URED ZA REVIZIJU INSTITUCIJA BIH
КАНЦЕЛАРИЈА ЗА РЕВИЗИЈУ ИНСТИТУЦИЈА БИХ
AUDIT OFFICE OF THE INSTITUTIONS OF BOSNIA AND HERZEGOVINA

www.revizija.gov.ba

Broj: 05-16-1-1431-11/22
Datum: 15. 12. 2022. godine

Povjerenstvo za financije i proračun
Zastupnički dom Parlamentarne skupštine Bosne i Hercegovine
Trg BiH 1
71000 Sarajevo

Predmet: Dostava Izvješća revizije učinka

Cijenjeni,

Sukladno članku 16. Zakona o reviziji institucija BiH (»Službeni glasnik BiH«, broj: 12/06), u privitku dopisa dostavljamo Vam Izvješće o provedenoj reviziji učinka na temu „Aktivnosti institucija BiH na osiguranju temeljnih pretpostavki za kibersigurnost".

S poštovanjem

GLAVNI REVIZOR

Hrvoje Tvrtković

Privitak:
- Izvješće revizije učinka

Dostavljeno:
- Povjerenstvu za financije i proračun Zastupničkog doma Parlamentarne skupštine Bosne i Hercegovine
- a/a.

URED ZA REVIZIJU INSTITUCIJA BIH
КАНЦЕЛАРИЈА ЗА РЕВИЗИЈУ ИНСТИТУЦИЈА БИХ
AUDIT OFFICE OF THE INSTITUTIONS OF BOSNIA AND HERZEGOVINA

www.revizija.gov.ba

IZVJEŠTAJ REVIZIJE UČINKA

„AKTIVNOSTI INSTITUCIJA BOSNE I HERCEGOVINE NA OSIGURANJU TEMELJNIH PRETPOSTAVKI ZA KIBERSIGURNOST“

Broj: 05-16-1-1431/22

Sarajevo, prosinac 2022. godine

Aktivnosti institucija BiH na osiguranju temeljnih pretpostavki za kibersigurnost

Ured za reviziju institucija BiH je proveo reviziju učinka na temu: „Aktivnosti institucija BiH na osiguranju temeljnih pretpostavki za kibersigurnost". Revizija je provedena sukladno Zakonu o reviziji institucija BiH, Međunarodnim standardima vrhovnih revizijskih institucija – ISSAI, INTOSAI smjernicama i metodologiji za rad revizije učinka vrhovnih revizijskih institucija u BiH.

Ured za reviziju institucija BiH je proveo reviziju s ciljem provjere jesu li institucije BiH efikasne u poduzimanju aktivnosti s ciljem osiguranja temeljnih pretpostavki za kibersigurnost.

Nalazi revizije ukazuju da institucije BiH nisu bile efikasne u poduzimanju aktivnosti s ciljem osiguranja temeljnih pretpostavki za kibersigurnost. Nedostaje strateški i zakonski okvir kibersigurnosti, a nije uspostavljen ni Tim za računalne incidente za institucije BiH. Institucije BiH su imale pasivan pristup u donošenju akata upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću i/ili standardima upravljanja informacijskom sigurnošću. Samo 14 od 68 institucija BiH je donijelo akte upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću.

Posljedice nedostatka temeljnih pretpostavki za kibersigurnost ugrožavaju poslovanje javne uprave i mogu dovesti do otuđenja podataka i financijskih sredstava neophodnih za funkcioniranje zemlje i svakodnevnog života građana.

Izvješće revizije sadrži preporuke upućene Vijeću ministara BiH, Ministarstvu komunikacija i prometa BiH, Ministarstvu sigurnosti BiH i institucijama BiH. Realizacijom preporuka trebalo bi se pridonijeti osiguranju temeljnih pretpostavki za kibersigurnost i unaprjeđenju kiberzaštite u institucijama BiH. Implementacija preporuka trebala bi doprinijeti i realizaciji Ciljeva održivog razvoja, a naročito ciljevima održivog investiranja u infrastrukturu i inovacije i razvoju učinkovitih, odgovornih i transparentnih institucija i omogućavanju pristupa informacijama.

Ured za reviziju je, sukladno odredbama Zakona o reviziji institucija BiH, dostavio Nacrt izvješća institucijama koje su bile obuhvaćene provedenom revizijom. Ovim institucijama je ostavljena mogućnost da daju svoje komentare i primjedbe na nalaze i zaključke obavljene revizije. Nakon toga je izrađeno konačno izvješće o provedenoj reviziji učinka.

GLAVNI REVIZOR

Hrvoje Tvrtković

ZAMJENIK GLAVNOG REVIZORA

Jasmin Pilica

ZAMJENIK GLAVNOG REVIZORA

Ranko Krsman

Kazalo

Korištene skraćenice

Skraćenica	Puni naziv
AJN	Agencija za javne nabave Bosne i Hercegovine
AZOP	Agencija za zaštitu osobnih podataka Bosne i Hercegovine
BiH	Bosna i Hercegovina
CERT	Tim za odgovor na računalne incidente
Direktiva NIS	Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije
EK	Europska komisija
EU	Europska unija
GT	Generalno tajništvo Vijeća ministara Bosne i Hercegovine
ISO	Međunarodna organizacija za standardizaciju (International Organization for Standardization)
IT	Informacijske tehnologije
MFT	Ministarstvo financija i trezora Bosne i Hercegovine
MKP	Ministarstvo komunikacija i prometa Bosne i Hercegovine
MS	Ministarstvo sigurnosti Bosne i Hercegovine
OSCE	Organizacija za sigurnost i suradnju u Europi
Politika upravljanja informacijskom sigurnošću	Politika upravljanja informacijskom sigurnošću u institucijama BiH za razdoblje 2017. – 2022. godina
RAK	Regulatorna agencija za komunikacije Bosne i Hercegovine
RH	Republika Hrvatska
Sjevernoatlantski savez	NATO
Služba za e-vladu pri GT	Služba za održavanje i razvoj elektroničkog poslovanja i e-vlade pri Generalnom tajništvu Vijeća ministara Bosne i Hercegovine
Sl. gl. BiH	Službeni glasnik Bosne i Hercegovine
UNDP	Program Ujedinjenih naroda za razvoj
VM	Vijeće ministara Bosne i Hercegovine

Izvršni sažetak

Ured za reviziju institucija BiH je proveo reviziju učinka s ciljem da utvrdi jesu li institucije BiH efikasne u poduzimanju aktivnosti s ciljem osiguranja temeljnih pretpostavki za kibersigurnost.

U nastavku su najvažniji nalazi i preporuke revizije:

- Aktivnosti na donošenju strateškog i zakonskog okvira kibersigurnosti pokrenute su još 2017. godine, a pet godina nakon toga, aktivnosti nisu okončane i strateški i zakonski okvir kibersigurnosti još uvijek nije donesen.
- Ni nakon pet godina od zaduženja VM-a, odgovorne institucije BiH nisu izradile strateški i zakonski okvir kibersigurnosti i izvjesno je da dinamika aktivnosti odgovornih institucija BiH neće osigurati završetak ovih aktivnosti u trenutno definiranom roku.
- Na razini institucija BiH ni nakon pet godina od donošenja Odluke VM-a o određivanju CERT-a za institucije BiH nije uspostavljen CERT koji bi učinkovito koordinirao i upravljao pružanjem odgovora na računalne incidente.
- Iako je VM zadužio MS da u kratkom roku poduzme aktivnosti s ciljem uspostave CERT-a za institucije BiH, MS za pet godina nije osigurao potrebne uvjete za uspostavu CERT-a.
- Institucije BiH su imale pasivan pristup u donošenju akata upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću i/ili standardima upravljanja informacijskom sigurnošću.
- Samo 14 od 68 institucija BiH je donijelo akte upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću.

Ured za reviziju institucija BiH je definirao preporuke s ciljem da se pridonese osiguranju temeljnih pretpostavki za kibersigurnost i unaprjeđenju kiberzaštite u institucijama BiH. Preporuke su upućene Vijeću ministara BiH, Ministarstvu komunikacija i prometa BiH, Ministarstvu sigurnosti BiH i institucijama BiH.

Preporuka Vijeću ministara BiH

- Definirati rokove za pripremu i odgovornost za izvještavanje o procesu pripreme relevantnih akata kibersigurnosti.

Preporuke Ministarstvu komunikacija i prometa BiH i Ministarstvu sigurnosti BiH

- Žurno okončati pripremu prijedloga relevantnih propisa kibersigurnosti i dostaviti ih Vijeću ministara na usvajanje.
- Izvijestiti VM o realizaciji Politike upravljanja informacijskom sigurnošću u institucijama BiH.

Preporuke Ministarstvu sigurnosti BiH

- Žurno okončati pripremu prijedloga strateškog okvira kibersigurnosti i dostaviti ga Vijeću ministara na usvajanje.
- Žurno osigurati organizacijske pretpostavke za formiranje Tima za odgovor na računalne incidente za institucije BiH.

Preporuka institucijama BiH

- Žurno donijeti akte upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću.

1. UVOD

1.1. Pozadina problema i motivi za studiju

Svakodnevna upotreba informacijskih tehnologija otvara čitav niz novih mogućnosti, ali i prijetnji od kibernapada i kiberkriminala od kojih posljedice mogu imati zastrašujuće implikacije na društvo i gospodarstvo.[1] Kibersigurnost predstavlja vrlo važnu komponentu u korištenju informacijskih tehnologija i zaštiti podataka od mogućih krađa, povrede informacijske sigurnosti i raznih malverzacija koje imaju negativan društveni, gospodarski i politički učinak. Značaj kibersigurnosti je posebno došao do izražaja u vrijeme epidemije korona virusa zbog povećane ovisnosti o informacijskoj tehnologiji.

Bosna i Hercegovina (BiH) značajno zaostaje za ostalim zemljama Europe u digitalnoj transformaciji društva pa tako i u kibersigurnosti.[2] Povećan broj kiberprijetnji i nedostaci u kiberzaštiti u BiH su teme u fokusu medija.[3] U BiH ne postoje službeni podatci o broju i vrsti kibernapada. Neslužbeni podatci govore da se broj kibernapada u BiH povećao za 1300 puta na tjednoj osnovi. Od 68 institucija BiH, 24 institucije BiH su imale zabilježene kibernapade.[4] Koliko je ovaj problem aktualan govori u prilog činjenica da su u tijeku pripreme ovog izvješća zabilježeni kibernapadi na institucije BiH.[5] Posljednji zabilježeni kibernapad na institucije BiH obustavio je rad uposlenih, a onemogućio pristup službenim stranicama skoro mjesec dana.[6]

Javna uprava je jedan od ključnih čimbenika za razvoj informacijskog društva i kao takva snosi odgovornost za kibersigurnost. BiH se sukladno svom opredjeljenju za pristupanje Europskoj uniji (EU) obvezala na unaprjeđenje kibersigurnosti. U BiH, bez obzira na opredjeljenje za pristupanje EU, još uvijek nisu osigurane temeljne pretpostavke za kibersigurnost,[7] iako je središnji pravni akt o kibersigurnosti EU donesen još 2016.

---

[1] Procjena je da će financijski učinak kiberkriminala na svjetsko gospodarstvo dosegnuti šest bilijuna američkih dolara godišnje do 2021., podatci dostupni na linku: The 2020 Official Annual Cybercrime Report - Herjavec Group

[2] BiH se nalazi na devetom mjestu u svijetu po riziku od kiberprijetnji ili na 86. mjestu po kibersigurnosti i značajno zaostaje za zemljama iz okruženja, dostupno na linku: https://cybernews.com/news/should-you-worry-100-countries-ranked-by-cyber-safety/

[3] BiH jedina država bez strategije o zaštiti računalnih podataka - Pogled.ba
Cyber napadi su realna i postojeća prijetnja za BiH | TEME | Al Jazeera
https://atlantskainicijativa.org/cyber-napadi-kao-rastuca-teroristicka-prijetnja-nespremnim-balkanskim-zemljama/
https://balkans.aljazeera.net/news/technology/2021/10/29/bosna-i-hercegovina-medju-najmanje-sigurnim-od-cyber-kriminala
Ugroženi privatni podaci 15.000 osoba iz BiH: Hakerski napad na servere Crvenog krsta | DEPO Portal
https://www.klix.ba/vijesti/bih/arnautovic-dobili-smo-informaciju-o-cyber-napadima-na-centralnu-izbornu-komisiju/220527130

[4] Prema podatcima iz Upitnika revizije učinka na temu kibersigurnost. Od 73 institucije BiH kojim je poslan Upitnik, 68 institucija je dostavilo odgovore na Upitnik.

[5] Izveden hakerski napad na servere Parlamenta BiH - www.vecernji.ba
SIPA odbila hakerski napad na ovu policijsku agenciju! (avaz.ba)

[6] https://inforadar.ba/institucije-bih-u-blokadi-vec-17-dana-server-cik-a-moguci-glavi-cilj-hakerskog-napada/
https://bljesak.info/vijesti/flash/zaposlenici-u-drzavnim-institucijama-vec-dva-tjedna-ne-rade-nista-zbog-hakerskog-napada/394589

[7] U Izvješću o napretku BiH za 2021. godinu navedeno je da nije postignut napredak u oblasti kibersigurnosti. Izvješće dostupno na linku: izvjestaj-o-bosni-i-hercegovini-za-2021-godinu_1636467943.pdf (dei.gov.ba)

godine.[8] Donošenjem odluka i zaključaka iz oblasti kibersigurnosti 2017. godine, Vijeće ministara BiH (VM) se opredijelilo za jačanje kibersigurnosti institucija BiH, ali još uvijek nije donesen strateški, zakonski i organizacijski okvir kibersigurnosti.[9]

Institucije BiH za poslovanje koriste informacijske sustave čija sigurnost je od izuzetnog značaja. Ugrožavanjem sigurnosti informacijskih sustava institucija BiH nastupile bi ozbiljne posljedice za funkcioniranje javne uprave i gospodarstva. Na primjer, ugrožavanjem sigurnosti sustava e-vlada uzrokovalo bi zastoj u radu VM-a i moglo bi se kasniti u donošenju važnih odluka za javnu upravu i građane. Napad na informacijski sustav Ministarstva financija i trezora BiH (MFT) ugrozio bi evidencije svih financijskih transakcija institucija BiH i mogao bi uzrokovati obustavu svih plaćanja iz proračuna BiH.

Rezultati predstudijskih istraživanja Ureda za reviziju institucija BiH također su ukazali na probleme u uspostavi kibersigurnosti institucija BiH.

Imajući na umu sve navedeno, Ured za reviziju institucija BiH donio je Odluku o provedbi revizije učinka u oblasti kibersigurnosti institucija BiH.

1.2. Cilj, obujam i ograničenja revizije

1.2.1. Cilj revizije

Cilj revizije je pokazati jesu li institucije BiH efikasne u poduzimanju aktivnosti s ciljem osiguranja temeljnih pretpostavki za kibersigurnost.

Svrha revizije je doprinijeti stvaranju kiberzaštite i jačanju kiberotpornosti institucija BiH kako bi se zaštitile institucije BiH, građani i ugled države.

Provedba ove revizije trebala bi doprinijeti realizaciji ciljeva održivog razvoja, a naročito ciljevima održivog investiranja u infrastrukturu i inovacije (cilj 9.) i razvoju učinkovitih, odgovornih i transparentnih institucija i omogućavanju pristupa informacijama (cilj 16.).

1.2.2. Obujam i ograničenja revizije

Predmet revizije su aktivnosti institucija BiH na osiguravanju temeljnih pretpostavki za kibersigurnost. U kontekstu ove studije temeljne pretpostavke se odnose na osiguravanje strateškog i zakonskog okvira kibersigurnosti, Tima za odgovor na računalne incidente (CERT) i sustava upravljanja informacijskom sigurnošću u institucijama BiH. S obzirom da je oblast kibersigurnosti široko područje revizija se nije bavila drugim mogućim pretpostavkama za kibersigurnost.

Analizirale su se aktivnosti odgovornih institucija BiH iz oblasti kibersigurnosti u osiguranju temeljnih pretpostavki za kibersigurnost. Promatrale su se aktivnosti VM-a koji je odgovoran za donošenje strateških odluka i zakonskih propisa u oblasti kibersigurnosti, određivanje rokova i odgovornosti za izvještavanje. Predmet analiza bile su i aktivnosti

[8] Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije je prvi zakon o kibersigurnosti na razini EU i predstavlja glavni stup Strategije za kibersigurnost EU iz 2013. godine.

[9] Odluka o određivanju Tima za odgovor na računalne incidente za institucije BiH, Odluka o usvajanju Politike upravljanja informacijskom sigurnošću u institucijama BiH za razdoblje 2017. – 2022. godine i Zaključak VM-a da se intenziviraju aktivnosti na izradi Strategije kibersigurnosti.

institucija BiH na uspostavi preventivnih mjera kibersigurnosti i donošenju akata upravljanja informacijskom sigurnošću. Analizirale su se informacije iz upitnika, kojim su ispitane 73 institucije BiH[10], a koje su relevantne za uspostavu kibersigurnosti.

Detaljnije su se analizirale aktivnosti institucija iz uzorka na uspostavi preventivnih mjera kibersigurnosti i donošenju akata upravljanja informacijskom sigurnošću. Implementacija preventivnih mjera kibersigurnosti koje su poduzete u institucijama iz uzorka nisu bile predmetom detaljnije analize.

U uzorak su izabrane institucije prema više kriterija. Ministarstvo komunikacija i prometa BiH (MKP) i Ministarstvo sigurnosti BiH (MS) su odgovorne institucije BiH u oblasti kibersigurnosti. Agencija za javne nabave BiH (AJN) je institucija visokog sigurnosnog rizika jer su informacijski sustavi otvoreni za sve sudionike javnih nabava u BiH. Agencija za zaštitu osobnih podataka BiH (AZOP) je institucija koja posjeduje registre osobnih podataka zbog čega je izuzetno važna kiberzaštita i primjer dobre prakse. Ministarstvo financija i trezora BiH (MFT) je institucija u kojoj je zabilježen kibernapad[11]. MFT također upravlja informacijskim sustavima za plaćanja iz proračuna institucija BiH u milijunskim iznosima. Generalno tajništvo VM BiH (GT) upravlja sustavom e-vlade čije servise koristi oko 58 institucija BiH. GT, između ostalog, utvrđuje način zaštite sustava e-vlade i pravila korištenja servisa e-vlade za korisnike. Regulatorna agencija za komunikacije BiH (RAK) je institucija koja po poslovima koje obavlja spada u kritičnu infrastrukturu i institucija koja je nedavno donijela okvir upravljanja informacijskom sigurnošću.

Revizija se nije bavila aktivnostima institucija BiH u oblasti kiberkriminala. Revizija nije analizirala regulativu koja se dodiruje sa kibersigurnošću, kao što je regulativa koja se odnosi na elektroničko poslovanje, komunikacije i zaštitu osobnih podataka. Nisu analizirane aktivnosti institucija BiH u uspostavi kibersigurnosti podataka koji su zaštićeni oznakom tajnosti.

Nije bilo ograničenja revizije.

1.3. Revizijska pitanja i kriteriji revizije

Revizija će dati odgovor na jedno glavno pitanje i tri revizijska potpitanja. Glavno revizijsko pitanje je:

Jesu li institucije BiH efikasne u poduzimanju aktivnosti s ciljem osiguranja temeljnih pretpostavki za kibersigurnost?

Za što bolje razumijevanje i analizu problema, te da bi se olakšalo prikupljanje potrebnih podataka, definirana su tri revizijska potpitanja:

1. Je li donesen strateški i zakonski okvir kibersigurnosti institucija BiH?
2. Je li uspostavljen Tim za odgovor na računalne incidente za institucije BiH?
3. Jesu li doneseni akti upravljanja informacijskom sigurnošću u institucijama BiH?

[10] Od 73 ispitane institucije svoje odgovore je dostavilo 68 institucija. Odgovore nisu dostavile Agencija za antidoping kontrolu BiH, Agencija za prevenciju korupcije i koordinaciju borbe protiv korupcije BiH, Centar za uklanjanje mina u BiH, Institut za nestale osobe BiH i Služba za zajedničke poslove institucija BiH. Upitnikom nisu ispitane Obavještajno-sigurnosna agencija i Ured za reviziju institucija BiH.

[11] Izvršeno nekoliko napada na e-mail i web stranicu MFT.

Kriteriji

Kriteriji revizije koje smo koristili u procjeni predmeta revizije utemeljeni su na Direktivi o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS direktiva), preporukama Europske komisije (EK) u oblasti kibersigurnosti, Odluci VM-a o određivanju CERT-a za institucije BiH iz 2017. godine, Odluci VM-a o usvajanju Politike upravljanja informacijskom sigurnošću iz 2017. godine, Zaključku VM-a iz 2017. godine kojim se intenziviraju aktivnosti na izradi strateškog okvira kibersigurnosti, Smjernicama za strateški okvir kibersigurnosti u BiH, Izvješću o ocjeni spremnosti za uspostavljanje CERT mreže u BiH, Pregledu kapaciteta kibersigurnosti u BiH i razgovorima sa predstavnicima institucija iz uzorka i akademskoj literaturi o kibersigurnosti i informacijskoj sigurnosti.[12]

Pod efikasnim poduzimanjem aktivnosti u kontekstu ove studije se podrazumijeva blagovremen[13] i proaktivan[14] odnos institucija BiH u poduzimanju aktivnosti potrebnih za osiguranje temeljnih pretpostavki za kibersigurnost.

Kriterij za prvo revizijsko potpitanje:[15]

Donesen je strateški okvir kojim se osigurava sustavni pristup u izgradnji kibersigurnosti i podiže svijest o važnosti kibersigurnosti u institucijama BiH u skladu sa definiranim rokovima. Donesen je zakonski okvir kojim se osigurava provedba mjera za postizanje visoke zajedničke razine mrežne i informacijske sigurnosti i nadležna tijela za provedbu i nadzor mjera mrežne i informacijske sigurnosti u institucijama BiH u skladu sa definiranim rokovima.

---

[12] Arbanas K. "Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti" Disertacija, Sveučilište u Zagrebu, Fakultet organizacije i informatike, 2021. godine

[13] U skladu sa definiranim rokovima VM-a na koja se referiramo u izvorima kriterija za revizijska pitanja.

[14] U konstantnom tijeku aktivnosti i inicijative na rješavanju problema.

[15] VM je u 2017. godini donio zaključak kojim se zadužuje MS da intenzivira aktivnosti na izradi Strategije kibersigurnosti. Odlukom VM-a o usvajanju Politike upravljanja informacijskom sigurnošću iz 2017. godine zadužuju se MKP i MS da izrade zakon o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava. U Programu rada MKP-a za 2018. godinu jedna od aktivnosti je bila izrada Nacrta zakona o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava. VM je u 2019. godini nakon razmatranja Informacije o ispunjavanju pravnog kriterija institucija BiH u procesu pridruživanja EU zadužio MKP da do kraja 2019. godine dostavi VM-u na usvajanje Nacrt zakona o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava. Prema preporukama EK-a u oblasti kibersigurnosti BiH treba usvojiti strategiju kibersigurnosti, izraditi akcijske planove na svim razinama vlasti i usvojiti zakon o kibersigurnosti. Usvajanjem preporuka EK-a iz 2019. godine, VM je usvojilo i listu aktivnosti prema kojoj je prvobitni rok za realizaciju preporuka 2020. godina, a zatim 2021. / 2022. godina. Odgovorne institucije su MS i MKP. U Programu rada MS-a za 2021. godinu jedna od aktivnosti je bila izrada nacrta zakona o mrežnoj i informacijskoj sigurnosti u institucijama BiH.

Kriterij za drugo revizijsko potpitanje:[16]

Na razini institucija BiH je uspostavljen operativan CERT za institucije BiH koji provodi aktivnosti upravljanja i koordiniranja prevencije i zaštite od sigurnosnih rizika u informacijskim komunikacijskim sustavima institucija BiH i ostale značajne aktivnosti u osiguranju kibersigurnosti. Uspostavljena je mreža CERT-ova u BiH koja vrši razmjenu informacija o incidentima i doprinosi razvoju pouzdanja i povjerenja među sudionicima mreže u BiH, i ostvaruje suradnju sa EU CERT-om i Agencijom EU za mrežnu i informacijsku sigurnost. Navedena tijela su uspostavljena u skladu sa definiranim rokovima.

Kriterij za treće revizijsko potpitanje:[17]

Institucije BiH su proaktivno donosile akte upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću. Institucije BiH su izradile akte na temelju smjernica i/ili međunarodnih standarda informacijske sigurnosti s ciljem uspostave sustava upravljanja informacijskom sigurnošću. MKP i MS su pratili implementaciju Politike upravljanja informacijskom sigurnošću u institucijama BiH i o realizaciji redovno izvještavale VM.

1.4. Izvori informacija i metode revizije

Primarne metode revizije, koje je koristio revizijski tim u cilju osiguranja informacija za dobivanje odgovora na postavljena revizijska pitanja, su intervjui sa predstavnicima institucija BiH, ispitivanje kroz upitnik i dokumentarni pregledi.

Podatci dobiveni iz intervjua s predstavnicima institucija mjerodavnim za oblast kibersigurnosti i institucija iz uzorka su uspoređeni s podatcima iz prikupljene dokumentacije iz institucija iz uzorka, upitnika i drugih izvora. Podatci i informacije dobiveni iz dokumentarnog pregleda i intervjua s predstavnicima institucija iz uzorka su međusobno uspoređivani.

Podatci su prikupljani pregledom i analizom sadržaja dokumentacije institucija mjerodavnih u oblasti kibersigurnosti i institucija iz uzorka, pregledom i analizom

---

[16] Odlukom VM-a o određivanju CERT-a za institucije BiH iz 2017. godine MS je trebalo u roku od tri mjeseca dostaviti VM-u na usvajanje prijedlog dopuna Pravilnika o unutarnjoj organizaciji MS-a s ciljem uspostave CERT-a. Programom rada MS-a za 2017. godinu bila je planirana aktivnost izrada odluka i akata unutarnje organizacije s ciljem uspostave CERT-a. Aktivnosti na izradi odluke o uspostavljanju mreže CERT-ova je planirana u Programu rada MS-a za 2021. godinu. Prema preporukama EK-a u oblasti kibersigurnosti BiH treba uspostaviti CERT-ove, odrediti državna nadležna tijela i pojedinačne kontakt točke. Usvajanjem preporuka EK-a iz 2019. godine, VM je usvojio i listu aktivnosti prema kojoj je prvobitni rok za realizaciju preporuka 2020. godina, zatim 2021. godina, a odgovorna institucija je MS. Akcijskim planom reforme javne uprave 2018. – 2022. planirana je aktivnost uspostave CERT-a do kraja 2022. godine.

[17] Prema Politici upravljanja informacijskom sigurnošću iz 2017. godine preporuča se institucijama BiH da implementiraju politike upravljanja informacijskom sigurnošću na unaprijed izrađenim standardima u cilju uspostave sustava upravljanja informacijskom sigurnošću sukladno uočenim zahtjevima i potrebama svake institucije pojedinačno. Politikom upravljanja informacijskom sigurnošću su ponuđene osnovne smjernice za izradu akata na temelju međunarodnih priznatih standarda. MKP i MS su zaduženi za detaljnu izradu smjernica. MKP je predvodio aktivnosti i odlučilo se izraditi 11 smjernica u tri seta. Programom rada MKP-a za 2018. godinu planirana je izrada četiri smjernice, za 2019. godinu tri smjernice i za 2020. godinu preostale četiri smjernice. Odlukom VM-a MKP i MS su zaduženi da godišnje izvještavaju VM o realizaciji Politike upravljanja informacijskom sigurnošću.

informacija iz upitnika, pregledom i analizom pravnih i strateških propisa u oblasti kibersigurnosti i drugih značajnih propisa, dostupnih analiza i pretraživanjem i izučavanjem podataka i stručne literature koji su od značaja za ovu studiju. Podatci prikupljeni pregledom i analizom dokumentacije o uspostavi kibersigurnosti institucija iz uzorka su međusobno uspoređivani.

1.5. Struktura izvješća

U poglavlju jedan predstavljeni su motivi koji su opredijelili Ured za reviziju institucija BiH da provede reviziju učinka na temu kibersigurnost u institucijama BiH. Ovo poglavlje sadrži cilj, obujam i ograničenja revizije, revizijska pitanja, kriterije revizije, te izvore i metode revizije.

Kroz drugo poglavlje daju se podatci i informacije nužne za razumijevanje kibersigurnosti, regulativnog okvira, strateškog opredjeljenja i uloge mjerodavnih institucija u oblasti kibersigurnosti.

U poglavlju tri predstavljeni su osnovni nalazi revizije do kojih se došlo provedenim istraživanjima. Poglavlje 3.1. nudi nalaze revizije koji ukazuju na nedostatak strateškog i zakonskog okvira za uspostavu kibersigurnosti u institucijama BiH, u poglavlju 3.2. prezentirani su nalazi koji ukazuju na nedostatak CERT-a u institucijama BiH, a u poglavlju 3.3. prezentirani su nalazi koji ukazuju na pasivan pristup institucija BiH u donošenju akata upravljanja informacijskom sigurnošću.

Poglavlje četiri prezentira zaključke revizije koji daju odgovor na revizijska pitanja.

Preporuke Ureda za reviziju institucija BiH čijom bi se provedbom trebalo doprinijeti uspostavi kibersigurnosti u institucijama BiH dane su u petom poglavlju.

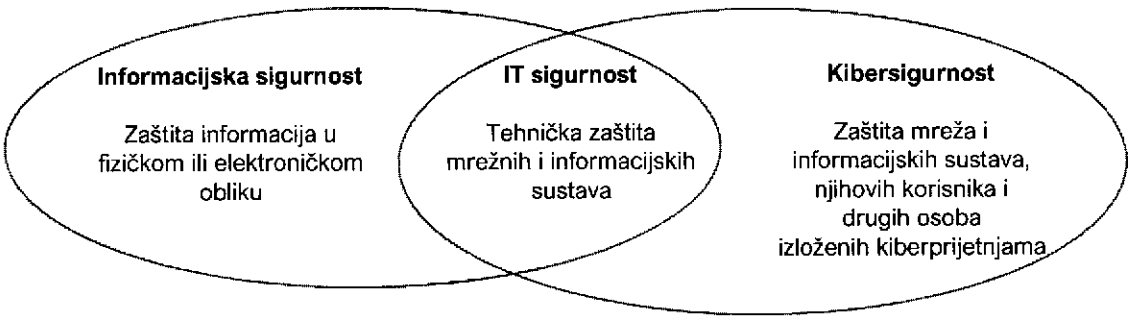
2. OPIS PREDMETA REVIZIJE

U ovom poglavlju predstavljeni su opći podatci bitni za razumijevanje kibersigurnosti, strateškog opredjeljenja za uspostavu kibersigurnosti, regulativnog okvira koji se odnosi na kibersigurnost u institucijama BiH i uloge mjerodavnih institucija BiH.

2.1. Kibersigurnost

Ne postoji općeprihvaćena, standardna definicija kibersigurnosti.[18] Kibersigurnost obuhvaća sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu. Kibersigurnost počiva na informacijskoj sigurnosti. Informacijska sigurnost obuhvaća aktivnosti kojima se postiže povjerljivost, cjelovitost i dostupnost informacija. Kibersigurnost obuhvaća isto, ali u kiberprostoru. Zaštita mrežnih i informacijskih sustava u kojima se informacije pohranjuju poznata je pod pojmom sigurnosti informacijskih tehnologija (IT sigurnost) i predstavlja jedan dio informacijske sigurnosti, odnosno kibersigurnosti koji se odnosi na tehničku zaštitu. Sljedeći grafikon prikazuje povezanost kibersigurnosti, informacijske i IT sigurnosti.

Grafikon 1.: Povezanost kibersigurnosti, informacijske sigurnosti i IT sigurnosti



Izvor: Europski revizorski sud

Kibersigurnost obuhvaća prepoznavanje, sprječavanje i otkrivanje kiberincidenata[19], pružanje odgovora na njih i oporavak od njih. Uspostavom kibersigurnosti u institucijama BiH sprječavaju se različiti incidenti, od slučajnog do namjernog otkrivanja informacija i osobnih podataka, zastoja u radu i nedostupnosti sustava koji su podrška građanima i poslovnim korisnicima.

2.2. Strateško opredjeljenje za kibersigurnost

Početni koraci u izgradnji kibersigurnosti su ostvareni potpisivanjem Konvencije o kibernetičkom kriminalu 2006. godine i Sporazuma o stabilizaciji i pridruživanju 2008. godine. Na putu ka EU BiH je preuzela obveze dostizanja određenih standarda u oblasti kibersigurnosti. Dvije najznačajnije regulative vezane za kibersigurnost na razini EU su Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih

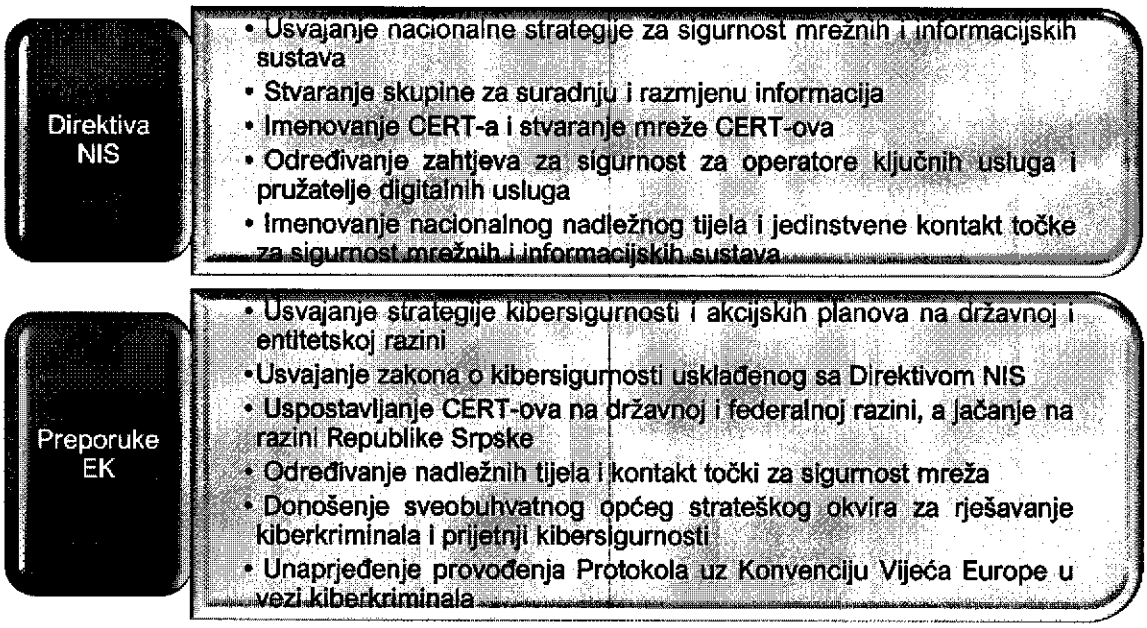
[18] Osim različitih definicija, postoje i različiti pojmovi kibersigurnosti. Kibernetička sigurnost je jedan od pojmova koji se poistovjećuje sa kibersigurnosti, iako postoje i različita tumačenja ova dva pojma. Ponekad se pojam kibersigurnosti poistovjećuje i sa informacijskom sigurnošću.

[19] Kiberincident je događaj koji izravno ili neizravno narušava ili ugrožava otpornost i sigurnost IT sustava i podataka koji se obrađuju, pohranjuju ili prenose u okviru tog sustava.

sustava širom Unije (Direktiva NIS),[20] donesena 2016. godine i Akt EU o kibersigurnosti,[21] donesen 2019. godine.

Usvajanjem preporuka EK, koje se upućuju BiH počev od 2016. godine, VM potvrđuje strateško opredjeljenje za uspostavu kibersigurnosti u institucijama BiH.[22] Sljedeći grafikon prikazuje preuzete obveze u oblasti kibersigurnosti.

Grafikon 2.: Preuzete obveze u oblasti kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Usvajanjem Akcijskog plana 1 reforme javne uprave za razdoblje 2018. – 2022. godina, VM je podržalo aktivnosti izrade zakonskih propisa zaštite informacijsko komunikacijske infrastrukture i elektroničkih usluga i uspostave CERT-a.[23]

Obveze uspostavljanja CERT-a za institucije BiH i usvajanja kriterija za identifikaciju kritične infrastrukture institucija BiH i načina zaštite iste su potvrđene usvajanjem Finalnog izvješća o realizaciji Akcijskog plana za realizaciju prioriteta iz Analitičkog izvješća EK za 2020. godinu.[24]

U Dodatku 1. izvješća ilustriran je primjer susjedne zemlje Republike Hrvatske (RH) i način na koji je ona na svom putu ka EU i nakon što je postala članica EU uspostavljala strateški i zakonski okvir kibersigurnosti.

---

[20] Direktivom NIS utvrđuju se mjere s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava unutar EU kako bi se poboljšalo funkcioniranje unutarnjeg tržišta.

[21] Aktom EU o kibersigurnosti nastoji se postići visoka razina kibersigurnosti, kiberotpornosti i povjerenja u EU utvrđivanjem ciljeva i zadaća Agencije EU za kibersigurnost i okvira za uspostavu dobrovoljnih europskih programa kibersigurnosne certifikacije za proizvode, usluge i postupke informacijske i komunikacijske tehnologije. Aktom EU o kibersigurnosti se stavlja izvan snage Uredba iz 2013. godine o Agenciji EU za mrežnu i informacijsku sigurnost.

[22] VM usvaja preporuke EK-a iz oblasti kibersigurnosti donesene na godišnjim sastancima Pododbora za pravdu, slobodu i sigurnost i Pododbora za inovacije, informacijsko društvo i socijalnu politiku.

[23] Odgovorne institucije BiH (Služba za održavanje i razvoj elektroničkog poslovanja i „e-vlade" GT, MS i AZOP) su trebale realizirati aktivnosti do kraja 2022. godine.

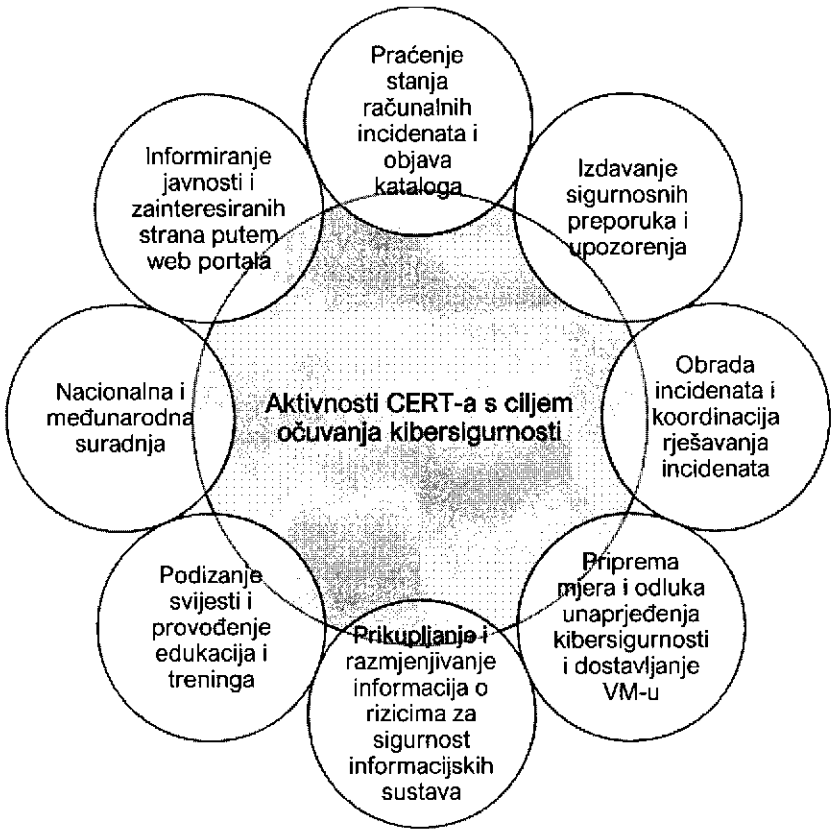
[24] VM je usvojilo Finalno izvješće na 18. sjednici VM-a, održanoj 22. 10. 2020. godine.

2.3. Regulativni okvir za kibersigurnost u institucijama BiH

Na razini institucija BiH ne postoji propis koji se isključivo bavi pitanjem kibersigurnosti i ovo pitanje djelomično je uređeno u okviru drugih propisa. Podzakonski propisi koji uređuju oblast kibersigurnosti u institucijama BiH su Odluka o određivanju CERT-a za institucije BiH[25] i Odluka o usvajanju Politike upravljanja informacijskom sigurnošću[26]. Obje odluke djeluju u preventivnom smislu.

Odlukom o određivanju CERT-a za institucije BiH osigurava se koordinirano djelovanje za prevenciju i zaštitu od sigurnosnih rizika i smanjenju posljedica od sigurnosnih incidenata. Donošenjem Odluke o određivanju CERT-a za institucije BiH stvoreni su preduvjeti za upravljanje kiberincidentima i jačanju kiberzaštite institucija BiH. Odlukom je određeno da se uspostavi CERT za institucije BiH u okviru MS-a. Sljedeći grafikon prikazuje planirane aktivnosti CERT-a za institucije BiH s ciljem očuvanja kibersigurnosti.

Grafikon 3.: Aktivnosti CERT-a s ciljem očuvanja kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Odlukom o usvajanju Politike upravljanja informacijskom sigurnošću stvoren je temelj za uspostavu sustava za upravljanje informacijskom sigurnošću u institucijama BiH sukladno

[25] Sl. gl. BiH, broj 25/17. Odluka o određivanju CERT-a za institucije BiH određuje CERT u MS-u, odnosno Sektoru za informatiku i telekomunikacijske sustave, te definira način djelovanja, modalitete i načine izvršavanja aktivnosti iz članka 6. Odluke, organizaciju i nadležnosti istog.

[26] Sl. gl. BiH, broj 38/17. Odlukom o usvajanju Politike upravljanja informacijskom sigurnošću usvaja se Politika upravljanja informacijskom sigurnošću koja definira odnos organizacije prema informacijskim dobrima i njena primarna svrha jeste da informira rukovoditelje, tehničke osobe i korisnike o bitnim zahtjevima za zaštitu informacijske imovine, uključujući ljude, hardverske i softverske resurse i podatke.

standardima za sigurnost informacijskih sustava[27], izradu zakonskih i podzakonskih propisa i programa informacijske sigurnosti. Uspostavom sustava upravljanja informacijskom sigurnošću osiguravaju se svi aspekti zaštite nekog informacijskog sustava i osigurava kvaliteta uspostavljenih mjera informacijske sigurnosti. Politikom upravljanja informacijskom sigurnošću razvija se svijest o upravljanju informacijskom sigurnošću i ukazuje da svaka institucija mora shvatiti neophodnost i potrebu realiziranja vlastite politike i uvođenja sustava za upravljanje informacijskom sigurnošću. Za realizaciju Politike upravljanja informacijskom sigurnošću određeni su MKP i MS.

2.4. Institucije BiH mjerodavne za kibersigurnost

Ministarstvo sigurnosti BiH

VM je odredio MS za uspostavu CERT-a, izradu Strategije kibersigurnosti i Zakona o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava. Poslovi u oblasti kibersigurnosti su dodijeljeni Sektoru za informatiku i telekomunikacijske sustave MS-a. Sektor za informatiku i telekomunikacijske sustave obavlja poslove na održavanju informatičke i mrežne opreme i druge poslove koje se odnose na informatičku i mrežnu opremu kao i poslove zaštite podataka u informacijskom sustavu MS-a.[28]

Ministarstvo komunikacija i prometa BiH

VM je odredio MKP za izradu Zakona o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava i smjernica za izradu internih akata upravljanja informacijskom sigurnošću. Poslovi na izradi Zakona i smjernica su dodijeljeni Sektoru za komunikacije i informatizaciju, točnije Odsjeku za informatizaciju. Neki od poslova Sektora za komunikacije i informatizaciju su priprema analiza i drugih materijala, kao temelj za unaprjeđenje politike razvoja sektora komunikacija i informatike, pripreme zakonskih i podzakonskih propisa u oblasti telekomunikacija i informatike i izrada propisa u oblasti informatike.[29]

---

[27] Standardi iz serije ISO 27000 (Sustav za upravljanje informacijskom sigurnošću) institucijama pružaju smjernice za izradu, primjenu i provjeru sigurnosti informacijskih sustava čime se osigurava povjerljivost, integritet i dostupnost informacijskog sadržaja, sustava i procesa unutar institucije. Iako se u Politici upravljanja informacijskom sigurnosti preporučuje uporaba standarda iz serije ISO 27000, u Politici upravljanja informacijskom sigurnošću su navedeni i ostali međunarodno priznati standardi informacijske sigurnosti.

[28] Prema Zakonu o ministarstvima i drugim tijelima uprave BiH (Sl. gl. BiH broj 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09, 87/12, 6/13, 19/16 i 83/17) MS je, između ostalog, mjerodavno za sprječavanje i otkrivanje činitelja kaznenih djela terorizma, trgovine drogom, krivotvorenja domaćih i strane valute i trgovine ljudima i drugih kaznenih djela sa međunarodnim ili međuentitetskim elementom i prikupljanje i korištenje podataka od značaja za sigurnost BiH.

[29] Prema Zakonu o ministarstvima i drugim tijelima uprave BiH (Sl. gl. BiH broj 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09, 87/12, 6/13, 19/16 i 83/17) MKP je, između ostalog, mjerodavno za pripremu i izradu strateških i planskih dokumenata u oblasti međunarodnih i međuentitetskih komunikacija, prometa, infrastrukture i informacijskih tehnologija.

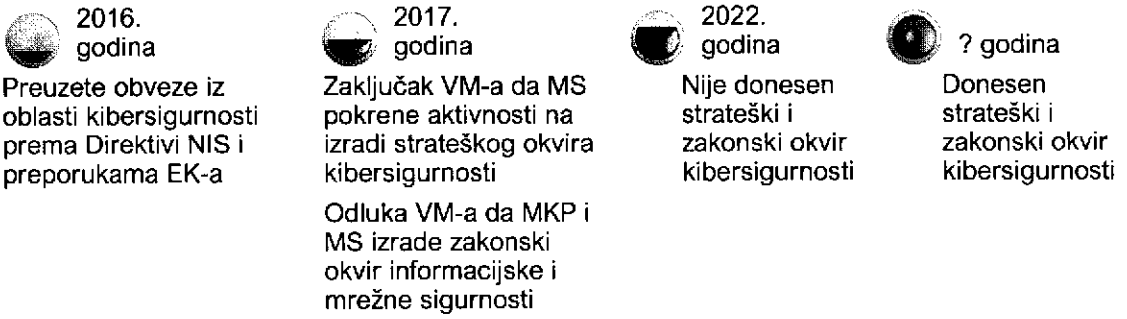
3. NALAZI REVIZIJE

U ovom poglavlju predstavljeni su nalazi revizije koji ukazuju na nedostatak temeljnih pretpostavki za izgradnju kibersigurnosti. Nalazi revizije su predstavljeni u tri poglavlja. U prvom poglavlju prezentirane su informacije o aktivnostima institucija BiH na donošenju strateškog i zakonskog okvira kibersigurnosti. U drugom poglavlju govorimo o aktivnostima formiranja CERT-a, a u trećem govorit ćemo o aktivnostima institucija BiH na donošenju akata upravljanja informacijskom sigurnošću.

3.1. Nedostatak strateškog i zakonskog okvira kibersigurnosti

U ovom poglavlju prezentirat ćemo nalaze revizije koji ukazuju da odgovorne institucije BiH nisu blagovremeno poduzimale aktivnosti na donošenju strateškog i zakonskog okvira kibersigurnosti. Aktivnosti na donošenju strateškog i zakonskog okvira kibersigurnosti pokrenute su još 2017. godine, a pet godina nakon toga, aktivnosti nisu okončane i strateški i zakonski okvir kibersigurnosti još uvijek nije donesen. Sljedeći grafikon prikazuje tijek uspostave obveze donošenja strateškog i zakonskog okvira kibersigurnosti.

Grafikon 4.: Tijek uspostave obveze donošenja strateškog i zakonskog okvira kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Iz grafikona je vidljivo da ni nakon pet godina od zaduženja VM-a odgovorne institucije BiH nisu izradile strateški i zakonski okvir kibersigurnosti i izvjesno je da dinamika aktivnosti odgovornih institucija BiH neće osigurati završetak ovih aktivnosti u trenutno definiranom roku.[30]

3.1.1. Nedostatak strateškog okvira kibersigurnosti

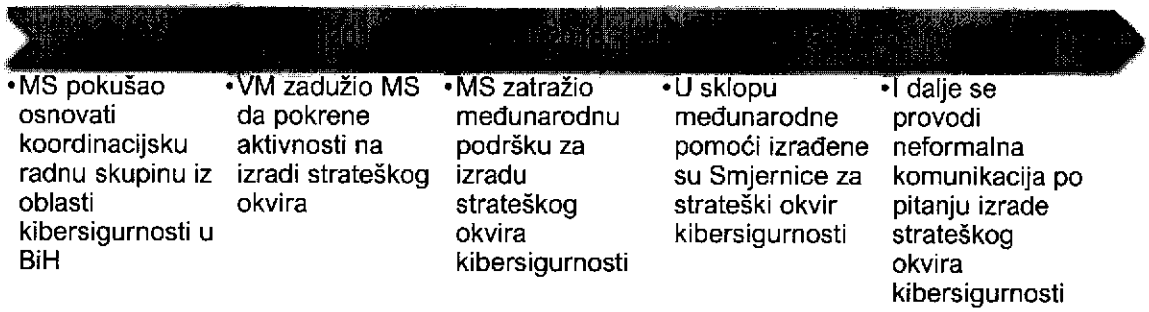
Za pet godina od kada je VM zadužio MS da poduzme aktivnosti na izradi strateškog okvira kibersigurnosti, MS nije uspio pripremiti strateški okvir kibersigurnosti koji bi VM usvojio.[31] Iako je VM 2017. godine zadužio MS da pokrene aktivnosti na izradi strateškog okvira, nije definirao rok niti način izvještavanja o realizaciji aktivnosti. Iako je VM naknadno definirao rokove za izradu strateškog okvira kibersigurnosti, MS nije u

[30] Trenutno definirani rok za izradu strateškog i zakonskog okvira kibersigurnosti je kraj 2022. godine.

[31] VM je na 107. sjednici, održanoj 6. 7. 2017. godine usvojio Analizu o usklađenosti pravnih propisa u oblasti kibersigurnosti u BiH, koju je pripremio MS i zadužio MS da intenzivira aktivnosti na izradi Strategije kibersigurnosti u BiH.

definiranim rokovima realizirao aktivnosti.[32] Sljedeći grafikon prikazuje aktivnosti MS-a na izradi strateškog okvira kibersigurnosti.

Grafikon 5.: Aktivnosti MS-a na izradi strateškog okvira kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Iz grafikona je vidljivo da je MS još 2016. godine pokušao osnovati radnu skupinu koja bi radila na izradi strateškog okvira kibersigurnosti, ali zbog nedostatka suglasnosti svih predstavnika entiteta, radna skupina nije osnovana. Narednih pet godina od zaduženja VM-a, MS nije pokušao osnovati radnu skupinu za izradu strateškog okvira. MS je tek nakon godinu dana od zaduženja VM-a poduzeo aktivnosti na izradi strateškog okvira i zatražio međunarodnu podršku. U sklopu međunarodne podrške osnovana je neformalna radna skupina za izradu strateškog okvira kibersigurnosti. Radna skupina zbog nedostatka suglasnosti svih članova nije izradila strateški okvir kibersigurnosti, već Smjernice za strateški okvir kibersigurnosti u BiH. Nije bilo drugih formalnih aktivnosti MS-a na izradi strateškog okvira kibersigurnosti. Prema izjavama predstavnika MS-a, vodi se neformalna komunikacija oko izrade strateškog okvira.

Trenutno, MS nije usuglasio i izradio model strateškog okvira kibersigurnosti prema preporukama EK-a, niti je pokušao izraditi prijedlog strateškog okvira za institucije BiH na temelju Smjernica za strateški okvir kibersigurnosti u BiH.[33] MS nije izvještavao VM o kašnjenju u realizaciji aktivnosti na izradi strateškog okvira kibersigurnosti, osim za potrebe praćenja preporuka EK-a.[34]

Posljedica trenutnog stanja je nepostojanje jasno definiranih strateških ciljeva za izgradnju kibersigurnosti. Zbog nedostatka usuglašenog strateškog okvira kibersigurnosti, BiH značajno zaostaje u ispunjavanju preuzetih obveza[35] i uređenju oblasti kibersigurnosti zbog čega je narušen ugled institucija BiH.[36] Prema izjavama sugovornika mjerodavnih institucija BiH, zbog nedostatka strateškog okvira donatori

[32] VM je u 2019. i 2020. godini usvojio preporuke EK-a sa listom aktivnosti. Prvobitno je predloženi rok EK za izradu strateškog okvira kibersigurnosti u BiH bio 2020. godina, a zatim je prolongiran za 2021. godinu. MS je određeno da vodi i koordinira aktivnosti na izradi strateškog okvira kibersigurnosti sa nadležnim institucijama BiH.

[33] Donesene Smjernice za strateški okvir kibersigurnosti u BiH predstavljaju početni korak u pravcu izgradnje kibersigurnosti i strateški okviri koji se izrade trebaju minimalno da sadrže navedene strateške ciljeve iz Smjernica za strateški okvir kibersigurnosti.

[34] MS je za potrebe praćenja preporuka EK-a navodio da nije usvojena strategija kibersigurnosti, da su aktivnosti na izradi i usuglašavanju modela strateškog dokumenta sukladno Direktivi NIS i ustavnim uređenjem BiH u tijeku i da je ovo pitanje koje treba riješiti na političkoj razini.

[35] U prilog navedenom govori i činjenica da je nedavno objavljena nova Direktiva NIS, a BiH još uvijek nije implementirala obveze iz prvotne direktive.

[36] Zajednička izjava većine predstavnika institucija iz uzorka, dok je veliki broj institucija BiH u popunjenom upitniku o kibersigurnosti naglasio da narušen ugled države i institucija BiH je moguća posljedica koja bi se desila u slučaju kibernapada ili računalnog incidenta.

smatraju da BiH ima neozbiljan pristup izgradnji kibersigurnosti zbog čega se manje sredstava ulaže u ovu oblast.

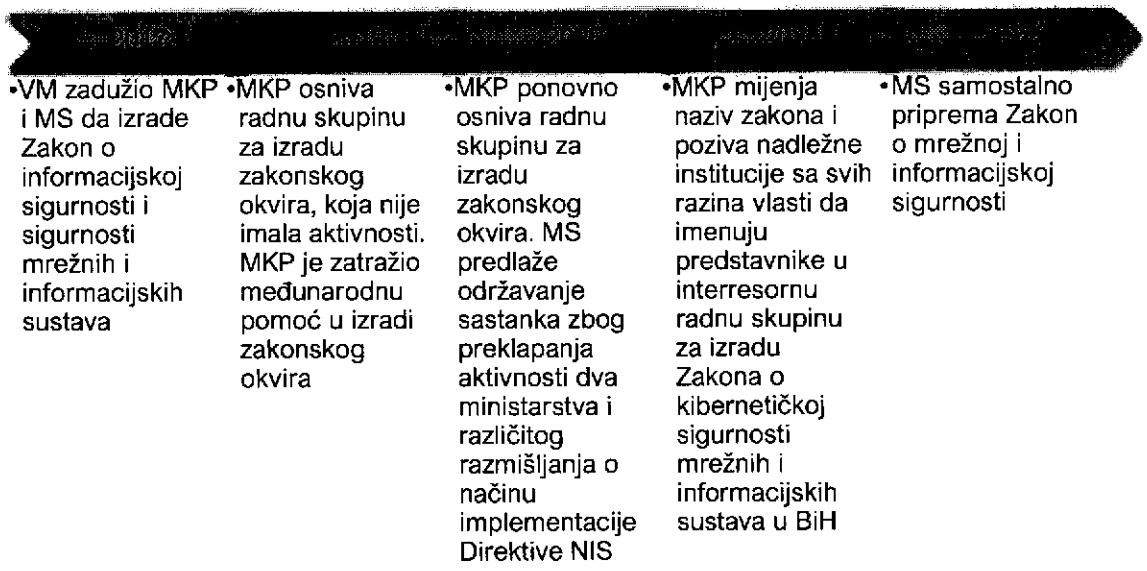
Nedostatak strateškog okvira doprinosi i zaostajanju u donošenju zakonskog okvira. O nedostatku zakonskog okvira govorimo u sljedećem poglavlju.

3.1.2. Nedostatak zakonskog okvira kibersigurnosti

Na razini institucija BiH ne postoji zakonski okvir kojim se regulira kibersigurnost, odnosno mrežna i informacijska sigurnost i nadležna tijela, iako je donošenje zakonskog okvira planirano još od 2017. godine. Posljedice su nedostatak mjera i standarda informacijske sigurnosti u institucijama BiH i nadležnih tijela koji bi osigurali provedbu i nadzor mjera i koordinaciju u sprječavanju kiberincidenata. Ovo je jedan od uzroka niske razine kibersigurnosti u institucijama BiH.

Odgovorne institucije BiH nisu izradile zakonski okvir kibersigurnosti u definiranim rokovima, iako je prošlo pet godina od zaduženja VM-a. VM je 2017. godine usvojio Politiku upravljanja informacijskom sigurnošću i stvorilo temelj za donošenje Zakona o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava. Za izradu zakonskog okvira VM je odredio MKP i MS, ali nije odmah definirao rok za realizaciju aktivnosti. Rokovi su definirani naknadno, 2019. i 2020. godine. Sljedeći grafikon prikazuje aktivnosti MKP-a i MS-a na izradi zakonskog okvira kibersigurnosti.

Grafikon 6.: Aktivnosti MKP-a i MS-a na izradi zakonskog okvira kibersigurnosti



Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, MKP i MS nisu blagovremeno i usuglašeno poduzimali aktivnosti na izradi zakonskog okvira kibersigurnosti. Jedan od razloga je različit pristup izradi zakonskog okvira kibersigurnosti i neusuglašeni stavovi oko načina implementacije Direktive NIS. Iako su za izradu zakonskog okvira određeni MKP i MS, aktivnosti je vodio MKP. MKP je tek nakon dvije godine od zaduženja VM-a poduzeo aktivnosti na osnivanju radne skupine. Iako je iste godine VM zadužio MKP da dostavi zakonski okvir na usvajanje do kraja 2019. godine, MKP nije vodio aktivnosti u sklopu radne skupine i izradio i

dostavio prijedlog zakonskog okvira VM-u.[37] Na taj način MKP i MS nisu realizirali aktivnosti u definiranim rokovima.

Ni u narednim godinama MKP i MS nisu uspjeli osnovati radnu skupinu za izradu zakonskog okvira niti su izradili zakonski okvir. Jedan od razloga zbog kojeg nije osnovana interresorna radna skupina za izradu zakonskog okvira u 2021. godini je nepostizanje suglasnosti svih predstavnika entiteta. MKP nije poduzimao dodatne aktivnosti na dobivanju suglasnosti entiteta niti je o navedenom problemu izvijestio VM. Na ovaj način nije iskorištena ni pružena međunarodna pomoć u izradi zakonskog okvira kibersigurnosti sukladno Direktivi NIS zbog čega se kasni u ispunjavanju preuzetih obveza. U danim okolnostima i zbog neusuglašenih stavova oko izrade zakonskog okvira sa MKP-om, MS samostalno priprema prijedlog zakonskog okvira.[38] Pripremljeni materijal još uvijek nije dobio formu konačnog prijedloga.[39]

MKP i MS nisu zajednički izvještavali VM o aktivnostima na izradi zakonskog okvira, iako je VM odredio MKP i MS da godišnje izvještavaju o realizaciji Politike upravljanja informacijskom sigurnošću. Samo je MKP kroz redovno izvještavanje informiralo VM da nije izrađen zakonski okvir. Nije bilo korektivnih aktivnosti VM-a na temelju redovnog izvještavanja.

Nedostatak obvezujućih mjera i standarda informacijske sigurnosti dovodi do većih rizika od kiberincidenata. U sljedećem poglavlju govorit ćemo o nedostatku tijela za sprječavanje kiberincidenata.

3.2. Nedostatak Tima za odgovor na računalne incidente – CERT-a

U ovom poglavlju prezentirat ćemo nalaze revizije koji ukazuju na kašnjenje u uspostavi CERT-a za institucije BiH i mreže CERT-ova.

Na razini institucija BiH, ni nakon pet godina od donošenja Odluke VM-a o određivanju CERT-a za institucije BiH, nije uspostavljen CERT koji bi učinkovito koordinirao i upravljao pružanjem odgovora na računalne incidente. Iako je VM zadužio MS da u kratkom roku poduzme aktivnosti s ciljem uspostave CERT-a za institucije BiH, MS za pet godina nije osigurao potrebne uvjete za uspostavu CERT-a. Posljedice su nedostatak proaktivnih i reaktivnih mjera s ciljem očuvanja kibersigurnosti institucija BiH i smanjenja posljedica računalnih incidenata.[40] Zbog navedenog, institucije BiH su izložene većim sigurnosnim rizicima i kiberprijetnjama.

---

[37] VM je na 174. sjednici, održanoj 2. 7. 2019. godine, usvojio Informaciju o ispunjavanju pravnog kriterija institucija BiH i zadužio MKP da najdalje do kraja 2019. godine dostavi VM-u na usvajanje nacrt zakona o informacijskoj sigurnosti i sigurnosti mrežnih i informacijskih sustava. Na istoj sjednici VM je usvojio preporuke EK-a i listu aktivnosti prema kojoj MKP i MS trebaju izraditi zakonski okvir kibersigurnosti usklađen sa Direktivom NIS do kraja 2019. godine. U 2020. godini rok je prolongiran do 2021. / 2022. godine.

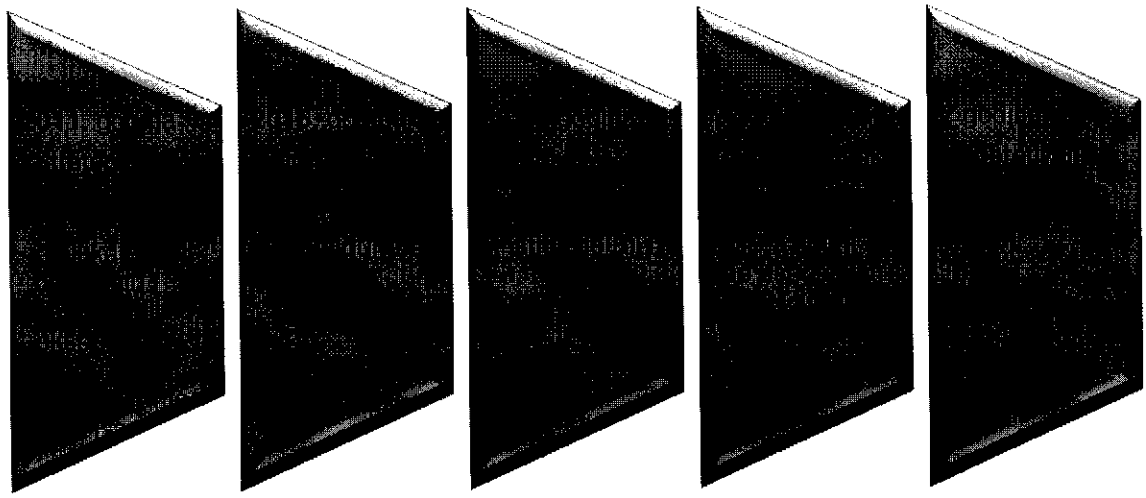
[38] Aktivnosti na izradi zakona o mrežnoj i informacijskoj sigurnosti institucija BiH MS je radio na temelju Programa rada MS-a i VM-a za 2021. MS je pripremio ovaj zakon u suradnji sa UNDP-om. MS je mišljenja da se zakonski okvir kibersigurnosti može raditi samo za institucije BiH, a MKP smatra da se Direktiva NIS u potpunosti može implementirati samo na način da se radi zakonski okvir kibersigurnosti koji će obuhvatiti sve kritične infrastrukture u BiH.

[39] MS nije poduzeo aktivnosti na formiranju radne skupine za izradu zakonskog okvira, niti je pripremljeni materijal prošao procedure usklađivanja i pribavljanja mišljenja nadležnih institucija BiH.

[40] Proaktivnim mjerama se djeluje prije incidenta i drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprječavanja ili ublažavanja mogućih šteta. Reaktivnim mjerama odgovara se na incidente te na druge događaje koji mogu ugroziti kibersigurnost informacijskih sustava.

Kao prijelomni trenutak za detaljnu analizu aktivnosti uspostave CERT-a za institucije BiH uzeto je donošenje Odluke o određivanju CERT-a za institucije BiH 2017. godine, iako su aktivnosti na uspostavi CERT-a započele još 2011. godine. Sljedeći grafikon prikazuje tijek uspostave CERT-a za institucije BiH.

Grafikon 7.: Tijek uspostave CERT-a za institucije BiH



Izvor: Ured za reviziju institucija BiH

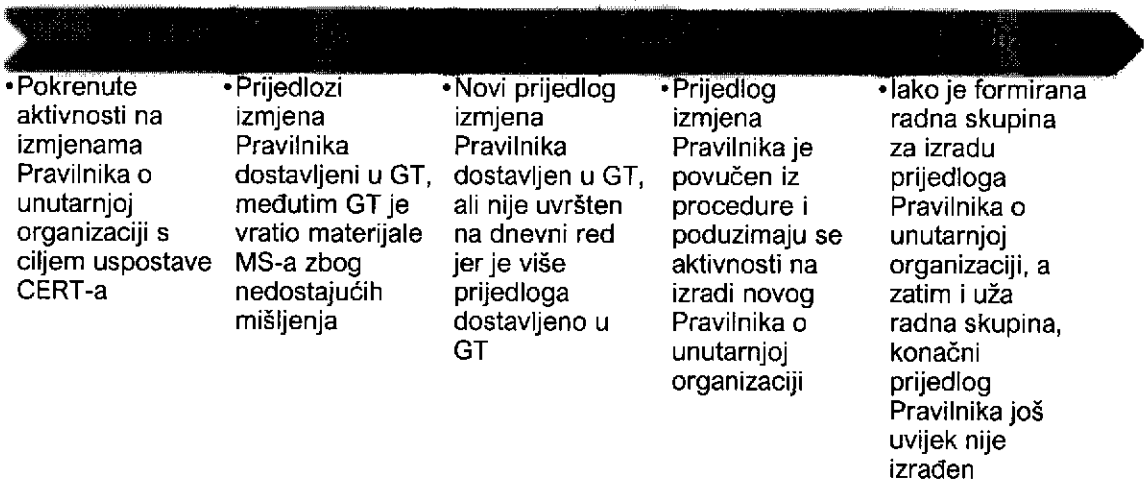
Kao što je vidljivo iz grafikona, aktivnosti na uspostavi CERT-a su započele još 2011. godine kada je VM usvojio Strategiju uspostave CERT-a u BiH i donijelo Odluku o osnivanju i imenovanju ekspertne radne skupine za formiranje CERT tijela u BiH. Ekspertna radna skupina je izradila Akcijski plan uspostave BiH CERT-a koji nije usvojen na VM-u. To je bila zadnja aktivnost na uspostavi BiH CERT-a. Prema izjavama sugovornika iz MS-a, koje je vodio navedene aktivnosti, nije bilo podrške svih sudionika radne skupine za daljnje aktivnosti na uspostavi BiH CERT-a. Narednih pet godina MS nije poduzimao aktivnosti na uspostavi CERT-a.

Naredna aktivnost na uspostavi CERT-a je poduzeta tek 2016. godine kada je VM usvojio Informaciju o aktivnostima MS-a u vezi sa kibersigurnosti.[41] VM je zadužio MS da izradi prijedlog odluke o određivanju CERT-a za institucije BiH, dostavi VM-u na usvajanje i izradi prijedloge odluka i akata unutarnje organizacije kojima će osigurati okvir za CERT za institucije BiH. VM je 2017. godine donio Odluku o određivanju CERT-a za institucije BiH i zadužio MS da u roku od tri mjeseca predloži VM-u dopunu Pravilnika o unutarnjoj organizaciji s ciljem uspostave CERT-a u MS-u.[42] MS nije u roku od tri mjeseca dostavio VM-u na usvajanje dopunu Pravilnika o unutarnjoj organizaciji s ciljem uspostave CERT-a za institucije BiH. Sljedeći grafikon prikazuje aktivnosti MS-a s ciljem uspostave CERT-a (detaljniji pregled je u Dodatku 2.).

[41] Informacija je usvojena na 64. sjednici VM-a, održanoj 14. 7. 2016. godine.

[42] Određeno je da se uspostavi posebna unutarnja organizacijska jedinica u okviru Sektora za informatiku i telekomunikacijske sustave MS-a.

Grafikon 8.: Aktivnosti MS-a s ciljem uspostave CERT-a za institucije BiH



Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, MS-u je trebalo godinu dana da pošalje prvi nekompletni prijedlog dopuna Pravilnika o unutarnjoj organizaciji u GT s ciljem uspostave CERT-a za institucije BiH. Iako je MS u 2018. godini u dva navrata dostavio GT-u nove prijedloge izmjena Pravilnika o unutarnjoj organizaciji, materijali nisu bili predmet razmatranja na sjednicama VM-a zbog nedostajućih mišljenja.[43] Nakon što su pribavljena potrebna mišljenja, MS je 2019. godine dostavio materijal u GT. Materijal ni tada nije bio predmet razmatranja VM-a jer je GT tražio da se MS izjasni koji točno materijal treba biti razmatran. Nakon toga MS povlači materijal iz daljnje procedure i poduzima aktivnosti na izradi novog Pravilnika o unutarnjoj organizaciji i formira radnu skupinu za izradu novog Pravilnika. Ni nakon pet godina MS u proceduru nije uputio kompletirani prijedlog Pravilnika o unutarnjoj organizaciji s ciljem uspostave CERT-a.

Trenutno nije poznato kada će MS izraditi prijedlog Pravilnika o unutarnjoj organizaciji i dostaviti VM-u.[44] S obzirom da nisu osigurani organizacijski preduvjeti za uspostavu CERT-a, nije poznato ni kada će CERT postati operativan i obavljati dodijeljene poslove.[45] Iako MS kroz redovno izvještavanje informira VM o kašnjenju u uspostavi CERT-a zbog neusvajanja izmjena Pravilnika o unutarnjoj organizaciji, VM nije tražio dodatna pojašnjenja.

S obzirom da MS nije uspostavio CERT, nije osigurao ni preduvjete za uspostavu mreže CERT-ova u BiH, zbog čega nije uspostavljena mreža CERT-ova.[46] Uspostavljanje CERT-a za institucije BiH i mreže CERT-ova su preuzete obveze koje nisu ispunjene. MS nije

[43] Prijedlozi izmjena Pravilnika su osim za CERT, sublimirali i druge izmjene koje se ne odnose na CERT.

[44] Sektor za informatiku i telekomunikacije je u više navrata informirao kabinet ministra o razlozima zbog kojih je potrebno pripremiti izmjene Pravilnika o unutarnjoj organizaciji, odnosno donijeti novi Pravilnik s ciljem uspostave CERT-a i izvršiti upošljavanje u CERT. U 2022. godini su tražili od Sektora za pravne, kadrovske i opće poslove pokretanje procedure usvajanja izmjena Pravilnika o unutarnjoj organizaciji s ciljem uspostave CERT-a. Na dostavljene informacije nije bilo konkretnih odgovora.

[45] Osim organizacijskih preduvjeta, potrebno je osigurati i tehničke preduvjete za CERT, što iziskuje dodatno vrijeme i sredstva. Prema izjavama sugovornika, nakon usvajanja prijedloga Pravilnika o unutarnjoj organizaciji potrebno je minimalno dvije godine da se osiguraju ostali preduvjeti za operativnost CERT-a.

[46] Uspostavljanje državnog CERT-a ne sprječava uspostavu i drugih CERT-ova, dapače relevantne preporuke govore da svaka država treba uspostaviti više CERT-ova, za svako ključno područje. Prema dostupnim informacijama, u BiH je uspostavljen CERT Republike Srpske, CERT Ministarstva obrane BiH i Akademski CERT. U Federaciji je CERT u fazi uspostavljanja.

uspostavio mrežu CERT-ova u definiranim rokovima.[47] Nedostatak mreže CERT-ova je jedan od razloga zašto nema registra ili kataloga kiberincidenata u BiH i pregleda upozorenja na potencijalne kiberprijetnje.

Nedostatak CERT-a doprinosi niskoj razini svijesti o važnosti očuvanja kibersigurnosti. U sljedećem poglavlju govorimo o nezadovoljavajućoj razini svijesti u institucijama BiH o važnosti očuvanja kibersigurnosti.

3.3. Pasivan pristup u donošenju akata upravljanja informacijskom sigurnošću

U ovom poglavlju prezentirat ćemo nalaze revizije koji ukazuju na nedovoljnu razinu kibersigurnosti, odnosno informacijske sigurnosti u institucijama BiH.

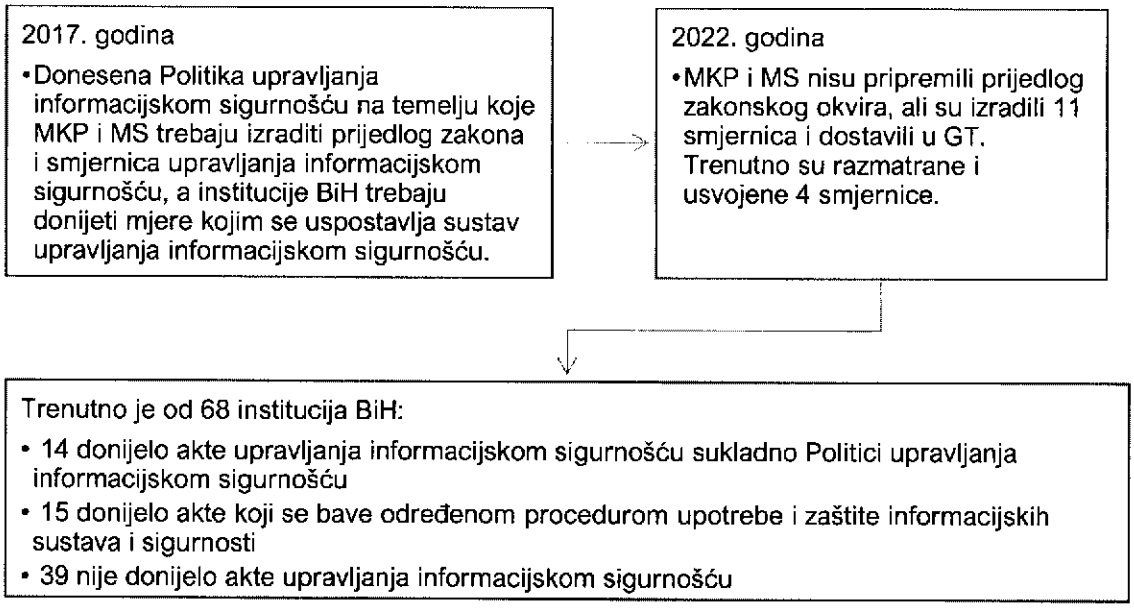
Institucije BiH su imale pasivan pristup u donošenju akata upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću i/ili standardima upravljanja informacijskom sigurnošću.[48] Ni nakon pet godina od donošenja Politike više od polovine institucija BiH nije donijelo akte upravljanja informacijskom sigurnošću. Neki od razloga pasivnog pristupa su nedostatak zakonskog okvira, neblagovremeno donošenje smjernica iz Politike upravljanja informacijskom sigurnošću[49] i nedovoljna razina svijesti o važnosti zaštite kibersigurnosti. Posljedice su slaba implementacija mjera i standarda informacijske sigurnosti što dovodi do niske razine informacijske sigurnosti u institucijama BiH. Sljedeći grafikon prikazuje trenutno stanje realizacije Politike upravljanja informacijskom sigurnošću.

[47] U listi aktivnosti EK-a za 2020. godinu rok za realizaciju osnivanja radne skupine za izradu Odluke o uspostavljanju mreže CERT-ova je prva polovina 2021. godine. U Programu rada MS-a za 2021. godinu planirana je izrada Odluke o uspostavljanju mreže CERT-ova u BiH.

[48] U Politici upravljanja informacijskom sigurnošću preporučuje se izrada politike institucije, kao krovnog dokumenta, na temelju koje će se izraditi ostali akti s ciljem uspostave sustava upravljanja informacijskom sigurnošću.

[49] U Politici upravljanja informacijskom sigurnošću opisano je 11 smjernica koje je potrebno izraditi, a to su: Smjernice o informatičkoj sigurnosti radnog mjesta, Smjernice o klasificiranju informacijskih resursa, Smjernice o korištenju prijenosnih uređaja, Smjernice o fizičkoj zaštiti informacija, Smjernice o kontroli pristupa i bilježenju događaja, Smjernice o upravljanju sigurnosnim incidentima, Smjernice o upravljanju sigurnosnim zakrpama, Smjernice o korisničkim računima i pravima pristupa, Smjernice o sigurnosnim preslikama, Smjernice o uposlenju i prekidu uposlenja i Smjernice za izradu metodologije procjene rizika.

Grafikon 9.: Dinamika realizacije Politike upravljanja informacijskom sigurnošću



Izvor: Ured za reviziju institucija BiH

Kao što je vidljivo iz grafikona, tek nakon pet godina od donošenja Politike upravljanja informacijskom sigurnošću je VM razmatrao i usvojio četiri smjernice iz Politike upravljanja informacijskom sigurnošću.[50] Iako je MKP dostavio svih 11 smjernica u GT, predmet razmatranja je bio samo jedan set smjernica, dok preostala dva nisu. Iz razgovora sa predstavnikom MKP-a očekuje se usvajanje i preostalih smjernica na nekoj od idućih sjednica VM-a.

MKP je izradu smjernica podijelio u tri seta. Iako je prvi set smjernica izrađen još 2018. godine, a u naredne dvije godine i ostala dva seta smjernica, tek početkom 2022. godine su dostavljene u GT. Proces pribavljanja mišljenja MFT-a na smjernice je bio dugotrajan. Iako je MKP u više navrata pokušao organizirati sastanak sa predstavnicima MFT-a s ciljem dobivanja suglasnosti MFT-a, do 2022. godine nije osigurana suglasnost MFT-a, zbog čega smjernice nisu bile predmet ranijeg razmatranja na VM-u. Zbog neblagovremenog donošenja smjernica propuštena je prilika da institucije BiH pristupe izradi akata na temelju smjernica iz Politike upravljanja informacijskom sigurnošću.

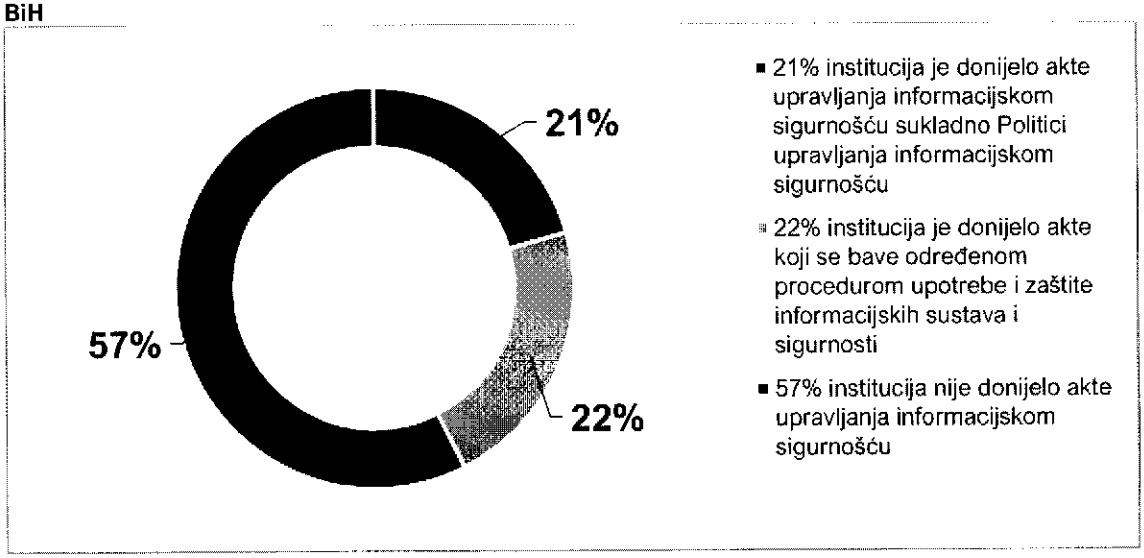
MKP i MS nisu izvještavali VM o slaboj realizaciji Politike upravljanja informacijskom sigurnošću, iako ih je VM zadužio da vrše godišnje izvještavanje. MKP je u dva navrata putem godišnjih izvješća o radu informirao VM o statusu smjernica iz Politike upravljanja informacijskom sigurnošću. Nije bilo povratnih informacija nakon usvajanja izvješća o radu MKP-a. MKP i MS nisu odredili način na koji bi pratili realizaciju Politike upravljanja informacijskom sigurnošću u institucijama BiH, niti raspolažu informacijama o stanju u institucijama BiH.

U izostanku informacija o implementaciji Politike upravljanja informacijskom sigurnošću, tim revizije je proveo ispitivanje u institucijama BiH i došao do podataka o trenutnom

[50] VM je na 54. sjednici, održanoj 28. 7. 2022. godine donio Odluku o usvajanju smjernica iz Politike upravljanja informacijskom sigurnošću i to četiri smjernice: Smjernice o korisničkim računima i pravima pristupa, Smjernice o sigurnosnim preslikama, Smjernice o uposlenju i prekidu uposlenja i Smjernice za izradu metodologije procjene rizika.

stanju.[51] Trenutno većina institucija BiH nije donijela akte upravljanja informacijskom sigurnošću usklađene sa Politikom upravljanja informacijskom sigurnošću i/ili međunarodnim standardima upravljanja informacijskom sigurnošću, a što se vidi iz sljedećeg grafikona.

Grafikon 10.: Trenutno stanje primjene Politike upravljanja informacijskom sigurnošću u institucijama BiH



Izvor: Ured za reviziju institucija BiH

Kao što se vidi iz grafikona, većina institucija BiH nije donijela usklađene akte upravljanja informacijskom sigurnošću, iako je od donošenja Politike upravljanja informacijskom sigurnošću prošlo pet godina. Prema dostavljenim odgovorima samo 14 od 68 institucija BiH je donijelo usklađene akte upravljanja informacijskom sigurnošću.[52] Od 68 institucija BiH 15 je donijelo akte koji se bave određenom procedurom upotrebe informacijsko komunikacijskih sustava, a određeni broj institucija je detaljnije razradio mjere zaštite informacijsko komunikacijskih sustava i sigurnosti informacija.[53]

Od 68 institucija BiH 39 nije donijelo akte upravljanja informacijskom sigurnošću. Institucije su navodile različite razloge zašto nisu donijele navedene akte. Određeni broj institucija koji nije donio vlastite akte je na sustavu e-vlade i smatra da je e-vlada zadužena za sigurnost. Sličan primjer je i kod određenog broja pravosudnih institucija, koje su na informacijskom sustavu Visokog sudbenog i tužiteljskog vijeća BiH. Određeni broj institucija BiH nije upoznato s Politikom upravljanja informacijskom sigurnošću ili je mišljenja da im nije potrebno upravljanje informacijskom sigurnošću za poslovanje.

[51] Provedeno je ispitivanje 73 institucije BiH, odgovore je dostavilo 68 institucija BiH na temelju kojih je utvrđeno trenutno stanje. Revizijski tim je u pojedinim slučajevima obavljao telefonske razgovore radi pojašnjenja određenih odgovora u cilju prezentiranja što točnijeg stanja. Bilo je manjih korekcija odgovora.

[52] Od 14 institucija koje su donijele akte upravljanja informacijskom sigurnošću, određeni broj je izradio akte upravljanja informacijskom sigurnošću i prije donošenja Politike upravljanja informacijskom sigurnošću i izvršio certifikaciju sustava upravljanja informacijskom sigurnošću.

[53] Prema dostavljenim odgovorima, 15 od 68 institucija BiH je donijelo akte upotrebe informacijsko komunikacijskih sustava i/ili zaštite sigurnosti informacija ili određene procedure upotrebe informacijsko komunikacijskih sustava, ali koji nisu usklađeni sa Politikom upravljanja informacijskom sigurnošću i/ili međunarodnim standardima informacijske sigurnosti.

Provedbom revizije u institucijama iz uzorka uočen je različit stupanj razvoja svijesti o važnosti upravljanja informacijskom sigurnošću. Sljedeća tablica prikazuje trenutno stanje u institucijama iz uzorka.

Tablica 1.: Trenutno stanje u institucijama iz uzorka

	Naziv institucije
Izrađeni akti upravljanja informacijskom sigurnošću	AZOP i RAK
Akti upravljanja informacijskom sigurnošću u izradi	MFT, MS i GT
Nisu izrađeni akti upravljanja informacijskom sigurnošću	AJN i MKP
Broj ispitanih institucija	7

Izvor: Ured za reviziju institucija BiH

Kao što se vidi iz tablice 1. samo su dvije od sedam institucija iz uzorka donijele akte upravljanja informacijskom sigurnošću u skladu sa Politikom upravljanja informacijskom sigurnošću. AZOP je Opću politiku sigurnosti informacija donio 2017. godine. RAK je Politiku sigurnosti informacijskog sustava donio 2019. godine.[54] Na sljedećoj ilustraciji prikazat ćemo primjer proaktivnog pristupa u uspostavi sustava upravljanja informacijskom sigurnošću.

Ilustracija 1.: Primjer proaktivnog pristupa u uspostavi upravljanja informacijskom sigurnošću

AZOP je još 2014. godine započeo izgradnju sustava upravljanja informacijskom sigurnošću u skladu sa ISO standardima informacijske sigurnosti. Inicijativa je poduzeta nakon što je zabilježen kiberincident na web stranicu što je dovelo do zastoja u radu od par sati. Inicijativa je poduzeta i prema preporukama Europskog odbora za zaštitu osobnih podataka, s obzirom da se u informacijskom sustavu AZOP-a nalaze registri osobnih podataka. Detaljne analize i koraci prema ISO standardu su urađeni sa angažiranom firmom. Opća politika sigurnosti informacija u skladu sa Politikom upravljanja informacijskom sigurnošću je donesena 2017. godine, koju prati izrada ostalih pravila informacijske sigurnosti. Dosada nije urađena certifikacija ISO standarda, ali je u planu.

Izvor: Ured za reviziju institucija BiH

Tri od sedam institucija iz uzorka su u fazi izrade akata upravljanja informacijskom sigurnošću u skladu sa Politikom upravljanja informacijskom sigurnošću. MFT i MS su nedavno pripremili nacrt akata upravljanja informacijskom sigurnošću u skladu sa Politikom upravljanja informacijskom sigurnošću, a GT je poduzeo početne aktivnosti na izradi. Iako su sve tri institucije mišljenja da nije dovoljna trenutna razina informacijske sigurnosti i da se treba unaprijediti, tek nakon pet godina od donošenja Politike informacijske sigurnosti su poduzele aktivnosti na izradi.[55] Sve tri institucije kao jedan od razloga su navele nedostatak kadra.

Dvije od sedam institucija iz uzorka nisu donijele akte upravljanja informacijskom sigurnošću. Obje institucije smatraju da se treba unaprijediti informacijska sigurnost, ali ni nakon pet godina od donošenja Politike upravljanja informacijskom sigurnošću nisu izradile akte upravljanja informacijskom sigurnošću. MKP nije pokrenuo aktivnosti jer je

[54] RAK je samostalno izradio politiku upravljanja informacijskom sigurnošću u skladu sa Politikom upravljanja informacijskom sigurnošću na temelju koje su izvedeni ostali pravilnici i naputci zaštite informacijske sigurnosti. Analize koje su bile potrebne za izradu politike su rađene u skladu sa smjernicama iz Politike upravljanja informacijskom sigurnošću.

[55] Sve tri institucije imaju određenu razinu zaštite informacijske sigurnosti. U MFT-u se primjenjuju pravilnici za uporabu i pristup informacijskom sustavu MFT-a i procedure iz 2009. godine, 2010. godine i 2012. godine. U MS-u se primjenjuju Pravilnik o izradi sigurnosnih kopija i oporavak podataka iz 2013. godine i procedure pristupa Mrežnom operativnom centru MS-a iz 2018. godine i prema izjavi sugovornika druge procedure koje nisu generalizirane. GT primjenjuje Pravilnik o uporabi zajedničkog informacijsko komunikacijskog sustava u VM-u iz 2013. godine.

čekao donošenje smjernica, iako je MKP izradilo nacrt smjernica.[56] AJN nije poduzimao aktivnosti jer nije bila upoznata sa Politikom upravljanja informacijskom sigurnošću.[57]

Većina institucija iz uzorka je imala zabilježenu određenu vrstu kiberincidenata. Od sedam institucija iz uzorka pet je imalo zabilježene kiberincidente na web stranicu, elektroničku poštu i incidente kod provajdera. Na primjeru institucija iz uzorka ilustrirat ćemo posljedice zabilježenih kiberincidenata i druge moguće posljedice koje su istaknute na razgovorima u institucijama BiH.

Ilustracija 2.: Istaknute posljedice i moguće posljedice u institucijama iz uzorka

Na temelju razgovora u institucijama iz uzorka zabilježeni kiberincidenti prouzrokovali su obustavu rada od nekoliko sati do par dana, nedostupnost web stranice i elektroničke pošte. Posljedice za institucije su bile ugrožavanje kibersigurnosti, neovlašten pristup informacijama, gubitak radnih sati i povećanje troškova na oporavku informacijskog sustava, kašnjenje u obavljanju poslova iz nadležnosti, gubitak povjerenja i narušen ugled institucije. Posljedice za korisnike usluga institucija je nemogućnost pristupa važnim informacijama, kao što su npr. javni pozivi za javne nabave ili neblagovremena plaćanja iz proračuna. Sve institucije iz uzorka su mišljenja da u slučaju ostvarenog kibernapada posljedice bi bile značajnije, od ugrožavanja sigurnosti, pouzdanosti i cjelovitosti podataka, oštećenja informacijskog sustava, oštećenja ili trajnog gubitka podataka, ugrožavanja osobne sigurnosti i sigurnosne situacije i funkcioniranja zemlje, narušene reputacije i odbijanje potencijalnih investitora.

Izvor: Ured za reviziju institucija BiH

Slaba primjena mjera i standarda informacijske sigurnosti dovodi do ugrožavanja kibersigurnosti i može dovesti do značajnih posljedica. Iako revizija nije detaljno analizirala primjenu mjera uočeno je da postoje određene slabosti u primjeni osnovnih mjera informacijske sigurnosti. Jedan od primjera je neodgovarajuća primjena lozinki za informacijski sustav.[58]

[56] Trenutno, MKP nema vlastite procedure već primjenjuju procedure e-vlade za uporabu zajedničkog informacijsko komunikacijskog sustava u VM-u.

[57] AJN je 2008. godine donio Odluku o upotrebi računara i zaštite podataka u 2008. godini i 2016. godine Interne i eksterne procedure backup-a.

[58] Naziv institucije ne navodimo da tu instituciju dodatno ne bismo izložili mogućnostima zlouporabe.

4. ZAKLJUČCI REVIZIJE

Ured za reviziju institucija BiH proveo je reviziju učinka s ciljem da provjeri jesu li institucije BiH efikasne u poduzimanju aktivnosti u osiguranju temeljnih pretpostavki za kibersigurnost. Provedena istraživanja, intervjui i analiza relevantne dokumentacije omogućila su nam da sagledamo postojeće stanje te da iznesemo sljedeći zaključak.

Institucije BiH nisu efikasne u poduzimanju aktivnosti s ciljem osiguranja temeljnih pretpostavki za kibersigurnost. Na razini institucija BiH nije osiguran strateški i zakonski okvir kibersigurnosti, niti je uspostavljen CERT za institucije BiH. Pojedinačne institucije BiH nisu bile efikasne u donošenju akata upravljanja informacijskom sigurnošću u skladu sa Politikom upravljanja informacijskom sigurnošću. Posljedice nedostatka temeljnih pretpostavki za kibersigurnost ugrožavaju poslovanje javne uprave i mogu dovesti do otuđenja podataka i financijskih sredstava neophodnih za funkcioniranje zemlje i svakodnevnog života građana.

4.1. Nije osiguran strateški i zakonski okvir kibersigurnosti

Na razini institucija BiH značajno se kasni u uspostavi strateškog i zakonskog okvira kibersigurnosti. Neblagovremeno definiranje rokova za realizaciju aktivnosti je pridonijelo slaboj realizaciji aktivnosti. Zbog nepostojanja strateškog i zakonskog okvira nisu osigurane temeljne pretpostavke za sustavnu izgradnju kibersigurnosti što je doprinijelo niskoj razini kibersigurnosti.

Odlaganje donošenja i usklađivanja strateškog i zakonskog okvira kibersigurnosti sa zakonodavstvom EU za posljedicu nema samo neispunjavanje preuzetih obveza već doprinosi tehnološkom zaostajanju institucija BiH. Tehnološko zaostajanje čini institucije BiH izloženijim većim sigurnosnim rizicima i prijetnjama što otežava digitalnu transformaciju javne uprave. Bez kibersigurnosti nije moguće uspostaviti digitalnu javnu upravu koja će pružati elektroničke usluge i koja će pridonijeti ostvarivanju pristupa jedinstvenom digitalnom tržištu.

Izrada strateškog okvira kibersigurnosti je izazov na koji MS nije blagovremeno odgovorio i bez osigurane podrške nije moglo ponuditi najbolje moguće rješenje, uvažavajući kompleksno uređenje BiH. Bez strateškog okvira nije moguće uspostaviti koordinirani i planski pristup izgradnji kibersigurnosti, a bez takvog pristupa je teško osigurati kiberzaštitu informacijskih sustava i mreža institucija BiH i njenih poslovnih subjekata i građana. Zbog nedostatka strateškog okvira donatori smatraju da BiH ima neozbiljan pristup izgradnji kibersigurnosti zbog čega manje sredstava ulažu u ovu oblast.

MKP i MS nisu zajednički pristupili pripremi zakonskog okvira kibersigurnosti i nisu ponudili najbolje moguće rješenje u danim okolnostima. Zakonski okvir kibersigurnosti nije donesen što je utjecalo na slabu implementaciju mjera i standarda informacijske sigurnosti u institucijama u BiH. Slaba implementacija mjera dovodi do većih rizika i ranjivosti na kiberprijetnje. U takvim situacijama koriste se informacijski i mrežni sustavi koji nemaju odgovarajuću razinu zaštite, a financijska sredstva i podatci koji pripadaju institucijama BiH su lakše dostupna za nezakonito korištenje.

4.2. Nije uspostavljen CERT za institucije BiH

Na razini institucija BiH značajno se kasni u uspostavi CERT-a za institucije BiH u odnosu na definirani rok. Zbog kašnjenja MS-a u osiguravanju potrebnih uvjeta nije uspostavljen CERT i nije osiguran koordinirani pristup u upravljanju pružanjem odgovora na kiberincidente. U izostanku koordiniranog pristupa nisu implementirane proaktivne i reaktivne mjere kibersigurnosti u institucijama BiH. Na taj način nije dostignuta odgovarajuća razina kiberpripravnosti razmjerna kiberprijetnjama.

Neformiranjem CERT-a odgovorna institucija BiH nije osigurala uvjete za uspostavu mreže CERT-ova zbog čega nema evidencija o kiberincidentima, niti razmjene informacija i sigurnosnih preporuka. U nedostatku CERT-a nisu osigurana sigurnosna upozorenja i preporuke za pružanje odgovora na kiberincidente zbog čega su informacijski i mrežni sustavi institucija BiH podobniji za realizaciju kiberprijetnji. Svaki zabilježeni kibernapad narušava ugled institucija BiH i bez odgovarajućeg pruženog odgovora čini veću i dugotrajniju štetu po institucije BiH.

4.3. Neefikasno donošenje akata upravljanja informacijskom sigurnošću

Većina institucija BiH nije imala proaktivan pristup u donošenju akata upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću. Neke od institucija BiH nisu ni bile upoznate da postoji Politika, a neke smatraju da im nije potrebno upravljanje informacijskom sigurnošću za poslovanje. MKP i MS nisu pratili implementaciju Politike upravljanja informacijskom sigurnošću u institucijama BiH i na taj način upoznali i aktivirali institucije BiH sa Politikom. Niska razina svijesti o važnosti kibersigurnosti je možda i najviše utjecala na pasivan pristup donošenju usklađenih akata upravljanja informacijskom sigurnošću. Tako je propuštena prilika da institucije BiH postignu odgovarajuću razinu zaštite informacijske sigurnosti koja je normirana i potrebna za sigurno i učinkovito poslovanje.

Implementacija preventivnih mjera informacijske sigurnosti u institucijama BiH nije dosljedna zbog čega nije ostvarena zadovoljavajuća razina kibersigurnosti. Institucije BiH zbog toga mogu biti podobnije za ugrožavanje kibersigurnosti što dovodi do značajnih posljedica i to ne samo za institucije, već za cijelu zemlju. Motiv za izgradnju kibersigurnosti potrebno je zasnivati na svijesti institucija BiH o važnosti zaštite kibersigurnosti, a ne na zaključcima međunarodnih izvješća. Bez kibersigurnosti nema ni tehnološkog napretka BiH, a može biti i ograničen ekonomski napredak.

5. PREPORUKE REVIZIJE

Na temelju provedenih istraživanja, nalaza i zaključaka revizije, Ured za reviziju daje sljedeće preporuke:

Preporuka Vijeću ministara BiH:

- **Definirati rokove za pripremu i odgovornost za izvještavanje o procesu pripreme relevantnih akata kibersigurnosti.**

VM svojim zaključkom može definirati rokove i odgovornost za izvještavanje o procesu pripreme relevantnih akata kibersigurnosti. Utvrđivanje rokova za izradu, jasnih odgovornosti i obveze izvještavanja o procesu izrade propisa i ostalih akata kibersigurnosti omogućit će VM-u lakši nadzor nad ovim procesom i potaći će efikasnost odgovornih institucija.

Preporuke Ministarstvu komunikacija i prometa BiH i Ministarstvu sigurnosti BiH:

- **Žurno okončati pripremu prijedloga relevantnih propisa kibersigurnosti i dostaviti ih VM-u na usvajanje.**

Odgovorna ministarstva trebaju ubrzati aktivnosti na pripremi usuglašenog i prihvatljivog prijedloga zakonodavnog okvira. S tim u vezi potrebno je okončati aktivnosti formiranja odgovorne radne skupine ili poduzeti druge potrebne aktivnosti koje će dovesti do prihvatljivog prijedloga zakonskog okvira koji će regulirati kibersigurnost, odnosno informacijsku sigurnost u institucijama BiH.

- **Izvijestiti VM o realizaciji Politike upravljanja informacijskom sigurnošću u institucijama BiH.**

S ciljem unaprjeđenja kibersigurnosti, odnosno informacijske sigurnosti u institucijama BiH, odgovorna ministarstva trebaju izvijestiti VM o realizaciji Politike upravljanja informacijskom sigurnošću i stanju u institucijama BiH. Odgovorna ministarstva se trebaju dogovoriti o načinu izvještavanja.

Preporuke Ministarstvu sigurnosti BiH:

- **Žurno okončati pripremu prijedloga strateškog okvira kibersigurnosti i dostaviti ga VM-u na usvajanje.**

Odgovorno ministarstvo treba ubrzati aktivnosti na pripremi usuglašenog i prihvatljivog prijedloga strateškog okvira. S tim u vezi potrebno je okončati aktivnosti formiranja odgovorne radne skupine ili poduzeti druge potrebne aktivnosti koje će dovesti do prihvatljivog prijedloga strateškog okvira koji će regulirati kibersigurnost, odnosno informacijsku sigurnost u institucijama BiH.

- **Žurno osigurati organizacijske pretpostavke za formiranje Tima za odgovor na računalne incidente za institucije BiH.**

Ovo može podrazumijevati da MS osigura organizacijske pretpostavke kroz izmjenu relevantnih akata ministarstva ili donese druge odluke kojim će se osigurati organizacijske pretpostavke za formiranje Tima za odgovor na računalne incidente za institucije BiH i dostavi VM-u na usvajanje.

Preporuka institucijama BiH:

- **Žurno donijeti akte upravljanja informacijskom sigurnošću sukladno Politici upravljanja informacijskom sigurnošću.**

S ciljem unaprjeđenja informacijske sigurnosti i uspostave sustava upravljanja informacijskom sigurnošću, institucije BiH koje nisu izradile akte usklađene sa Politikom upravljanja informacijskom sigurnošću, trebaju izraditi akte na temelju smjernica i standarda informacijske sigurnosti iz Politike upravljanja informacijskom sigurnošću.

Tim revizije učinka:

Magdalena Pejak
Viši revizor učinka - voditelj tima

Danijel Čolo
Rukovoditelj Odjela za reviziju učinka

Jasmina Zuko
Samostalni revizor učinka - član tima

Radivoje Jeremić
Rukovoditelj Odjela za kontrolu kvalitete, metodologiju i planiranje revizije učinka

DODATCI

Dodatak 1. Ilustracija primjera susjedne zemlje Republike Hrvatske

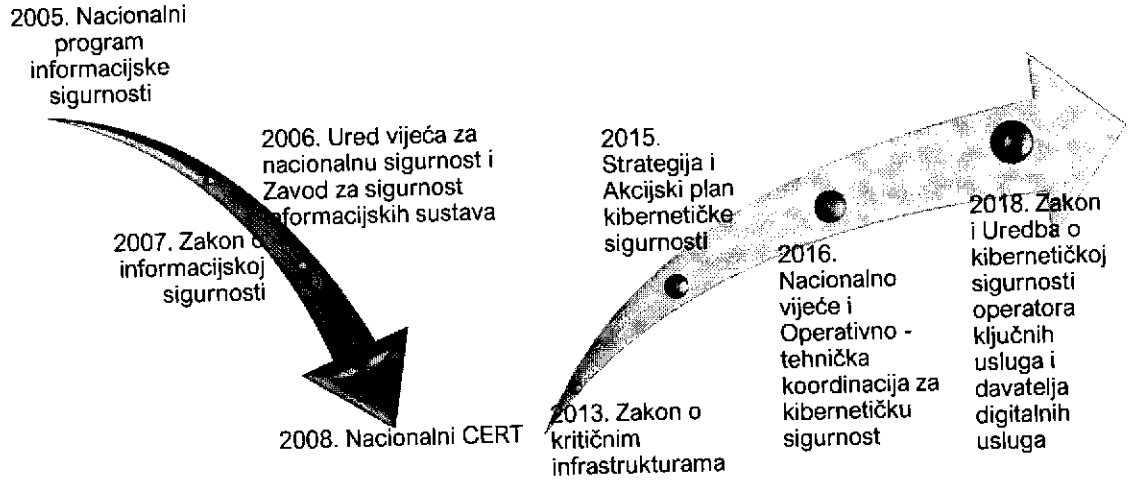
Dodatak 2. Kronologija aktivnosti Ministarstva sigurnosti BiH na izmjenama i dopunama Pravilnika o unutarnjoj organizaciji i pripreme novog Pravilnika o unutarnjoj organizaciji

Dodatak 3. Reference

Dodatak 1. Ilustracija primjera susjedne zemlje Republike Hrvatske

RH ima razrađen zakonski i organizacijski okvir kibersigurnosti. Kao zemlja članica EU i Sjevernoatlantskog saveza (NATO), RH je implementirala zakonodavstvo EU i NATO-a u oblasti kibersigurnosti. Sljedeći grafikon prikazuje vremenski tijek uspostave krovnog okvira kibersigurnosti u RH.

Grafikon 11.: Uspostava okvira kibersigurnosti u RH



Izvor: Ured za reviziju institucija BiH

Informacijska sigurnost u RH je regulirana Nacionalnim programom informacijske sigurnosti i Zakonom o informacijskoj sigurnosti.[59] Navedena regulativa je stvorila temelj za implementaciju mjera i standarda informacijske sigurnosti u RH i organizacijski ustroj. Prema tome, tijela državne uprave, lokalne i područne samouprave te pravne osobe s javnim ovlastima koja su vlasnici neklasificiranih informacijskih sustava u RH, dužni su donijeti opći akt upravljanja informacijskom sigurnošću, odrediti odgovorne osobe za upravljanje informacijskom sigurnošću, osigurati provođenje propisanih minimalnih mjera informacijske sigurnosti sukladno normama za upravljanje informacijskom sigurnošću Međunarodne organizacije za standardizaciju (ISO) 27001 i uspostaviti kanale komunikacije sa tijelima nadležnim za prevenciju i koordinaciju odgovora na računalno – sigurnosne incidente.

Djelovanje u području informacijske sigurnosti je dodatno ojačano i prošireno donošenjem Strategije i Akcijskog plana kibernetičke sigurnosti. Donošenjem Strategije kibernetičke sigurnosti, RH je sustavno pristupila provođenju aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora u skladu sa Direktivnom NIS. Stvoren je i temelj za donošenje Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kojim je osigurana provedba mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebna važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta.[60]

---

[59] Dodatno, podzakonski propisi koji reguliraju informacijsku sigurnost u RH su Uredba o mjerama informacijske sigurnosti, Smjernice za postupanje s neklasificiranim podatcima i Pravilnik o standardima sigurnosti neklasificiranih informacijskih sustava.

[60] Donesena je i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.

Djelovanje u prevenciji i zaštiti od računalnih incidenata, RH je organizacijski podijelila između dva tijela, Nacionalnog CERT-a i Zavoda za sigurnost informacijskih sustava. Ova dva tijela surađuju i razmjenjuju informacije. Sudjeluju u članstvu međunarodnih i europskih organizacija u oblasti kibersigurnosti. Surađuju i sa Nacionalnim vijećem za kibernetičku sigurnost, odnosno Uredom vijeća za nacionalnu sigurnost u čijem su sastavu, koji djeluje kao jedinstvena nacionalna kontaktna točka.

Nacionalni CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u RH, čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u RH. Nacionalni CERT se bavi i incidentima sa značajnim učinkom prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državna tijela i davatelje digitalnih usluga.

Zavod za sigurnost informacijskih sustava je središnje državno tijelo za prevenciju i zaštitu od računalnih ugroza informacijskih sustava državnih tijela RH i obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava i upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka.

Pored navedenog okvira, postoje i drugi zakonski i podzakonski propisi i tijela koji su važni za informacijsku sigurnost u RH koje zbog obimnosti nismo navodili.[61]

[61] Neki od zakonski propisa koji su važni za informacijsku sigurnost u RH su Zakon o tajnosti podataka, Zakon o zaštiti osobnih podataka, Zakon o elektroničkoj ispravi, Zakon o sigurnosnim provjerama, Zakon o sigurnosno – obavještajnom sustavu, Kazneni zakon i ostali zakonski i podzakonski propisi. Ostale institucije informacijske sigurnosti u RH su Akademska i istraživačka mreža, Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, Agencija za zaštitu osobnih podataka i Središnji državni ured za e-upravu.

Dodatak 2. Kronologija aktivnosti Ministarstva sigurnosti BiH na izmjenama i dopunama Pravilnika o unutarnjoj organizaciji i pripreme novog Pravilnika o unutarnjoj organizaciji

15. 7. 2016. godine GT prema MS	Obavijest o zaključku VM-a: VM usvojio Informaciju o aktivnostima MS-a u vezi sa kibersigurnosti i s tim u vezi, između ostalog zadužilo MS da izradi prijedloge odluka i akata unutarnje organizacije radi osiguravanja okvira za BiH CERT za institucije BiH.
8. 3. 2017. godine VM usvojio Odluku o određivanju CERT-a za institucije BiH	**U cilju realizacije Odluke, MS će u roku od tri mjeseca, od dana donošenja ove Odluke, predložiti VM-u dopunu postojećeg Pravilnika o unutarnjoj organizaciji br. 01-02-125/08 od 9. 4. 2009. godine, s ciljem uspostavljanja posebne unutarnje organizacijske jedinice u okviru Sektora za informatiku i telekomunikacijske sustave MS-a.**
19. 4. 2017. godine Pomoćnik ministra za informatiku i telekomunikacijske sustave prema Kabinetu ministra	Predmet: Informacija o potrebi izmjene i dopune Pravilnika o unutarnjoj organizaciji MS-a radi realizacije zaključka VM-a i uspostavljanja CERT-a za institucije BiH: Predmetne izmjene i dopune treba da obuhvate izmjenu naziva i opisa poslova Sektora za informatiku i telekomunikacijske sustave, postojećih unutarnjih organizacijskih jedinica – odsjeka, te pojedinih izvršilaca u Sektoru. Također, potrebno je uvođenje novog odsjeka u okviru Sektora, tj. Odsjeka za CERT i sigurnost IKT sustava i povećanje broja izvršilaca u Sektoru.
12. 6. 2017. godine MS prema Ministarstvu pravde	**Predmet: Prijedlog opisa poslova službeničkih radnih mjesta, mišljenje, traži se: Traži se mišljenje na opis poslova službeničkih radnih mjesta razvrstanih u kategorije (radna mjesta: sustav inženjeri, projektant programeri, stručni savjetnici, administratori IKT, itd.).**
12. 9. 2017. godine MS prema Ministarstvu pravde	Predmet: Hitno dostavljanje mišljenja na prijedlog opisa poslova službeničkih radnih mjesta: Traži se mišljenje na opis poslova službeničkih radnih mjesta razvrstanih u kategorije. Isti akt kao 12. 6. 2017. godine.
9. 10. 2017. godine MS prema Ministarstvu pravde	**Predmet: Hitno dostavljanje mišljenja na prijedlog opisa poslova službeničkih radnih mjesta (isto kao 12. 6. 2017. i 12. 9. 2017. godine).**
23. 10. 2017. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se: Izmjenama u pravilnik uvode novi Odsjek za CERT u okviru Sektora za informatiku i telekomunikacijske sustave, dopuna opisa poslova i opisi radnih mjesta u Sektoru.
MS prema Ministarstvu pravde	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se;
MS prema Uredu za zakonodavstvo	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se;
1. 11. 2017. godine Ured za zakonodavstvo prema MS-u	**Predmet: Mišljenje na Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji: Ured za zakonodavstvo ukazuje MS-u da je potrebno da pribavi mišljenja od MP-a i MFT-a. Istovremeno ukazuje na obavezu donošenja novih pravilnika, te na obavezu iz člana 41. Aneksa I Metodologije procjene utjecaja prilikom izrade propisa Jedinstvenih pravila za izradu pravnih propisa u institucijama BiH.**
16. 11. 2017. godine Ministarstvo pravde prema MS-u	Predmet: Mišljenje na opis poslova radnih mjesta: MP daje pozitivno mišljenje i konstatira da je prijedlog poslova svih 10 radnih mjesta pravilno sastavljen.
22. 11. 2017. godine Ministarstvo pravde prema MS-u	**Predmet: Mišljenje na Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji: MP je mišljenja da bi opravdanost formiranja novog sektora trebalo preispitati s aspekta nadležnosti MS-a.**
8. 12. 2017. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se: Izvršene korekcije koje se odnose

	na zaposlenička radna mjesta u Sektoru za informatiku i telekomunikacijske sustave, te popunjen obrazac za razvrstavanje radnih mjesta srednje stručne spreme u platne razrede za radno mjesto 10. 18. Tehničar za sigurnost IKT sustava – referent specijalista.
11. 1. 2018. godine MS prema MFT-u	**Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, dopuna, dostavlja se: Vrše dopunu sa obrascem broj 2a o fiskalnoj procjeni utjecaja, a koji se odnosi na spomenuti pravilnik.**
13. 4. 2018. godine MS prema MFT-u	Predmet: Urgencija na davanje Mišljenja na Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, traži se: Aktom od 13. 2. 2018. godine MS je dostavio objedinjen tekst Prijedloga Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a da MFT na isti da svoje mišljenje.
13. 4. 2018. godine MS prema GT-u	**Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, dostavlja se: U prilogu akta dostavljaju mišljenja nadležnih institucija, s obzirom da je pod tekućim pitanjima na 139. sjednici VM-a kao točka dnevnog reda ovaj prijedlog Pravilnika. Također, navode da u prilogu dostavljaju objedinjeni Prijedlog Pravilnika u koji su sublimirali pored Jedinice interne revizije, izmijenjene strukture organizacijske jedinice i naziva Sektora za azil, Sektora za informatiku i telekomunikacijske sustave.**
23. 5. 2018. godine MS prema MFT-u	Predmet: Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, dostavlja se: Dostavljaju na mišljenje sa izvršenom fiskalnom procjenom utjecaja za spomenuti pravilnik.
20. 7. 2018. godine MS prema MFT-u	**Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se – urgencija: Urgencija veza na akt od 23. 5. 2018. godine na koji MFT još uvijek nije odgovorilo, ni dva mjeseca nakon prvobitnog akta.**
23. 8. 2018. godine MS prema MFT-u	Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se – urgencija: Urgencija veza na akt od 23. 5. 2018. i 20. 7. 2018. godine na koje MFT nakon čak tri mjeseca nije odgovorilo. U ovoj urgenciji se MS poziva na obveze uspostave središnje kontakt točke i uspostave Odsjeka za suradnju sa Europolom, zatim na obvezu uspostave CERT-a.
30. 8. 2018. godine (zaprimljeno u MS 28. 11. 2018. godine) MFT prema MS-u	**Predmet: Mišljenje na Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a: između ostalog, nije usklađeno financijski, budući da financijska usklađenost podrazumijeva osiguranost sredstava u Proračunu institucija BiH (predloženo povećanje za 710.000 KM). MFT je mišljenja da je razvrstavanje radnog mjesta referent specijalista za prijenos tajnih podataka izvršeno suprotno odredbama Metodologije. MFT ne može podržati predloženu izmjenu, nego upućuju MS da razmotri da važeće nepopunjene pozicije zamijeni sa pozicijama radi kojih se dopunjava važeći pravilnik.**
12. 9. 2018. godine MS prema GT-u	Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, dostavlja se: MS u skladu s obvezama iz Sporazuma o suradnji s Europolom predlaže uspostavu Odsjeka za suradnju sa Europolom. Povjerenstvo Ministarstva pravde je dalo pozitivno mišljenje na opis poslova službeničkih radnih mjesta sistematiziranih u Odsjeku za suradnju s Europolom. Za sistematizaciju Odsjeka za CERT i sigurnosti IKT sustava dato je pozitivno mišljenje Ureda za zakonodavstvo i Ministarstva pravde. Uspostavlja se i Jedinica interne revizije u skladu sa Zakonom o internoj reviziji institucija BiH za šta je dato pozitivno mišljenje MFT-a, Ureda za zakonodavstvo i Povjerenstva Ministarstva pravde za analizu opisa poslova radnih mjesta državnih službenika. U Sektoru za azil, Odsjeku

	za prihvat i program, neophodno je povećanje broja izvršilaca. Neophodno je formirati Odsjek za Središnji registar. Mišljenje MFT-a nije dostavljeno za ovu izmjenu. Na Pravilnik koji obuhvata sve izmjene i dopune koje su prethodno rađene u fazama zatraženo je mišljenje svih nadležnih institucija. Opisi poslova službeničkih radnih mjesta usklađeni su sa mišljenjem Povjerenstva Ministarstva pravde koja je nadležna za analizu opisa poslova radnih mjesta državnih službenika, izuzev tri radna mjesta sistematizirana u Odsjeku za središnji registar, Sektora za zaštitu tajnih podataka. Mišljenje MFT-a nije dostavljeno, iako je zatraženo 23. 5. 2018. godine, te urgirano 20. 7. 2018. i 23. 8. 2018. godine. Mišljenje Ureda za zakonodavstvo od 26. 6. 2018. godine je uvaženo i ugrađeno, osim razvrstavanja ovih radnih mjesta u odgovarajuće odsjeke.
19. 9. 2018. godine GT prema MS-u	**Predmet: Dopuna materijala, traži se: Nedostaje mišljenje MFT-a sa obrascem 2a o fiskalnoj procjeni utjecaja. Napomena da po potrebi pribave inovirana mišljenja nadležnih institucija u slučajevima kada je pozitivnost prethodnih mišljenja bila uvjetovana ugradnjom određenih sugestija.**
24. 9. 2018. godine MS prema GT-u	Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, odgovor, dostavlja se: Posebno se ističe da je u smislu realizacije Sporazuma o suradnji između Europola i BiH obveza MS-a da najkasnije do 30. 9. 2018. godine uspostavi Odsjek za suradnju sa Europolom. Istakli su da je izostala suradnja Ministarstva pravde (na traženo mišljenje i dvije urgencije, tri mjeseca poslije im odgovorili da ne mogu dati mišljenje dok se ne dovrši postupak razvrstavanja službeničkih radnih mjesta) i suradnja sa MFT-om (na traženo mišljenje i dvije urgencije do ovog datuma nije stigao odgovor).
25. 12. 2018. godine MS prema MFT-u	**Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, mišljenje, traži se: U skladu s mišljenjem MFT-a od 30. 8. 2018. godine (koji je MS zaprimio 28. 11. 2018.) MS prihvata primjedbe i sugestije date na razvrstavanje zaposleničkih radnih mjesta u platne razrede, kao i konstataciju da je potrebno za svako zaposleničko radno mjesto precizirati kategoriju. Uz prijedlog Pravilnika je dostavljen i Obrazac 2a o fiskalnoj procjeni učinka.**
21. 1. 2019. godine MS prema MFT-u	Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a, dopuna, traži se: U prilogu akta je dostavljen Obrazac 2a o fiskalnoj procjeni učinka kao i obrazac za razvrstavanje radnih mjesta srednje stručne spreme u platne razrede C3, C4, C5.
29. 1. 2019. godine MFT prema MS-u	**Predmet: Mišljenje na Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a: MFT je mišljenja da je razvrstavanje radnog mjesta referent specijalista za prijenos tajnih podataka izvršeno suprotno odredbama Metodologije. MFT sugerira da se za svako zaposleničko radno mjesto precizira kategorija i da se ista uskladi sa platnim razredom za koju je dobivena suglasnost. Potrebno je ograničiti radne zadatke i odgovornost Odsjeka za CERT samo na informacijske sustave MS-a. U dijelu Pravilnika koji se odnosi na Odsjek za suradnju s Europolom, isti nije usklađen sa Zakonom o Direkciji za koordinaciju policijskih tijela. MFT podržava financijski aspekt prijedloga pravilnika u dijelu koji se odnosi na sistematiziranje pozicija JIR i u Sektoru za azil, ali istovremeno upućuje predlagatelja da umjesto predloženog broja izvršilaca i sistematiziranja tri odsjeka razmotri sistematiziranje drugih unutarnjih organizacijskih jedinica sa manjim brojem izvršilaca.**

11. 11. 2019. godine MS prema GT-u	Predmet: Prijedlog Pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS, dostavlja se: U prilogu akta su obligatorna mišljenja nadležnih institucija. U skladu sa mišljenjima nadležnih institucija iz ovog prijedloga izostavljene su izmjene i dopune kojima bi se uspostavio Odsjek za suradnju s Europolom i Odsjek za središnji registar, tako da ovaj Pravilnik o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji obuhvaća: uspostavu Jedinice interne revizije, izmjene u Sektoru za azil u smislu povećanja broja izvršilaca i uspostavu Odsjeka za CERT i sigurnost IKT sustava.
15. 11. 2019. godine GT prema MS-u	**Predmet: Upit, dostavlja se: Uvidom u evidencije GT-a konstatira da već imaju zaprimljen Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS od 12. 9. 2018. godine. S tim u vezi potrebno je da se MS hitno izjasni da li prethodno dostavljeni Prijedlog navedenog pravilnika povlači iz procedure razmatranja na sjednicama VM-a kako bi bilo jasno i nedvosmisleno koji od predloženih materijala bi članovi VM-a trebali razmotriti i o istom se izjašnjavati na sjednici.**
30. 12. 2019. godine GT prema MS-u	Predmet: Pregled materijala, dostavlja se: Pregled materijala zaključno sa 26. 12. 2019. godine, na kojem je između ostalog i Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS (stari prijedlog).
6. 1. 2020. godine Kabinet ministra svim sektorima MS i upravnim organizacijama u sastavu MS-a	**Predmet: Pregled materijala i zahtjev za mišljenjem, traži se: Zahtjev za kratkim obrazloženjem vezano za materijal koji će se naći na sjednici VM-a. Od sektora i ostalih se, između ostalog, traži da obrazlože razloge zbog kojih neka od navedenih točaka treba ostati u proceduri ili ju je potrebno vratiti radi dorade.**
8. 1. 2020. godine Kabinetu ministra MS-a	Predmet: Pregled materijala i zahtjeva za mišljenjem, dostavlja se: Pomoćnik ministra za Sektora za informatiku i telekomunikacijske sustave upućuje Kabinetu ministra da je između ostalog, Prijedlog pravilnika o unutarnjoj organizaciji potrebno razmotriti po hitnom postupku.
8. 1. 2020. godine Kabinet ministra MS prema GT-u	**Pregled: Obavijest o aktima koji su u prethodnom razdoblju dostavljeni u GT, dostavlja se: Obavijest za GT da iz daljnje procedure, radi ažuriranja i dopune, povlače, između ostalog i Prijedlog pravilnika o izmjenama i dopunama Pravilnika o unutarnjoj organizaciji MS-a (zaprimljen 15. 11. 2018. godine).**
8. 10. 2020. godine Ministar sigurnosti donosi Odluku o formiranju radne skupine za pripremu Prijedloga pravilnika o unutarnjoj organizaciji MS-a	Formira se Radna skupina za pripremu prijedloga Pravilnika o unutarnjoj organizaciji MS-a. Radna skupina je dužan pripremiti Prijedlog pravilnika u roku od 30 dana i blagovremeno i u što kraćem roku dostaviti uz Izvješće o urađenom u Kabinet ministra. Na sastanku stručnog kolegija MS-a koji je održan 16. 9. 2020. godine zatraženo je formiranje Radne grupe za pripremu prijedloga Pravilnika o unutarnjoj organizaciji MS-a.
15. 10. 2020. godine Ministar sigurnosti donosi Odluku o izmjeni Odluke o formiranju radne skupine	**Mijenja se tajnik Radne skupine. Ostali dijelovi Odluke ostaju nepromijenjeni.**
26. 11. 2020. godine Radna skupina za izradu Prijedloga	Zapisnik: Između ostalog, utvrđeno je, da je obzirom na obiman materijal, pitanja koja se reguliraju, usuglašavaju sa važećom zakonskom i podzakonskom regulativom, potrebno duže vremensko

pravilnika o unutarnjoj organizaciji MS-a	razdoblje za pripremu Prijedloga pravilnika. Članovi Radne skupine predlažu da se prvobitno uradi procjena primjene postojeće sistematizacije, te u odnosu na rezultate, vrši i izmjena Pravilnika.
21. 1. 2021. godine Radna skupina za izradu Prijedloga pravilnika o unutarnjoj organizaciji MS-a	**Zapisnik: između ostalog, Radna skupina se upoznala sa sadržajem prijedloga Usporedne analize važećeg Pravilnika o unutarnjoj organizaciji sa dostavljenim materijalima ispred Sektora. Ispred svakog sektora su predložene određene izmjene, a ispred Sektora za informatiku i telekomunikacijske sustave predloženo je povećanje broja izvršilaca, koje se najviše odnosi na uspostavljanje CERT-a. Svi prisutni članovi mišljenja su da treba opravdati povećanje predloženih radnih mjesta i razmotriti mogućnost i opravdanu potrebu objedinjavanja određenih odsjeka i sektora po srodnosti poslova u skladu sa navedenim odlukama o načelima i kriterijima. Na sastanku je iznesen i stav Kabineta da sistematizacija i unutarnja organizacija treba ići u okviru važećih radnih mjesta koja su nepopunjena, a da male korekcije po pitanju radnih mjesta nisu problem.**
10. 2. 2021. godine Radna skupina za izradu Prijedloga pravilnika o unutarnjoj organizaciji MS-a	Na dnevnom redu ovog sastanka Radne skupine bila je samo jedna točka i to razmatranje obima nadležnosti Inspektorata kao organizacijske jedinice u sastavu MS-a. Nije bilo drugih točaka dnevnog reda.
5. 3. 2021. godine Radna skupina za izradu Prijedloga pravilnika o unutarnjoj organizaciji MS-a	**Pored razmatranja informacija sa sastanka zainteresiranih sektora u pogledu obima nadležnosti Inspektorata, također je predsjedavajuća obavijestila prisutne da će opisi radnih mjesta sektora biti sastavni dio Aneksa pravilnika, te da je potrebno u što kraćem roku dostaviti obrazloženja i obrasce od strane sektora koji to do sada nisu učinili. U skladu sa diskusijom, usvojen je Zaključak:** **1. Dostaviti Kabinetu ministra Prijedlog pravilnika o unutarnjoj organizaciji,** **2. Dostaviti Izvješće sa dostavljenim obrazloženjima od strane sektora Kabinetu ministra, a koji se tiču usporedne analize važećeg Pravilnika i Prijedloga pravilnika o unutarnjoj organizaciji,** **3. Predložiti Kabinetu ministra da se formira uža Radna skupina od tri člana koja će dalje nastaviti rad na realizaciji Prijedloga pravilnika.**
22. 3. 2021. godine Predsjedavajuća Radne skupine dostavlja Informaciju o rezultatima Kabinetu ministra	Radna skupina je pripremila Prijedlog pravilnika o unutarnjoj organizaciji, osnovni tekst uz napomenu da će se Aneks pravilnika – sistematizacija radnih mjesta naknadno pripremiti u ovisnosti od konačno utvrđenog broja radnih mjesta i Izvješće u formi usporedne analize po sektorima važećeg Pravilnika sa Prijedlogom pravilnika predloženim od strane svih sektora. Također se, između ostalog, predlaže formiranje uže Radne skupine od tri člana koja će dalje nastaviti rad na realizaciji Prijedloga pravilnika.
10. 5. 2021. godine Ministar sigurnosti donosi Odluku o formiranju Uže radne skupine koja će nastaviti rad na pripremi prijedloga Pravilnika o unutarnjoj organizaciji MS-a	**Formira se uža Radna skupina koja će nastaviti dalji rad na pripremi Prijedloga pravilnika o unutarnjoj organizaciji. Radna skupina je dužna poslove na pripremi Prijedloga pravilnika okončati blagovremeno, u što kraćem roku, dostaviti Izvješće o urađenom u Kabinet ministra sigurnosti. Ovom Odlukom stavljaju se izvan snage Odluka o formiranju Radne skupine za pripremu prijedloga Pravilnika o unutarnjoj organizaciji od 8. 10. 2020. godine i Odluka o izmjeni Odluke o formiranju Radne skupine za pripremu Prijedloga pravilnika o unutarnjoj organizaciji od 15. 10. 2020. godine.**

Dodatak 3. Reference

1. Akcijski plan 1 uz Strategiju reforme javne uprave, 2006. godina <https://parco.gov.ba/hr/dokumenti/rju-dokumenti/akcioni-plan-1-uz-strategiju-reforme-javne-uprave/> Pristupljeno 9. 9. 2022. godine
2. Akcijski plan za razdoblje 2018. – 2022. godina, 2020. godina <https://parco.gov.ba/hr/rju/o-rju-2/strateski-okviri-za-rju/> Pristupljeno 9. 9. 2022. godine
3. Akt Europske Unije o kibersigurnosti, 2019. godina <https://eur-lex.europa.eu/legal-content/HR/LSU/?uri=CELEX:32019R0881> Pristupljeno 9. 9. 2022. godine
4. Arbanas K. "Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti" Disertacija, Sveučilište u Zagrebu, Fakultet organizacije i informatike, 2021. godine
5. Bosna i Hercegovina i Europska Unija, Sporazum o stabilizaciji i pridruživanju, 2008. godina <https://www.dei.gov.ba/bs/stabilization-agreement> Pristupljeno 9. 9. 2022. godine
6. Direkcija za europske integracije, Finalno izvješće o realizaciji akcijskog plana za realizaciju prioriteta iz analitičkog izvješća Europske Komisije, 2020. godina
7. Direktiva 2016/1148 Europskog parlamenta i Vijeća, Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, 2016. godina <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148#document1> Pristupljeno 9. 9. 2022. godine
8. Europska Komisija, Izvješće o Bosni i Hercegovini za 2021. godinu, 2021. godina <https://www.dei.gov.ba/uploads/documents/izvjestaj-o-bosni-i-hercegovini-za-2021-godinu_1636467943.pdf> Pristupljeno 9. 9. 2022. godine
9. Global Cyber Security Capacity Centre in collaboration with the World Bank, "Cybersecurity capacity review Bosnia and Herzegovina", March 2019
10. International Telecommunication Union, "Readiness assessment report to establish a CIRT network in Bosnia and Herzegovina", August 2018
11. ISO (2018) ISO/IEC 27000:2018(en): Information technology — Security techniques — Information security management systems — Overview and vocabulary, Velika Britanija: ISO, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Pristupljeno 9. 9. 2022. godine
12. Konvencija o kibernetičkom kriminalu, Službeni glasnik Bosne i Hercegovine – Međunarodni ugovori broj: 06/06, 2006. godina
13. Ministarstvo sigurnosti Bosne i Hercegovine, „Analiza o usklađenosti pravnih propisa iz oblasti kibersigurnosti u Bosni i Hercegovini", 2017. godina
14. Odluka o određivanju Tima za odgovor na računalne incidente za institucije Bosne i Hercegovine, Službeni glasnik Bosne i Hercegovine, broj 25/17, 2017. godina
15. Odluka o osnivanju i imenovanju ekspertne radne skupine za izvršenje svih neophodnih priprema za formiranje CERT tijela u Bosni i Hercegovini, Službeni glasnik Bosne i Hercegovine, broj 06/12, 2011. godina
16. Odluka o usvajanju Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017. – 2022. godine, Službeni glasnik Bosne i Hercegovine, broj 38/17, 2017. godina
17. Pravilnik o unutarnjoj organizaciji i sistematizaciji Ministarstva sigurnosti Bosne i Hercegovine, broj: 01-02-125/09, 2009. godina

18. Program reformi Bosne i Hercegovine za razdoblje 2019. – 2020. godina, 2019. godina
19. Smjernice za strateški okvir kibersigurnosti u Bosni i Hercegovini, 2022. godina
20. Središnji državni ured za e-Hrvatsku, „Nacionalni program informacijske sigurnosti u Republici Hrvatskoj“, 2005. godina
21. Strategija i Akcijski plan kibernetičke sigurnosti Republike Hrvatske, Narodne novine 108/2015, 2015. godina
22. Strategija uspostave CERT-a u Bosni i Hercegovini, 2011. godina
23. Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine 68/2018, 2018. godina
24. Zakon o informacijskoj sigurnosti Republike Hrvatske, NN 79/07, 2007. godina
25. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga Republike Hrvatske, Narodne novine 64/2018, 2018. godina
26. Zakon o kritičnim infrastrukturama Republike Hrvatske, Narodne novine 56/2013, 2013. godina
27. Zakon o ministarstvima i drugim tijelima uprave Bosne i Hercegovine, Službeni glasnik Bosne i Hercegovine, broj 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09, 87/12, 6/13, 19/16 i 83/17, 2003. godina