Veleučilište u Virovitici

ET²eR vol. IV, br. 2, 2022., str. 26-31

UDK: 007:004
Stručni rad (Professional work)

NIST - okvir za kibernetičku sigurnost

Enes Ciriković[1], Dora Fabijanić[2]

[1]Veleučilište u Virovitici, Ulica Matije Gupca 78, 33000, Virovitica, enes.cirikovic@vuv.hr

[2]Studentica Veleučilišta u Virovitici, Ulica Matije Gupca 78, 33000, Virovitica, dora.fabijanic@vuv.hr

Sažetak

Kako digitalni svijet postaje sve veći dio svakodnevnice i kako broj korisnika i resursa Interneta sve više raste, tako i broj mogućih incidenata kibernetičke sigurnosti raste. To znači da je potrebna dobra osviještenost o prijetnjama, te uspostava dobrih praksi i politika kako bi se osjetljive informacije zaštitile unutar i izvan organizacija. Vladina agencija NIST u SAD-u je razvila okvir za kibernetičku sigurnost koja pruža pomoć organizacijama kako bi uspostavile dobru kibernetičku sigurnost i dobar program za upravljanjima rizicima kibernetičke sigurnosti. U ovome radu opisani su osnovni pojmovi kibernetičke sigurnosti i njezine prijetnje, te namjena, struktura, implementacija, prednosti i nedostaci NIST okvira za kibernetičku sigurnost.

Ključne riječi

kibernetička sigurnost, NIST, okvir za kibernetičku sigurnost, osjetljive informacije , rizici kibernetičke sigurnosti

Abstract

As the digital world becomes an increasing part of everyday life and as the number of Internet users and resources grows, so does the number of possible cybersecurity incidents. This means that there is a need for good awareness of threats, and the establishment of good practices and policies to protect sensitive information inside and outside the organization. The U.S. government's NIST agency has developed a cybersecurity framework that provides assistance to organizations to establish good cybersecurity and a good cybersecurity risk management program.

This paper describes the basic concepts of cyber security and its threats, as well as the purpose, structure, implementation, advantages and disadvantages of the NIST framework for cyber security.

Keywords

cybersecurity, cybersecurity framework, cybersecurity risks, NIST, sensitive informations

Uvod

U današnje vrijeme sve više organizacija digitalizira poslovne procese, a ljudi postaju ovisniji o tehnologijama kao što su mobiteli, računala, tableti ili Internet. Društvene mreže, kupovina, Internet bankarstvo i poslovni servisi su samo neki primjeri velike izloženost osjetljivih informacija kibernetičkim napadima, što znači da organizacije i fizičke osobe vrlo lako mogu postati žrtve krađe identiteta, pokušaja iznuđivanja ili gubitka datoteka i informacija. Broj prijetnji kibernetičke sigurnosti je sve veći, stoga osiguravanje kibernetičke sigurnosti i osvješćivanje o njezinoj važnosti postaje jedna od ključnih stavki za održavanje funkcioniranja današnjeg društva. Standardi kibernetičke sigurnosti skup su najboljih praksi, politika, i koncepata čiji je cilj obrana sustava, mreža, programa, uređaja i informacija od kibernetičkih napada. [1]

Kako bi zaštitio Sjedinjene Američke Države od napada na kibernetičku sigurnost, predsjednik Obama izdao je Izvršnu naredbu za razvoj okvira kibernetičke sigurnosti, promovirali i poticanje usvajanja praksi kibernetičke sigurnosti i uključenje snažne zaštite privatnosti i građanskih sloboda. NIST (engl. *National Institute of Standards and Technology*) je prema direktivi postao voditelj razvoja okvira za smanjenje kibernetičkog rizika na kritičnu infrastrukturu te je 2013. godine krenuo s istraživanjem s ciljem prikupljanja ključnih informacija od industrija, akademskih zajednica i drugih sudionika. Ispitivali su organizacije o procjenjivanju rizika, trenutnoj upotrebi postojećih okvira, standarda i smjernica kibernetičke sigurnosti te o pravnim aspektima određenih okvira, standarda, najboljih praksi i izazovima pri ispunjenju takvih zahtjeva.

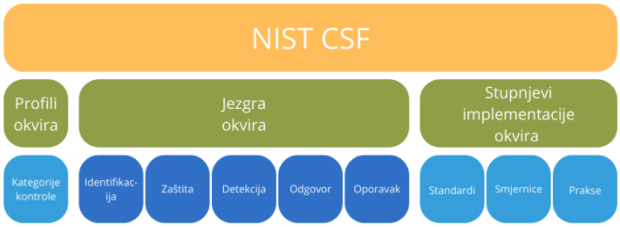
Na temelju prikupljenih informacija NIST je 2014. godine objavio prvu verziju okvira za kibernetičku sigurnost koji identificira postojeće prakse za informiranje o odlukama organizacije o upravljanju rizicima koje se odnose na prevenciju i otkrivanje, odgovor i oporavak od problema kibernetičke sigurnosti. [4]

1. Struktura okvira za kibernetičku sigurnost

Analizom provedenih istraživanja i radionicama u svim tipovima organizacija NIST je identificirao zajedničke karakteristike i teme kibernetičke sigurnosti koje se ponavljaju. Neke od zajedničkih točaka su razumijevanje okruženja prijetnje, procjena rizika, razine zrelosti i odgovori na incidente. Te teme i točke su korištene i uključene kroz cjelokupan razvoj okvira.

Okvir za kibernetičku sigurnost je pristup upraljavnju baziran na kibernetičkom sigurnosnim rizikom koji se sastoji od tri dijela: jezgra okvira, stupnjevi implementacije okvira i profili okvira kao što je i prikazano na slici 1. Svaka komponenta okvira jača vezu između poslovnih pokretača i aktivnosti kibernetičke sigurnosti. [3]

SLIKA 1: STRUKTURA NIST OKVIRA ZA KIBERNETIČKU SIGURNOST



Izvor: izrada autora

1.1. Jezgra okvira za kibernetičku sigurnost

Prema izvoru [3] jezgra NIST okvira je skup aktivnosti kibernetičke sigurnosti, željenih aktivnosti i rezultata te primjenjivih referenci uobičajenih u sektorima kritične infrastrukture, odnosno predstavlja standarde, smjernice i prakse koje omogućuju komunikaciju između multidiscipinatnih timova. Sastoji se od pet neprekidnih funkcija: identifikacija, zaštita, detekcija, odgovor i oporavak koje su ujedno i najviša razina apstrakcije uključene u okvir. Jezgra okvira identificira temeljne ključne kategorije i potkategorije za svaku funkciju te ih povezuje s primjerima informativnim referencama (standardi, smjernice i prakse za svaku podkategoriju).

Aktivnosti u funkciji „Identifikacija“ su temelj za učinkovito korištenje okvira. Ova funkcija pomaže u razvoju organizacijskog razumijevanja upravljanja kibernetičkim rizicima, poslovnog konteksta, resursa te omogućuje organizaciji da se usredotoči i odredi svoje prioritete u skladu sa strategijom upravljanja rizicima i poslovnim potrebama. Kategorije unutar ove funkcije uključuju upravljanje imovinom, procjenu rizika, strategiju upravljanja rizicima.

Funkcija „Zaštita“ opisuje odgovarajuće mjere zaštite pri isporuci kritičnih infrastrukturnih usluga. Omogućuje ograničavanje ili obuzdavanje utjecaja potencijalnog štetnog događaja kibernetičke sigurnosti. Neki primjeri kategorija ove funkcije su kontrola pristupa, svijest i obuka, sigurnost podataka...

Funkcija „Detekcija“ definira odgovarajuće aktivnosti za prepoznavanje pojave događaja kibernetičke sigurnosti i omogućava njegovo pravovremeno prepoznavanje. Primjeri kategorija

funkcije detekcije su procesi otkrivanja i kontinuirano praćenje sigurnosti.

Odgovarajuće aktivnosti za poduzimanje radnju u vezi s otkrivenim incidentom kibernetičke sigurnosti opisane su u funkciji odgovora. Kategorije uključene unutar funkcije „Odgovor" detekcije su planiranje odgovora, komunikacija, analiza i poboljšanja.

Funkcija „Oporavak" identificira odgovarajuće aktivnosti za održavanje planova za otpornost i vraćanje svih sposobnosti ili usluga koje su bile narušene tokom incidenta. Podržava pravovremeni oporavak u normalne operacije kako bi smanjili utjecaj incidenta kibernetičke sigurnosti. Primjeri kategorija su planiranje oporavka, poboljšanja i komunikacija.

Zajedno ove funkcije pružaju strateški pogled na životni ciklus upravljanja rizikom kibernetičke sigurnosti unutar organizacije te pomažu organizacijama osposobiti upravljanje rizikom kibernetičke sigurnosti na visoku razinu.

1.2. Slojevi implementacije okvira i profili okvira

Slojevi implemenacije okvira (*eng. "Tiers"*) pružaju kontekst o tome kako organizacija organizacija gleda na rizike kibernetičke sigurnosti i upravljanje tim rizicima. Ti slojevi opisuju do kojeg stupnja organizacija upravlja rizicima kibernetičke sigurnosti prema karakteristikama definiranih u okviru. Stupanj upravljanja rizicima kibernetičke sigurnosti odražava napredak od neformalnog, reaktivnog odgovora do agilnih pristupa i dobre informiranosti o riziku. Kako bi organizacija odabrala željeni stupanj prvo mora razmotriti svoje trenutne prakse upravljanja rizicima, prijetnje okoliša, zakonske i regulatorne zahtjeve, ciljeve poslovanja te organizacijska ograničenja.

Profil okvira predstavlja ishode koje je organizacija odabrala iz kategorija okvira i potkategorija na temelju vlastitih poslovnih potreba. Može se koristiti za identifikaciju i usporedbu trenutnog Profila organizacije i ciljanog Profila. Kako bi razvila Profil, organizacija analizom svih kategorija i potkategorija, uzimajući u obzir poslovanje i procjenu rizika, može odrediti koje su njima najvažnije kategorije. Također, može dodavati kategorije i potkategorije ovisno o potrebama za smanjenje rizika organizacije. Osim toga, koristi se i kao podrška pri određivanju prioriteta, mjerenja napretka, provođenje samoprocjene i komunikaciju unutar jedne ili više organizacija. [4]

2. Zastupljenost okvira i implementacija kibernetičke sigurnosti prema NIST modelu

Okvir nije dizajniran da zamjeni postojeće procese identificiranja i upravljanja rizicima kibernetičke sigurnosti. Njegova svrha je određivanje nedostataka u trenutnom pristupu prema rizicima i razviti smjernice za poboljšanje sigurnosti. Uporabom okvira kao alata za upravljanje rizikom kibernetičke sigurnosti, organizacija može odrediti najvažnije aktivnosti za pružanje kritičnih usluga i odrediti prioritete kako bi se maksimizirao učinak ulaganja. Odnosno, okvir je osmišljen kao nadopuna postojećeg poslovanja i operacija kibernetičke sigurnosti ili temelj za novi program kibernetičke sigurnosti .

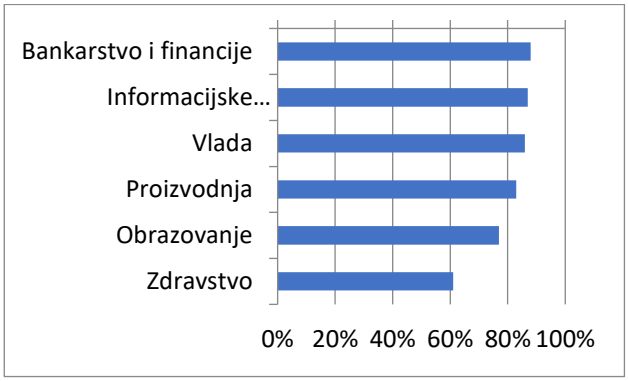
Također, NIST razumije različitost tvrtki i uzima u obzir da su mala i srednja poduzeća ograničena resursima za upravljanje rizikom. Kontinuirano pokušavaju stvoriti okvir koji ne samo da se bavi budućim rizicima, već pruža i nacrte upravljanja rizikom za organizacije, bez obzira na njihovu veličinu. To znači da male i srednje i velike tvrtke mogu profitirati radom kroz okvir. [4]

Predrasude o smanjenoj mogućnosti usvajanja NIST okvira kod malih poduzeća zbog cijene ili neimanja resursa smanjili su rezultati istraživanja 2016. godine. Kod tvrtki sa više od 10000 zaposlenika je vjerojatnost da će biti usvojena sigurnosni okvir je 90% , ali čak i kod tvrtki s manje od 1000 zaposlenika prijavljuju se stope usvajanja od 77%. [3]

2.1. Zastupljenost NIST okvira

Usvajanje sigurnosnih okvira postaje uobičajena praksa. Istraživanja su pokazala da 84% tvrtki koristi neki sigurnosni okvir. Općenito industrije u kojima je najzastupljenije usvajanje sigurnosnog okvira su bankarstvo i financije, informacijska tehnologija, vlada i proizvodnja sa stopama usvajanja iznad 80%. Zatim slijedi obrazovanje ima stopu usvajanja sa 77% i zdravstvo sa 61% i ostalo prikazano na slici 2.

SLIKA 2: STOPE USVAJANJA SIGURNOSNIH OKVIRA

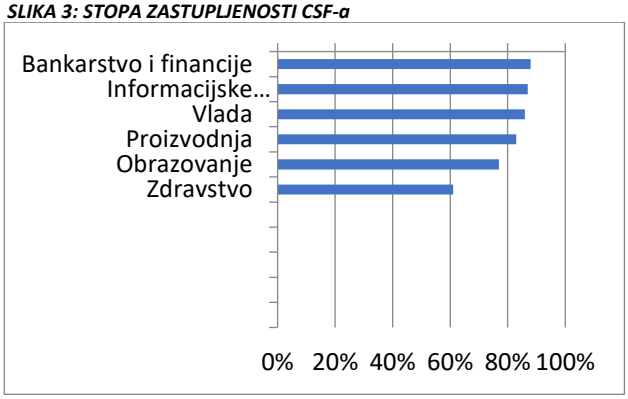


Izvor: izrada autora

Mnogi sigurnosni okviri imaju jaku reputaciju u određenim područjima. CSF kao inicijativa vlade SAD-a sa stopom usvajanja od 29%, PCI povezan s maloprodajom koja se oslanja na transakcije kreditnim karticama ima stopu usvajanja 47%, dok je ISO najpoznatiji međunarodno sa 32% stope usvajanja.

Istraživanje provedeno 2016. pokazuje da postoji široki raspon industrija čije su tvrtke usvojile CSF osim vlade čija je stopa zastupljenosti 14%. Primjenu vidimo u bankarstvu 19%, informacijskim tehnologijama 14%, zdravstvu 12%, obrazovanju 5% i još mnogo toga prikazano na slici 3. [3]

SLIKA 3: STOPA ZASTUPLJENOSTI CSF-a



Izvor: izrada autora

2.2. Koraci implementacije kibernetičke sigurnosti

Osim okvira kibernetičke sigurnosti, okvir za poboljšanje kritične infrastukture kibernetičke sigurnsti pruža i osnovne smjernice za implementaciju kroz proces od sedam koraka.

Prvi korak je određivanje prioriteta i opsega („Odredite prioritet i opseg“). U ovom koraku potrebno je identificirati poslovne ciljeve i najvažnije prioritete organizacije kako bi u potpunosti razmjeli organizacijski pristup prema procjeni riziku i određivanju prioriteta sigurnosnih aktivnosti. Omogućava organizacijama donošenje strateških odluka u vezi opesga sustava i sredstava koje podržavaju odabrane poslovne procese unutar organizacije.

Nakon određivanja ciljeva i prioriteta organizacije slijedi orijentacijski korak („Orijentacija“). U obzir se uzimaju tehnologije i kroz ovaj korak organizacije identificiraju prijetnje i ranjivosti sustava određenog u prvom koraku.

Treći korak je „Kreiranje trenutnog profila organizacije“. Uspostavom trenutnog profila organizacije dobivaju uvid u trenutačno stanje kibernetičke sigurnosti unutar organizacije. Samim stvaranjem trenutnog Profila organizacije, ona može otkriti da već postiže željene ishode, utvrditi da ima mjesta za poboljšanje, osmisliti plan za jačanje trenutnih praksi, otkriti preveliko ulaganje u postizanje određenih ishoda i iskoristiti te informacije kako bi promijenila prioritete resursa i prakse.

Sljedeći korak („Provedite procjenu rizika“) je provođenje procjene rizika koristeći trenutačne metodologije organizacije za upravljanje rizikom. Te informacije su ključne za peti korak implementacije.

Nadalje, u petom koraku („Kreiranje ciljanog profila“) potrebno je odrediti profil koji organizacija želi postići. Profil ciljanog stanja bazira se na procjeni okvirnih kategorija i podkategorija koje opisuju željene ishode kibernetičke sigurnosti.

U šestom koraku („Odredite, analizirajte i odredite prioritete praznina“) organizacije provode analizu nedostataka s ciljem poboljšanja trenutnog stanja. Te praznine se identificiraju preklapanjem trenutnog i ciljanog profila.

Zadnji, sedmi korak je „Provedba akcijskog plana“. Uzimajući u obzir informacije sakupljene u prethodnim koracima poduzimaju se potrebne radnje kako bi se popunile identificirane praznine i kreće se s radom na postizanju ciljanog profila. [5]

2.3. Razine zrelosti implementacije u NIST-u

Okvir za kibernetičku sigurnost se može implementirati na nekoliko razina koje pomažu pri provođenju procjene i planiranja aktivnosti kibernetičke sigurnosti. Svaka razina opisuje koje atribute treba uzeti u obzir pri izradili ciljanog profila ili dovršavanja trenutnog profila. Tri kategorije koje opisuju razine su Proces upravljanja rizikom, Program integriranog upravljanja rizicima i Vanjsko sudjelovanje.

Proces upravljanja rizikom razmatra razinu do koje su definirane i primjenjene prakse upravljanja rizicima kibernetičke sigurnosti organizacije.

Program integriranog upravljanja rizicima uzima u obzir svijest o riziku kibernetičke sigurnosti na razini cijele organizacije. Razine unutar ove kategorije se povečavaju ovisno o definiranju, implementaciji i prilagođavanju procesa i procedura temeljenih na riziku koje je odobrio menadžment.

Vanjsko sudjelovanje je kategorija koja ovisi o razini aktivnog dijeljenja informacija organizacije s vanjskim partnerima kako bi se poboljšala sigurnost i informiranost o zapažanjima i događajima. [5]

TABLICA 1: RAZINE ZRELOSTI IMPLEMENTACIJE U NIST-U

Razina implementacije	Kategorija		
	Proces upravljanja rizikom	Program integriranog upravljanja rizicima	Vanjsko sudjelovanje
Djelomična	Prakse upravljanja rizicima nisu formalizirane, prioriteti kibernetičke sigurnosti nisu direkto utemeljini na ciljevima organizacije ili rizicima.	Ograničena svijest i nepravilno upravljanje rizikom kibernetilčke sigurnosti. Organizacija možda nema procese koji omogućuju dijeljenje informacija o kibernetičkoj isgurnosti unutar organizacije.	Organizacija možda nema uspostavljene procese za sudjelovanje u koordinaciji ili suradnji s drugim subjektima.
Obavješteni o riziku	Prakse upravljanja rizikomodobrava uprava, ali se ne mogu uspostaviti kao politika organizacije. određivanje prioriteta aktivnosti kibernetičke sigurnosti utemeljene su na ciljevima organizacije, okruženosti prijetnjama	Na organizacijskoj razini postoji svijet o rizicima kibernetičke sigurnosti, ali pristup upravljanja tim rizikom nije uspostavljen na razini cijele organizacije. Definirani su i implementirani procesi i postupci odobreni od strane uprave i temeljeni na postojećim rizicima. Osoblje ima odgovarajuće resurse za obavljanje svojih dužnosti kibernetičke sigurnosti.	Organizacija zna svoju ulogu u širem ekosustavu, ali nije formalizitala svoje sposobnosti za interakciju i dijeljenje informacija izvana.
Ponovljivo	Organizacijske prakse upravljanja rizicima službeno su odobrene i izložene kao politika, redovito se ažururaju na temelju primjene procesa upravljanja rizicima na promjene u zahtjevima poslovanja	Organizacijske prakse upravljanja rizicima službeno su odobrene i izražene kao politika. Organizacijske prakse kibernetičke sigurnosti redovito se ažuriraju na temelju primjene procesa upravljanja rizicima s obzirom na zahtjeve poslovanja i promjenjive prijetnje.	Organizacija razumije svoje ovisnosti i pratnere te prima informacije od tih partnera koje omogućuju suradnju i donošenje odluka o upravljanju na temelju rizika unutar organizacije kao odgovor na događaje.
Prilagodljivo	Organizacija prilagođava svoje prakse kibernetičke sigurnosti na temelju naučenih lekcija i prediiktivnih pokazatelja izvedenih iz prethodnih i trenutnih aktivnsoti kibernetičke sigurnosti. Kroz proces kontinuiranog poboljšanja koji uključuje napredne tehnologije i prakse kibernetičke sigurnosti, organizacija se aktivno prilagođava promjenjivom okruženju kibernetičke sigurnosti i pravodobno odgovara na rastuće i sofisticirane prijetnje	Postoji organizacijski pristup upravljanju rizikom kibernetičke sigurnosti koji koristi politike, procese i postupke temeljene na riziku za rješavanje potencijalnih događaja kibernetičke sigurnosti. Upravljanje rizikom kibernetičke sigurnosti dio je organizacijske kulture i razvija se iz svijesti o prethodnim aktivnostima, informacijama koje dijele drugi izvori i stalne svijesti o aktivnostima na njihovim sustavima i mrežama.	Organizacija upravlja rizikom i aktivno dijeli informacije s partnerima kako bi se osiguralo da se točne, aktualne informacije distribuiraju i koriste za osiguravanje kibernetičke sigurnosti prije nego što dođe do događaja kibernetičke sigurnosti.

Izvor: ISACA © 2014 - Implementing the NIST Cybersecurity Framework, Figure 13

3. Zašto koristiti NIST okvir?

Prema NIST službenoj stranici okvir je prilagođen za organizacije svih veličina, sektora i zrelosti, te ga je moguće prilagoditi svim potrebama organizacija. On ne nalaže organizacijama kako da postignu rezultate te time omogućuje skalabilnost. Ovisno o proračunu kojim organizacija raspolaže ona može pristupiti ishodu na način koji je za njih izvediv.

NIST okvir pruža okvirne smjernice uključujući najbolje prakse koje pomažu organizacijama u provedbi dugoročnih sigurnosnih postupaka i upravljanja rizicima. Osmišljen je kako bi nadopunio, a ne zamijenio, program kibernetičke sigurnosti i procese upravljanja rizicima. Osim što to pridonosi sveukupnoj sigurnosti poslovnih procesa, pridonosi smanjenju troškova u budućnosti u smislu smanjenja broja potencijalnih incidenata kibernetičke sigurnosti.

Također, olakšava usvajanje novih sigurnosnih procedura koje je ključno za osiguravanje usklađenosti sa zakonima i protokolima o kibernetičkoj sigurnosti. NIST okvir je posebno važan za poslovna partnerstva jer neke organizacije ne žele poslovati s organizacijama koje nisu usvojile smjernice NIST-a.

Sveukupno komponente donose pomoć u sagledavanju konteksta o tome kako organizacija gleda na upravljanje rizikom kibernetičke sigurnosti, usmjeravaju organizacije da razmotre odgovarajuće razine strogosti za svoj program kibernetičke sigurnosti te se može koristiti kao komunikacijski alat za raspravu o prioritetima misije, sklonosti riziku i proračunu.

Jedna loša strana NIST okvira je nedostatak automatizacije implementacije i nedostatak resursa. Okvir ne sadrži puno informacija kako automatizirati neke od koraka, a kako se svijet kibernetičke sigurnosti nastavlja razvijati i mijenjati, automatizacija postaje ključna za raspodjelu resursa i bolji sigurnosni položaj. Također, drugi nedostatak je nemogućnost mjerenja kibernetičkog rizika i napredaka u stvarnim terminima. Najveći problem danas je to što NIST ima malo toga za reći o prijetnjama koje nastaju korištenjem okruženja u oblacima i osiguranju sustava računalstva u oblaku.

Bez obzira na ove nedostatke, nema većih razloga da se ne implementira NIST okvir za kibernetičku sigurnost kao početna točka u uspostavi kibernetičke sigurnosti, čak i ako postavljanje može uključivati neke početne prepreke. Organizacija može nastojati ići iznad i dalje od mjera navedenih u okviru ako smatra da je potrebno kako bi zaštitili svoje podatke, podatke klijenata i pojednostavili organizaciju. [2][5]

4. Zaključak

Nagli uspon digitalne aktivnosti u modernom životu stvorio je potrebu uspostave snažne kibernetičke sigurnosti. Kako bi pomogao tim organizacijama NIST je razvio okvir za kibernetičku sigurnost koji je moćan alat za organizaciju i poboljšanje trenutnog programa ili opće uspostave kibernetičke sigurnosti unutar organizacije.

Sastoji se od tri komponente: jezgra okvira, stupnjevi implementacije okvira i profili okvira. Jezgra okvira pokriva pet važnih područja odnosno funkcija kibernetičke sigurnosti („Identifikacija“, „Zaštita“, „Detekcija“, „Odgovor“, „Oporavak“) koje se sastoje od niza instrukcija i najboljih praksi kao pomoć organizacijama pri uspostavi kostura kibernetičke sigurnosti. Stupnjevi implementacije okvira i profili okvira sadrže set preporuka i standarda koji pripremaju organizacije za bolju pripremljenost, lakšu identifikaciju i detekciju incidenata kibernetičke sigurnosti. Organizacija može sama birati kategorije i razine koje želi implementirati u svoje prakse i poslovne procese. Okvir je vrlo fleksibilan i skalabilan te ga je moguće prilagoditi svim potrebama i mogućnostima organizacije, odnosno organizacija može sama birati svoj ciljani profil. Iako je prvobitno bio namijenjen za privatni sektor u SAD-u i operatora kritične infrastrukture, njegova korisnička baza je narasla na organizacije diljem svijeta.

Unatoč postojanju nekih prepreka kao što su manjak resursa, automatizacije koraka implementacije i najveće prepreke minimalne informiranosti o prijetnjama korištenja korištenjem oblaka, implementacija NIST okvira je vrlo dobra polazišna točka pri uspostavi kibernetičke sigurnosti i upravljanju rizicima kibernetičke sigurnosti.

Literatura

[1] CISCO stranica https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

[2] CyberSaint Security stranica, https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework

[3] Dimensional Research, sponsored by Tenable Network Security: Trends in Security Framework Adoption: A Survey of IT and Security Professionals, March 2016

[4] ISACA © 2014 - Implementing the NIST Cybersecurity Framework

[5] Službena stranica vlade SAD-a, https://www.nist.gov