

- zaštita od umetanja skripti (engl. Cross-site scripting, XSS) – ovaj napad omogućuje otmicu web stranice i zlonamjernu promjenu unutar legitimne web stranice, koja se zatim pokreće kao zaražena skripta u web pregledniku korisnika, omogućujući napadaču krađu osjetljivih informacija ili lažno predstavljanje korisnika.

Vatrozid web aplikacija provjerava promet na razini paketa, koristeći pravila duboke inspekcije paketa za identifikaciju sigurnih aplikacija na temelju kojih dopušta ili odbija svaki paketni pristup mreži. Korištenjem slijedećih mehanizama se donose odluke:

- profiliranje aplikacije – WAF analizira cjelokupno ponašanje i strukturu web aplikacije, uključujući tipične zahtjeve, dopuštene vrijednosti i vrste podataka, te kombinaciju pozitivnih i negativnih sigurnosnih modela kako bi pružio sveobuhvatnu zaštitu. Na taj način stvara profil aplikacije koji pomaže u prepoznavanju i blokiranju abnormalnih ili zlonamjernih zahtjeva,

- korištenje algoritama umjetne inteligencije i strojnog učenja za analizu uzoraka prometa - prate promet, ponašanje i karakteristike svakog tipa prometa kako bi se identificirale anomalije i optimizirale politike u stvarnom vremenu za sveobuhvatnu zaštitu uz

minimalno ili nimalo lažno pozitivnih rezultata. Dodatno se mogu koristiti i kontekstualne informacije o prirodi i svrsi aktivnih kampanja prijetnji,

- prilagodba ponašanja vatrozida web aplikacija trenutno definiranim pravilima,

- nadzor zloupotrebe API-ja uslijed pogrešne konfiguracije sigurnosnih parametara, neispravne autentifikacije, pogrešno konfiguriranih parametara samog API-ja, korištenje softvera otvorenog koga, nepoštivanje preporučenih sigurnosnih praksi,

- zaštita od automatiziranog pristupa botova i robota web stranicama korištenjem kombinacije tehnika temeljenih na izazovima i ponašanju za prepoznavanje i filtriranje prometa takvih alata,

- ugrađena analitika ponašanja web aplikacije koja kombinira ponašanje prometa s opterećenjem poslužitelja kako bi se identificiralo DDoS uvjete. Na taj način se stvaraju i postavljaju dinamički potpisi za zaštitu u stvarnom vremenu,

- mehanizmi za sprječavanje curenja podataka uz automatsko otkrivanje i maskiranje osjetljivih korisničkih podataka i vjerodajnica. Zaštita uključuje šifriranje podataka na sloju aplikacije te zaštitu prometa u prijenosu TLS protokolom.

Zadatak WAF rješenja je prihvatiti i odgovoriti na zahtjeve za web sadržajem s Interneta pružajući sredstva za filtriranje mrežnog prometa, dok još uvijek dopušta web aplikacijama da se povežu izravno na Internet. Umjesto stvaranja zida između unutarnjih i vanjskih mrežnih resursa propušta prijateljski promet i blokira zlonamjerni promet. Na taj način može spriječiti napade koji pokušavaju iskoristiti nedostatke u web aplikacijama, kao što su nepravilno dizajnirane web aplikacije, napadi ubacivanjem koda, lažiranja zahtjeva na drugom sjedištu (engl. Cross Site Request Forgery, CSRF), uskraćivanje usluga i drugi. Bitno je za napomenuti da WAF rješenje ne popravlja temeljne ranjivosti ili nedostatke u web aplikacijama, već sprječava napadače blokiranjem uobičajenih puteva napada i ograničavanjem zahtjeva. Dodatno, vatrozid web aplikacija bilježi promet web aplikacija, pokušaje napada i korake koje organizacija poduzima kako bi osigurala svoje web aplikacije, što su koraci potrebni za aktivnosti revizije i usklađenosti s regulatornim i zakonskim zahtjevima.

U opisanom modelu implementiran je mrežni WAF koji je smješten u svakom podatkovnom centru korisnika kako bi se ostvarila visoka dostupnost rješenja. Prednosti takve implementacije su smanjena latencija, jer se može instalirati što bliže štićenim lokalnim web aplikacijama, veća fleksibilnost i kontrola nad načinom na koji je konfiguriran, a time i naprednija sigurnost. WAF rješenje je integrirano s web aplikacijama u načinu rada koji se naziva transparentni obrnuti *proxy* u kojem su web aplikacije svjesne postojanja vatrozida, ali klijenti nisu. WAF prihvaća promet na adresama i portovima koji se vanjskim klijentima pojavljuju kao aplikacijske adrese i portovi, dok same web aplikacije rade na različitim internim adresama i portovima što pruža veću izolaciju i mogućnost provjere prometa prije nego što stigne do aplikacija. WAF provjerava promet i odlučuje hoće li ga proslijediti tim portovima i adresama. Po pitanju sigurnosnih modela, implementiran je hibrini WAF koji koriste elemente popisa blokiranih (engl. black list) i dopuštenih (engl. white list) lista odnosno zahtjeva.

5.2 Sustav za balansiranje web prometa

Sustav za balansiranje prometa sastoji se od softverskih modula za lokalnu i globalnu raspodjelu aplikacijskog prometa te DNS zaštite.

Za potrebe servisa koji su dostupni s Interneta, kao i za interne servise dostupne korisnicima, koristi se globalni DNS sustav za balansiranje web prometa (engl. Global Service Load Balancer, GSLB) koji osigurava preusmjeravanje upita na ispravnu IP adresu neovisno o pružatelju internet usluga. Tim sustavom se izbjegava ručno mijenjanje DNS zapisa na višestrukim uređajima u mreži u slučaju ispada nekog servisa te smanjuje vrijeme propagacije istoga. Kako bi se ostvarila visoka dostupnost, sustav se sastoji od dva uređaja smještena u glavnim sistem sobama.

Softverski modul namijenjen upravljanju opterećenjem poslužitelja na razini svakog pojedinog podatkovnog centra je u ulozi obrnutog posredničkog poslužitelja (engl. reverse proxy). To znači da na sebe preuzima klijentske konekcije, dok u pozadini uspostavljaju posebnu konekciju prema poslužiteljskoj strani. Pri tome koriste algoritme za balansiranje opterećenjem poslužitelja u pozadini. U mogućnosti je raditi i SSL terminaciju (engl. SSL offload ili SSL bridging).

Softverski modul namijenjen pametnom upravljanju globalne raspodjele aplikacijskog prometa između različitih podatkovnih centara koristi DNS zapise. Kako bi obavljao svoju funkciju

provjerava stanje servisa čije zapise sadrži te radi automatsko ažuriranje DNS zapisa s obzirom na status servisa. Na temelju informacija o trenutnom stanju pojedine aplikacije upravlja zapisima i radi raspodjelu korisničkih zahtjeva. Dodatno pruža i zaštitu DNS prometa, zaštitu od *DNS Cache Poisoning* napada te zaštitu za ranjivosti vezane uz DNS DDoS napade.

Kako bi se izbjeglo ručno mijenjanje DNS zapisa na svim uređajima u mreži koji koriste određeni servis, duže vrijeme nedostupnosti pojedinog servisa zbog vremena potrebnog za sve izmjene te smanjila mogućnost ljudske greške, sustav za balansiranje web prometa predstavlja autoritativni poslužitelj za sve interne i javne domene i poddomene te obavlja funkciju javnog DNS poslužitelja za javno dostupne servise. Kako bi se osigurala visoka dostupnost sustava, po jedan uređaj je implementiran u svakom od podatkovnih centara.

5.3 Sustav za zaštitu elektroničke pošte

U današnjem svijetu digitalne transformacije i sve većeg korištenja elektroničke pošte u poslovanju, povećavaju se i opasnosti koje dolaze uz elektroničku poštu. Shodno tome, potrebno je razmišljati i kako se zaštiti od napada i malicioznih prijetnji koji se mogu propagirati kroz elektroničku poštu. Preporuka je implementacija rješenja za zaštitu elektroničke pošte koje pruža naprednije načine analize.

Kako opisani model koristi O365 uslugu elektroničke pošte u oblaku, rješenje za zaštitu elektroničke pošte je također implementirano u oblaku. Rješenje radi na način da se elektronička pošta preusmjerava na pregled i analizu iz O365 oblaka u oblak implementiranog rješenja koje pruža zaštitu od naprednih malicioznih prijetnji i nepoznatih (enlg. zero-day) napada. Za potrebe kontrole, detektiranja i blokiranja mogućih prijetnji, uz dubinsku inspekciju prometa, rješenje koristi i izvođenje sumnjivih datoteka i pristup URL-ovima u izoliranom virtualnom okruženju (engl. sandbox). Dodatno se koriste i servisi u oblaku koji se svake sekunde nadopunjuju novim informacijama o prijetnjama koristeći globalnu inteligentnu mrežu proizvođača rješenja koja služi za primanje i dijeljenje informacija o naprednim i nepoznatim prijetnjama kao što su *zero-day* napadi. Odrađuje se analiza svakog priloga elektroničke pošte i URL-a te se šalju u karantenu svi koji predstavljaju potencijalne sigurnosne prijetnje uključujući i *spear-fishing* elektroničku poštu. Dolazna pošta se drži u karanteni dok se svi privici ne analiziraju na maliciozna ponašanja unutar okoline virtualne mašine. Za malicioznu elektroničku poštu koja je stavljena u karantenu šalju se notifikacije korisnicima.

5.4 Sustav za zaštitu od DDoS napada

Digitalne transformacije sa sobom donose i nove izazove a jedan od njih je i povećavana opasnost od uskraćivanja usluge odnosno nedostupnosti nekog poslovnog servisa. Vjerojatnost takvih napada svakim danom raste, a gubici s kojima se organizacije suočavaju se povećavaju. Shodno tome, potrebno je razmišljati i kako se zaštiti od takve vrste napada i izbjeći gubitke i ostale rizike koji mogu nastati. Preporuka je implementacija rješenja za zaštitu od DDoS napada.

Rješenje je implementirano u transparentnom načinu rada (engl. inline mode) na Internet linkovima kako bi moglo pasivno promatrati dolazni promet i slati ga dalje prema lokalnoj mreži bez unošenja dodatnog kašnjenja zbog analize prometa. U slučaju detekcije napada, uređaj automatski aktivira zaštitu i blokira napadački promet na samom ulazu u mrežu, dok legitimni promet neometano prolazi. Korištenjem više izvora informacija automatsko detektiranje i blokiranje distribuiranih napada za uskraćivanje usluga (*Distributed Denial of Service, DDoS*) se odvija unutar nekoliko sekundi. Kako moderni DDoS napadi koriste nove tehnike za iskorištavanje ranjivosti koje tradicionalna sigurnosna rješenja ne mogu spriječiti, takvi napadi mogu uzrokovati ozbiljne zastoje u mreži osobito za organizacije koje ovise o mreži i web servisima kako bi mogle pružati usluge. Sustav za zaštitu od DDoS napada omogućava dodatnu zaštitu u sklopu sigurnosnog perimetra organizacije kako bi na vrijeme spriječio destruktivne DDoS napade, prije nego oni uzrokuju štetu. Implementirano rješenje pruža sljedeće funkcionalnosti:

- blokiranje širokog raspona napada s prilagodljivom višeslojnom zaštitom:
    - zaštita bazirana na analizi ponašanja (engl. behavioral protection) koja se definira pomoću više elemenata na osnovu kojih se postavljaju granice i blokira neregularan promet,
    - automatski generirani i predefinirani potpisi (engl. signatures),
    - korištenje naprednih tehnika upita i odgovora (engl. challenge/response),
    - blokiranje napada koji nisu bazirani na ranjivostima, nego zloupotrebljavaju resurse poslužitelja - aplikacijski DoS – HTTP, SIP i ostale vrste napada poplava (engl. flood attacks),
    - blokiranje DoS/DDoS napada koji iscrpljuju mrežne resurse,
- preciznu zaštitu od napada na slijedeće načine:
    - generiranje potpisa u stvarnom vremenu za svaki uzorak napada koristeći do 20 različitih parametara,

- brzom reakcijom i ažuriranjem generiranih potpisa u stvarnom vremenu kako bi se zaštitilo od nadolazećih napada,
- blokiranjem napada bez blokiranja legitimnog korisničkog prometa,
- inteligentnom detekcijom povremenih naglih promjena u prometu (engl. flash traffic), pri čemu se uočava razlika između legitimnih porasta prometa i napada (pomoću analize ponašanja prometa u stvarnom vremenu).

Rješenje pruža i intuitivno, prilagodljivo grafičko sučelje s preciznim forenzičkim uvidom u DDoS napade koje omogućava povijesni pregled napada, te detaljne informacije o raznim parametrima i prirodi napada.

6 Zaključak

Digitalizacija osim pozitivnih strana donosi i neke negativne, kao na primjer povećani broj kibernetičkih napada, sve više vektora napada na sustave. Teško je u današnjem svijetu pronaći sustav koji nije u riziku od kibernetičkih napada. Shodno tome, svaka organizacija koja brine o svojoj sigurnosti bi trebala raditi na podizanju svijesti o informacijskoj sigurnosti i raditi na poboljšanju sigurnosti unutar kritične infrastrukture. Kao početna točka u tom procesu može poslužiti NIS/NIS2 direktiva koja služi kao smjernica za nacionalnu strategiju kibernetičke sigurnosti državama članicama EU, no može biti i jako dobra podloga za strategiju kibernetičke sigurnosti pojedine organizacije. NIS/NIS 2 direktiva daje i popis minimalnih sigurnosnih mjera koje bi trebalo implementirati, te alate za upravljanje životnim ciklusom sigurnosne strategije. Dodatno potiče države EU, a time i organizacije u njima, na uključivanje u razne inicijative za unapređenje i razvoj vještina i mehanizama kibernetičke sigurnosti, te programe suradnje i koordiniranih aktivnosti za otkrivanje i dijeljenje informacija o ranjivostima i načinima zaštite. Time bi organizacije podigle svijest ali i znanje cjelokupne organizacije o rizicima koje donosi modernizacija poslovanja te potrebnim zaštitnim mehanizmima koje je potrebno implementirati. U konačnici uključivanjem i primjenjivanjem nacionalne strategije kibernetičke sigurnosti na više sektora dobiva se veća i sigurnija zaštita država članica te veća mreža sudionika razmjena informacija o sigurnosnim ugrozama i prijetnjama, te podizanje nivoa znanja i svjesnosti o potencijalnim prijetnjama i scenarijima napada.

Osim podizanja svijesti i znanja, potrebna su i tehnička rješenja koja pružaju mogućnost implementacije predloženih sigurnosnih mjera. Jedan skup tih rješenja su rješenja za softverski definirane mreže koja pokušavaju riješiti nove izazove pružajući sigurnost, automatizaciju, kontinuitet poslovanja i povećanu agilnost. Temeljna načela tih rješenja su ograničen pristup aplikacijama s najmanjim privilegijama i kontinuiranom provjerom identiteta čime se smanjuje površina napada, za udaljenu komunikaciju se uspostavljaju sigurni šifrirani tuneli, upravljanje komponentama se vrši iz centralne točke, odvaja se kontrolna ravnina od podatkovne ravnine. Implementacija takvih rješenja uvelike smanjuje rizike kibernetičke sigurnosti, no eliminirati taj rizik u potpunosti je nemoguće. Iz tog razloga, prilikom implementacije softverski definiranih mreža, posebna pažnja treba se obratiti na slijedeće točke:

- osigurati ispravnu konfiguraciju ključnih komponenti sa stalnim nadzorom i bilježenjem svake promjene kako bi mogla se revidirati u slučaju problema i/ili proboja,

- napraviti dobru segmentaciju mreže i ograničiti pristup kako bi se što više onemogućilo lateralno kretanje napadača u slučaju krađe identiteta,
- pregledavati, bilježiti i analizirati sav promet na mreži (za šifrirani promet prikupljati meta podatke) kako bi se otkrilo aktivnog napadača ili upotreba zlonamjernog softvera,
- voditi brigu o pohrani prikupljenih podataka o mreži i točci upravljanja kako bi se zaštitili od napadača,
- voditi brigu o upotrebi entiteta koji nemaju korisnički identitet (npr. softverski agenti, uređaji za Internet stvari) za koje postoji rizik identificiranja lažno pozitivnih i lažno negativnih radnji koje onda u konačnici utječu na cjelokupni sigurnosni položaj organizacije,
- iako nije nužno vezano samo uz ovaj koncept, preporuka je implementirati rješenja za zaštitu od napada uskraćivanja usluge zbog rizika koji takvi napadi predstavljaju.

Kako bi se postigla i zaštita poslovno kritičnih aplikacija, sve više i više organizacija implementiraju i dodatna tehnička rješenja kao što su vatrozidi web aplikacija, rješenja za zaštitu od DDoS napada, rješenja za zaštitu elektroničke pošte, rješenja za zaštitu DNS prometa i slična. Takva rješenja pružaju takozvanu zaštitu u dubinu, odnosno na više nivoa, blokirajući moguće prijetnje web stranicama, zaštitu od uskraćivanja usluge odnosno nedostupnosti nekog poslovnog servisa, zaštitu od naprednih malicioznih prijetnji i nepoznatih (engl. zero-day) napada, zaštitu od DNS *Cache Poisoning* i DNS DDoS napada. Temelj takvih rješenja su sigurnosna pravila i politike koje organizacije moraju pažljivo definirati i primijeniti kako bi odgovarala potrebama njihovih aplikacija te prilagođavati kako se sustav i aplikacije razvijaju i mijenjaju.

Stalno mijenjanje pravila može dovesti do puno lažno pozitivnih rezultata ili još gore do lažno negativnih kojima se riskira propuštanje zlonamjernog prometa. Ovim izazovima dodatno doprinose i okruženja mikro servisa gdje se verzije mogu mijenjati i više puta dnevno što bi trebalo povlačiti i provjeru i potencijalno mijenjanje pravila, što može predstavljati velike izazove za mnoge organizacije.

Svako od obrađenih rješenja je učinkovito za namijenjeno područje no kako bi se postigla holistička obrambena strategija potrebna je implementacija više tehničkih sigurnosnih rješenja sukladno poslovnim potrebama pojedine organizacije. Ne postoji jedno rješenje primjenjivo na sve. Svaka organizacija je priča za sebe, te je potrebno proći cijeli proces od uspostave strategije i programa informacijske sigurnosti, klasifikacije sve imovine i sustava, analize rizika sukladno poslovnim zahtjevima, uspostavljanja svih procesa, politika i procedura predviđenih

programom informacijske sigurnosti, do uspostave sigurnosnih kontrola kroz implementaciju tehničkih rješenja. Uz to treba imati na umu da niti jedan od koraka tog procesa nije jednokratni projekt već to postaje iterativan proces koji zapravo postaje način promišljanja o informacijskoj sigurnosti cijelog sustava a ne nužno same organizacije. Stoga je potrebno pronaći djelotvorna i učinkovita rješenja za buduće izazove informacijske sigurnosti te promijeniti način na koji cijela organizacija razmišlja o povjerenju te općenito kibernetičkoj sigurnosti i integrirati taj način razmišljanja u buduće projekte. Potrebno je osnovati višefunkcionalne timove, koje čine mrežni, sigurnosni, aplikativni arhitekti, inženjeri i tehničari, kako bi osvijestili što je povjerenje u mrežnom, sigurnosnom, aplikativnom kontekstu, koje su potencijalne zloupotrebe istoga te općenito koji su sve izazovi sigurnosni izazovi koje donosi modernizacija poslovanja. Takav tim dalje radi na razvoju strategije kibernetičke sigurnosti pojedine organizacije koja je usklađena s poslovnim potrebama i regulatornim postavkama, ograničenjima u korisničkom iskustvu, te troškove kako bi to dalje predstavio višim slojevima organizacije s ciljem buduće implementacije te strategije.

Popis literature

[1] E. U. A. f. C. -. ENISA, “Interoperable EU RM Toolbox,” [Mrežno]. Dostupno na: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox. [Posjećeno 9. Ožujka 2023.].

[2] E. N. a. I. S. A. ENISA, “ENISA Guidebook on National Cyber Security Strategies_Final.pdf,” Prosinac 2012. [Mrežno]. Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools. [Posjećeno 6. Ožujka 2023.].

[3] “Vijest o Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga,” 19. Srpanj 2018. [Mrežno]. Dostupno na: https://www.zakon.hr/cms.htm?id=31153. [Posjećeno 5. Ožujka 2023.].

[4] “Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti,” Carnet, 2019.

[5] E. U. A. f. C. -. ENISA, “Minimum Security Measures for Operators of Essentials Services,” [Mrežno]. Dostupno na: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services. [Posjećeno 8. Ožujka 2023.].

[6] J. Kinervag, “Build Security Into Your Network's DNA: The Zero Trust Network Architecture,” 5. Studeni 2010. [Mrežno]. Dostupno na: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. [Posjećeno 2. Veljače 2023.].

[7] J. B. David Holmes, “The Definition Of Modern Zero Trust,” 24. Siječanj 2022. [Mrežno]. Dostupno na: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/. [Posjećeno 6. Veljače 2023.].

[8] O. B. S. M. S. C. Scott Rose, “Special Publication 800-207: Zero Trust Architecture,” Kolovoz 2020. [Mrežno]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Posjećeno 5. Siječnja 2023]..

[9] “Zero Trust Maturity Model Pre-decisional Draft,” June 2021. [Mrežno]. Dostupno na: https://www.cisa.gov/sites/default/files/publications/CISA%2520Zero%2520Trust%2520Maturity%2520Model_Draft.pdf. [Posjećeno 15. Siječnja 2023.].

[10] “Cisco SD-WAN Cloud scale arhitecture,” 2019.

[11] “Top 10 Web Application Security Risks,” [Mrežno]. Dostupno na: https://owasp.org/www-project-top-ten/. [Posjećeno 18. Veljače 2023.].

[12] J. Kinervag, “No More Chewy Centers: The Zero Trust Model Of Information Security Architecture And Operations Playbook,” 23. Ožujak 2016. [Mrežno]. Dostupno na: https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf. [Posjećeno 4. Veljače 2023.].

[13] »Zero trust security model,« [Mrežno]. Dostupno na: https://en.wikipedia.org/wiki/Zero_trust_security_model. [Posjećeno 16. Siječnja 2023.].

[14] “Software-defined networking,” [Mrežno]. Dostupno na: https://en.wikipedia.org/wiki/Software-defined_networking. [Posjećeno 18. Siječnja 2023.].

[15] K. Raina, “Zero trust security explained: principles of the zero trust model,” *Crowdstrike Cybersecurity 101,* 17. Listopad 2022.

[16] “Cisco Systems Software-Defined Access for Distributed Campus Solution Adoption Prescriptive Reference Deployment Guide,” 2019.

[17] “Cisco Validated Design User-to-Data-Center Access Control Using TrustSec Design Guide,” 2015.

[18] “NSX Reference Design Guide Network Virtualization Design Guide,” 2020.

[19] S. p. e. 10, “Zero Trust,” 28. Ožujka 2022. [Mrežno]. Dostupno na: https://www.span.eu/hr/spanoptic-podcast/. [Posjećeno 29. Ožujka 2022.].

[20] “The Fortinet SDN Security Framework Agile Security for Software-Defined Networks and Data Centers,” 2016.

[21] S. H, “Zero trust architecture design principles,” 20. Studenog 2019. [Mrežno]. Dostupno na: https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles. [Posjećeno 31. Siječnja 2023.].

[22] T. Hristov, “Understanding the vSAN Witness Host,” 2. Kolovoz 2021. [Mrežno]. Dostupno na: https://core.vmware.com/blog/understanding-vsan-witness-host. [Posjećeno 25. Ožujka 2023.].

[23] E. U. A. f. C. -. ENISA, “NIS Directive,” [Mrežno]. Dostupno na: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new. [Posjećeno 5 March 2023].

[24] E. U. A. f. C. -. ENISA, “National Cybersecurity Assessment Framework (NCAF) Tool,” [Mrežno]. Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/. [Posjećeno 7. Ožujka 2023.].

[25] “Direktiva (EU) 2016/1148 Europskog parlamenta i vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije,” *Službeni list Europske unije,* Srpanj 2016.

[26] V. HR, “Prijedlog uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga,” Srpanj 2018.

[27] K. Filla, “NIS direktiva: Još jedan razlog zašto vam treba sigurno IT okruženje,” 25. Travanj 2018. [Mrežno]. Dostupno na: https://mreza.bug.hr/nis-direktiva-jos-jedan-razlog-zasto-vam-treba-sigurno-it-okruzenje/. [Posjećeno 6. Ožujka 2023.].

[28] G. Knezović, “EU jača kibernetičku sigurnost novom NIS2 direktivom,” 29. Svibanj 2022. [Mrežno]. Dostupno na: https://mreza.bug.hr/eu-jaca-kiberneticku-sigurnost-novom-nis2-direktivom/. [Posjećeno 6. Ožujka 2023.].

[29] “Web application firewall,” [Mrežno]. Dostupno na: https://en.m.wikipedia.org/wiki/Web_application_firewall. [Posjećeno 12. Veljače 2023.].

[30] “What is a WAF? Web Application Firewall,” [Mrežno]. Dostupno na: https://nonamesecurity.com/learn-what-is-web-application-firewall. [Posjećeno 11. Veljače 2023.].

[31] M. Giannelis, “What is Web Application Firewall (WAF) and How is it Used to Protect Your Website?,” [Mrežno]. Dostupno na: https://www.techbusinessnews.com.au/what-is-web-application-firewall-waf-and-how-is-it-used-to-protect-your-website/. [Posjećeno 12. Veljače 2023.].

[32] B. Lutkevich, “Web application firewall (WAF),” Studeni 2019. [Mrežno]. Dostupno na: https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF. [Posjećeno 14. Veljače 2023.].

[33] “What Is A Web Application Firewall (WAF) and How Does It Work,” [Mrežno]. Dostupno na: https://www.radware.com/cyberpedia/application-security/what-is-waf/. [Posjećeno 17. Veljače 2023.].

[34] “What is a WAF? | Web Application Firewall explained,” [Mrežno]. Dostupno na: https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf/. [Posjećeno 18. Veljače 2023.].

[35] “How does a web application firewall (WAF) work?,” [Mrežno]. Dostupno na: https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf/. [Posjećeno 18. Veljače 2023.].

[36] “What Is a WAF? | Web Application Firewall Explained,” [Mrežno]. Dostupno na: https://www.paloaltonetworks.com/cyberpedia/what-is-a-web-application-firewall. [Posjećeno 18. Veljače 2023.].

[37] “WAF vs. Firewall: Web Application & Network Firewalls,” [Mrežno]. Dostupno na: https://www.fortinet.com/resources/cyberglossary/waf-vs-firewall. [Posjećeno 20. Veljače 2023.].

[38] F5, “Protection for Every App, Anywhere Solution overview,” 2022.

[39] F5, “BIG-IP Local Traffic Manager,” 2022.

[40] “BIG-IP DNS,” [Mrežno]. Dostupno na: https://www.f5.com/products/big-ip-services/big-ip-dns. [Posjećeno 2. Travnja 2023.].

[41] Fireeye, “Data sheet Fireeye Email Security Cloud Edition,” 2019.

[42] “DDoS Protection For Any Environment: On-Premise, Private and Public Clouds, and Hybrid Environments,” [Mrežno]. Dostupno na: https://www.radware.com/solutions/ddos-protection/. [Posjećeno 4. Travnja 2023.].

[43] “DefensePro X: The Next Level of DDOS Protection,” [Mrežno]. Dostupno na: https://www.radware.com/products/defensepro/. [Posjećeno 4. Travnja 2023].