Prilog II

Izvješće o provedenoj analizi (samoprocjeni) usklađenosti sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti

Sadržaj

1. Uvod

Ovaj dokument predstavlja izvješće o GAP analizi usklađenosti Hrvatske agencije za poljoprivredu i hranu (u daljnjem tekstu HAPIH) sa Zakonom o kibernetičkoj sigurnosti NN 14/2024 i Uredbom o kibernetičkoj sigurnosti NN 135/2024, kojom se u hrvatsko zakonodavstvo prenosi Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije (Direktiva NIS2).
Uredba o kibernetičkoj sigurnosti utvrđuje mjerila i kriterije za razvrstavanje subjekata, mjere upravljanja kibernetičkim sigurnosnim rizicima, način njihove provedbe, obveze vezane uz izvještavanje o značajnim incidentima, vođenje popisa ključnih i važnih subjekata te provođenje samoprocjena kibernetičke sigurnosti. Cilj joj je povećati otpornost organizacija na kibernetičke prijetnje, unaprijediti zaštitu mrežnih i informacijskih sustava te osigurati kontinuitet pružanja usluga u slučaju incidenata.
S obzirom na rastuće regulatorne zahtjeve i sve složenije kibernetičke prijetnje, usklađenost s ovim zakonskim okvirom postaje ključan strateški cilj za organizacije u Republici Hrvatskoj. Kroz ovo izvješće organizacija dobiva jasne smjernice o potrebnim prilagodbama i preporukama za unaprjeđenje sustava upravljanja kibernetičkom sigurnošću i operativnom otpornošću. Ovo Izvješće identificira trenutno stanje HAPIH-a u odnosu na zahtjeve Zakona i Uredbe o kibernetičkoj sigurnosti te ukazuje na područja koja zahtijevaju poboljšanja.

2. Pojmovi i skraćenice

BCP (Business Continuity Plan) – Plan kojim se osigurava nastavak ili brza ponovna uspostava ključnih poslovnih procesa u slučaju prekida
BIA (Business Impact Analysis) – Analiza kojom se utvrđuju ključni poslovni procesi, posljedice njihova prekida i ciljevi oporavka
DRP (Disaster Recovery Plan) – Plan oporavka informacijskih sustava, infrastrukture i podataka nakon ozbiljnog incidenta
GAP analiza – Analiza odstupanja između trenutačnog stanja i regulatornih zahtjeva kibernetičke sigurnosti
HAPIH – Hrvatska agencija za poljoprivredu i hranu
IKT – Informacijsko-komunikacijska tehnologija
Kibernetička sigurnost – Skup mjera za zaštitu mrežnih i informacijskih sustava, podataka i usluga od prijetnji u kibernetičkom prostoru
MAO (Maximum Acceptable Outage) – Maksimalno prihvatljivo trajanje prekida poslovnog procesa
RPO (Recovery Point Objective) – Najveći dopušteni gubitak podataka izražen u vremenu
RTO (Recovery Time Objective) – Ciljano vrijeme oporavka poslovnog procesa ili sustava
SDO (Service Delivery Objective) – Minimalna prihvatljiva razina usluge tijekom prekida ili oporavka
SLA (Service Level Agreement) – Ugovorena razina usluge s vanjskim dobavljačem

3. Opseg analize usklađenosti

Ova GAP analiza obuhvaća procjenu usklađenosti HAPIH-a sa zahtjevima Zakona i Uredbe o kibernetičkoj sigurnosti (Prilog II. Uredbe). Fokus analize je na ključnim područjima regulative, uključujući:

- Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima
- Upravljanje programskom i sklopovskom imovinom
- Upravljanje kibernetičkim sigurnosnim rizicima
- Sigurnost ljudskih potencijala i digitalnih identiteta
- Osnovne prakse kibernetičke higijene
- Osiguravanje kibernetičke sigurnosti mreže
- Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima
- Sigurnost lanca opskrbe
- Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava
- Kriptografija
- Postupanje s incidentima
- Kontinuitet poslovanja i upravljanje kibernetičkim krizama
- Fizička sigurnost

3. Metodologija provedbe analize

Evaluacija usklađenosti provedena je kroz sustavnu GAP analizu, koja uključuje sljedeći metodološki pristup:

- **Pregled relevantnih odredbi Zakona i Uredbe** – analiza regulatornih zahtjeva i obveza za ključne i važne subjekte.
- **Usporedba s postojećim politikama i praksama** – pregled i analiza internih politika, procedura, smjernica i implementiranih sigurnosnih mjera i kontrola u organizaciji.
- **Intervjui i konzultacije** – provođenje razgovora s ključnim dionicima HAPIH-a, kako bi se steklo dodatno razumijevanje postojećih procesa i izazova u usklađenju s regulativom.
- **Identifikacija kritičnih slabosti** – utvrđivanje područja gdje postoje odstupanja od regulatornih zahtjeva, kako s aspekta dokumentiranosti tako i s aspekta implementiranosti konkretnih organizacijskih i tehničkih mjera.
- **Prijedlog preporuka za poboljšanja** – definiranje konkretnih mjera za rješavanje utvrđenih nedostataka, kroz akcijski plan provedbe usklađivanja HAPIH-a.

Ova metodologija nadopunjuje se specifično definiranim smjernicama Naručitelja (HAPIH) za učinkovitu provedbu aktivnosti usklađivanja sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti, a iste se prepoznaju kroz sljedeće korake:

- **Analiza interne dokumentacije** – pregled svih internih akata, pravilnika i politika Naručitelja koji se odnose na upravljanje informacijskom sigurnošću, zaštitu laboratorijskih podataka, kontinuitet rada laboratorija i odgovora na incidente.
- **Identifikacija ključnih poslovnih procesa** – definirati kritične laboratorijske i administrativne procese čije neometano funkcioniranje osigurava provedbu ispitivanja, verifikaciju rezultata, sigurnost hrane te javnozdravstveni nadzor. Provodi se sveobuhvatna analiza utjecaja na poslovanje (Business Impact Analysis – BIA).
- **Procjena sigurnosti fizičkih i digitalnih lokacija** – provjera postojećih sigurnosnih mjera na laboratorijskim lokacijama, centrima za obradu podataka, uzorkovnim mjestima i skladištima uzoraka, uključujući zaštitu od fizičkih i digitalnih prijetnji.
- **Analiza ugovora s trećim stranama** – pregled ugovornih odnosa s vanjskim dobavljačima IKT usluga, održavanja laboratorijskih sustava i digitalne infrastrukture, s ciljem procjene njihove usklađenosti s kibernetičkim sigurnosnim zahtjevima te otpornosti na incidente.
- **Procjena sigurnosti dobavljačkog lanca** – utvrditi potrebu za nadzorom ili revizijom trećih strana koje imaju pristup kritičnim laboratorijskim informacijskim sustavima, u skladu s načelima i obvezama iz Zakona o kibernetičkoj sigurnosti, Uredbe o kibernetičkoj sigurnosti i Direktive o mrežnoj i informacijskoj sigurnosti (NIS2).
- **Analiza sektorskih specifičnosti** – prepoznati specifične izazove zdravstvenog sektora poput osjetljivosti podataka o zdravlju, zakonskih obveza zaštite podataka, potrebe za očuvanjem kontinuiteta laboratorijskih analiza te suradnje s nacionalnim i međunarodnim tijelima.
- **Procjena prijetnji ključnim uslugama** – evidentiranje mogućih scenarija koji bi mogli ugroziti ključne laboratorijske funkcije, digitalno izvještavanje i sigurnosne protokole te procijeniti njihov potencijalni utjecaj na stabilnost usluga.
- **Analiza postojećih planova i procedura** – identificiranje i procjena postojećih dokumenata relevantnih za izradu Plana kontinuiteta poslovanja (Business Continuity Plan – BCP) i Plana oporavka od ugroza (Disaster Recovery Plan – DRP), posebno usmjerene na rad laboratorijskih i IT sustava.

Slijedeći ovu metodologiju, osigurano je da su rezultati GAP analize prikazani u ovom dokumentu temeljeni na procjeni postojećih politika, procedura, sigurnosnih mjera i kontrola implementiranih u organizaciji te da su rezultati analize jednoznačno usporedivi sa zahtjevima Zakona i Uredbe o kibernetičkoj sigurnosti. Na temelju utvrđenih nedostataka, kroz akcijski plan usklađenja, formulirat će se preporuke za poboljšanje koje će HAPIH-u omogućiti uspješnu tranziciju prema punoj usklađenosti.

4. Uključene strane

U provođenju ove GAP analize sudjelovali su sljedeći ključni dionici:

- **Predstavnici HAPIHA**: odgovorne osobe za područje kibernetičke sigurnosti i upravljanja informacijskim sustavima, kao i predstavnici relevantnih poslovnih sektora, službi ili odjela.
- **Vanjski konzultanti i stručnjaci**: neovisni stručnjaci za kibernetičku sigurnost i regulativu Zavoda za informatičku djelatnost Hrvatske.

5. Rezultati analize usklađenosti

Sukladno Zakonu i Uredbi o kibernetičkoj sigurnosti, obveznici Zakona, kategorizirani kao važni subjekti, s aspekta dokumentiranosti implementiranih mjera kibernetičke sigurnosti, trebaju imati izrađen i usvojen minimalni set dokumentacije sustava kibernetičke sigurnosti.
U okviru provedene GAP analize usklađenosti sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti (Prilog II., mjere 1–13), izvršen je pregled postojeće interne dokumentacije HAPIH-a koja se odnosi na upravljanje informacijskom/kibernetičkom sigurnošću.
Analiza je pokazala da HAPIH posjeduje određene elemente dokumentacije i operativne prakse koje djelomično adresiraju zahtjeve Uredbe, no da nedostaje cjelovit, formalno uspostavljen i međusobno povezan sustav dokumenata kibernetičke sigurnosti, kako to zahtijeva regulatorni okvir.

5.1 Analiza interne dokumentacije

Na temelju rezultata GAP analize utvrđeno je sljedeće:

- Postoji formalni akt imenovanja odgovorne osobe za kibernetičku sigurnost (Administrator za kibernetičku sigurnost), s naglaskom na obveze prijave značajnih incidenata i komunikaciju s nadležnim tijelima.
- Provodi se (na poslovnoj razini) upravljanje informacijskom imovinom, ali ne postoji dokumentirana metodologija upravljanja informacijskom imovinom niti uspostavljen i održavan registar informacijske imovine te nije provedena sigurnosna klasifikacija po kritičnosti informacijske imovine.
- Postoje operativne IT procedure i dobre prakse (HelpDesk, upravljanje korisničkim zahtjevima, osnovna trijaža sigurnosnih događaja), no one nisu objedinjene u formalnu proceduru upravljanja incidentima.
- Dio organizacijskih i procesnih pravila proizlazi iz postojećih ISO sustava upravljanja (npr. ISO 9001), ali isti nisu mapirani na zahtjeve kibernetičke sigurnosti niti formalno integrirani u sustav upravljanja kibernetičkim rizicima.
- Upravljanje kibernetičkim rizicima provodi se implicitno kroz IT i organizacijske odluke, ali ne postoji formalna metodologija procjene rizika, niti Registar kibernetičkih rizika.

- Internim aktima definirano je i provode se dobre sigurnosne prakse pri novom zapošljavanju ili promjeni radnog mjesta postojećih zaposlenika, postoje zapisi zaduženja i razduženja opreme.
- Upravljanje pristupima, korisničkim pravima i autentifikacijom postoji na tehničkoj razini, ali ne postoji jedinstvena politika ili procedura kontrole pristupa.
- Najvećim dijelom slijede se dobre prakse osnovne kibernetičke higijene, ali iste nisu formalno dokumentirane/propisane.
- Postoje ugovori/sporazumi s ključnim IKT dobavljačima, ali nije uspostavljen i ne prati se registar izravnih IKT dobavljača, niti je propisano (dokumentirano) upravljanje IKT dobavljačima.
- Evidentiranje događaja i nadzor (logiranje) provodi se tehnički, ali nije regulirano internim aktom koji definira opseg, odgovornosti, zadržavanje dnevničkih zapisa (logova) i nadzor.
- Dobro je dokumentiran i uspostavljen postupak internog razvoja informacijskih sustava, samo isti treba dopuniti sa sigurnosnog aspekta.
- Provedena je Analiza utjecaja prekida poslovnih procesa (BIA), kojom su definirani RTO, RPO, SDO i MAO za ključne i potporne procese HAPIH-a, što predstavlja važan temelj za uspostavu sustava kontinuitet poslovanja.
- Kontinuitet poslovanja postoji na analitičkoj razini (provedena je BIA), ali nije formaliziran kroz Plan kontinuiteta poslovanja (BCP) i Plan oporavka IKT sustava (DRP), niti su predviđena testiranja planova.
- Implementirane su mjere fizičke sigurnosti, ali iste nisu formalno i dokumentirane.

Sukladno nalazima GAP analize i zahtjevima Priloga II. Uredbe o kibernetičkoj sigurnosti, utvrđeno je da HAPIH-u nedostaju sljedeći ključni dokumenti sustava kibernetičke sigurnosti, a isti su nužni za dokazivu usklađenost:

Temeljni strateški dokumenti

- **Politika kibernetičke sigurnosti HAPIH-a** kao krovni dokument **te tematske politike** (zasebno ili kao sastavni dio krovne Politike kibernetičke sigurnosti HAPIH-a:
    - *Politika upravljanja informacijskom imovinom*
    - *Politika upravljanja rizicima*
    - *Politika postupanja s incidentima*
    - *Politika upravljanja lozinkama i MFA*
    - *Politika kontrole pristupa*
    - *Politike za upravljanje povlaštenim računima i računima za administraciju sustava*
    - *Politika sigurnosti lanca opskrbe*
    - *Politika upravljanja kriptografijom*
    - *Politika kontinuiteta poslovanja*
    - *Politika fizičke sigurnosti*

Operativne procedure/pravila/metodologije

- Procedura/Pravila/Metodologija upravljanja rizicima kibernetičke sigurnosti
- Procedura/Pravila/Metodologija upravljanja informacijskom imovinom
- Procedura/Pravila upravljanja kibernetičkim incidentima (uključujući prijavu, obradu, evidenciju i učenje iz incidenata)
- Procedura/Pravila upravljanja digitalnim identitetima
- Procedura/Pravila za logičku i fizičku kontrolu pristupa
- Procedura/Pravila upravljanja lozinkama i MFA
- Procedura/Pravila upravljanja osnovnom kibernetičkom higijenom (radne upute za korištenje: e-mail-a i web pretraživača – resursa na internetu, prijenosnih medija, rada na daljinu, prijenosni računalnih i telekomunikacijskih uređaja, upute za zaštitu od zloćudnog softvera, itd.)
- Procedura/Pravila upravljanja ranjivostima i sigurnosnim ažuriranjima
- Procedura/Pravila za upravljanje promjenama u informacijskim i mrežnim sustavima
- Procedura/Pravila upravljanja sigurnošću mreže
- Procedura/Pravila upravljanja kriptografijom
- Procedura/Pravila upravljanja dnevničkim zapisima
- Procedura/Pravila upravljanja sigurnošću u lancu opskrbe (dobavljači IKT i laboratorijskih sustava)
- Procedura/Pravila upravljanja sigurnosnim kopijama (backup procedura) i oporavkom podataka te redudantnim resursima
- Procedura/Pravila fizičke zaštite

Planovi kontinuiteta i otpornost

- Plan kontinuiteta poslovanja (BCP)
- Plan oporavka od katastrofe / oporavka IKT sustava (DRP)
- Plan testiranja i održavanja planova kontinuiteta i oporavka

Krizno upravljanje i komunikacija

- Plan upravljanja kibernetičkim krizama i komunikacijom u slučaju kibernetičkog incidenta

Upravljanje ljudskim potencijalima

- Program/Plan osposobljavanja i podizanja svijesti zaposlenika o kibernetičkoj sigurnosti
- Evidencija provedenih edukacija i provjera znanja

Registri:

- Registar informacijske imovine
- Registar rizika
- Registar izravnih IKT dobavljača

Revizije, Izvještavanje, Unaprjeđenje sustava kibernetičke sigurnosti

- Dokumentirane metrike kibernetičke sigurnosti
- Obrazac – Izvještaj o stanju kibernetičke sigurnosti
- Obrazac – Procjena usklađenosti ugovora/sporazuma s ključnim IKT dobavljačima

Zaključak

Na temelju provedene GAP analize zaključuje se da HAPIH:

- posjeduje određene pojedinačne elemente i operativne prakse relevantne za kibernetičku sigurnost,
- međutim ne posjeduje cjelovit, sustavno uređen i dokumentiran sustav kibernetičke sigurnosti, kako to zahtijevaju Zakon i Uredba o kibernetičkoj sigurnosti,
- ključni nedostatak odnosi se na izostanak formalnih politika, procedura i planova, osobito u području upravljanja informacijskom imovinom, kibernetičkim rizicima, incidentima te kontinuitetom poslovanja.

Iz navedenog proizlazi potreba za izradom i usvajanjem cjelovitog skupa internih akata kibernetičke sigurnosti HAPIH-a.

5.2 Identifikacija ključnih poslovnih procesa - BIA

Svi detaljni nalazi, metodologija i pojedinačne analize po HAPIH poslovnim procesima dokumentirani su u zasebnom dokumentu **„Izvješće_Analiza utjecaja prekida procesa_20251215“**. U nastavku se daje sažeti prikaz ključnih rezultata provedene analize utjecaja na poslovanje (Business Impact Analysis – BIA), s naglaskom na identifikaciju ključnih laboratorijskih i administrativnih procesa HAPIH-a te njihov značaj za osiguravanje kontinuiteta poslovanja, sigurnosti hrane i javnozdravstvenog nadzora.

Provedba i obuhvat BIA analize

Analiza utjecaja na poslovanje provedena je kao sveobuhvatna procjena utjecaja prekida temeljnih poslovnih procesa HAPIH-a u slučaju izvanrednih događaja, uključujući scenarije potpune ili djelomične nedostupnosti ICT infrastrukture, aplikativnih sustava, opreme ili fizičkih lokacija. Analiza je provedena u skladu s pristupom „najgoreg mogućeg scenarija“, s ciljem utvrđivanja stvarne otpornosti organizacije i prioriteta oporavka. U okviru BIA-e su prikupljeni i obrađeni podaci o:

- međuovisnostima temeljnih, potpornih i upravljačkih poslovnih procesa,
- operativnim, financijskim, regulatorno-pravnim, reputacijskim i organizacijskim posljedicama prekida poslovanja,
- ključnim resursima potrebnima za održavanje minimalne razine rada,

- ciljevima oporavka poslovnih procesa, uključujući vrijeme oporavka (RTO), dopušteni gubitak podataka (RPO), minimalnu razinu usluge (SDO) i maksimalno dopušteno trajanje prekida (MAO).

Identifikacija ključnih poslovnih procesa

Provedenom analizom identificirani su temeljni poslovni procesi koji imaju ključnu ulogu u osiguravanju neometanog rada HAPIH-a, provedbi laboratorijskih ispitivanja, verifikaciji rezultata, sigurnosti hrane i provedbi javnozdravstvenog nadzora. Analizirani procesi obuhvaćaju laboratorijske, administrativne, potporne i upravljačke funkcije, čime je osigurano cjelovito sagledavanje utjecaja prekida na poslovanje organizacije.

Među identificiranim procesima nalaze se:

- laboratorijski procesi ispitivanja (npr. ispitivanje plodnosti tla, analiza vina, ispitivanje kvalitete sirovog mlijeka, fitosanitarni nadzor, kontrola i praćenje GMO-a),
- administrativni i regulatorni procesi (npr. upis u registre, priznavanje sorti poljoprivrednog bilja, financijsko-planski i računovodstveni poslovi),
- potporni procesi (npr. poslovni proces IT podrške, tehnički poslovi i poslovi održavanja),
- upravljački procesi (upravljanje HAPIH-om i koordinacija ključnih poslovnih aktivnosti).

Za svaki od analiziranih procesa procijenjena je razina kritičnosti i tolerancija na prekid, pri čemu su pojedini procesi identificirani kao vremenski i regulatorno osjetljiviji zbog izravnog utjecaja na zakonske obveze, sigurnost hrane i dostupnost javnih usluga.

Rezultat analize utjecaja prekida poslovanja

Rezultati BIA analize (**Izvješće_Analiza utjecaja prekida procesa_20251215**) pokazuju da prekid poslovnih procesa HAPIH-a može imati različite razine utjecaja, ovisno o vrsti i trajanju prekida. U analizi su identificirani procesi kod kojih kratkotrajni prekidi imaju ograničen utjecaj, ali i procesi kod kojih dulji prekidi mogu dovesti do značajnih regulatornih, operativnih i reputacijskih posljedica.

Za sve analizirane procese definirani su mjerljivi ciljevi oporavka:

- RTO, kao maksimalno dopušteno vrijeme potrebno za uspostavu minimalne razine rada procesa,
- RPO, kao maksimalno dopušteni gubitak podataka u slučaju prekida,
- SDO, kao minimalna razina usluge prihvatljiva tijekom trajanja prekida,
- MAO, kao maksimalno dopušteno vrijeme potpunog ili djelomičnog prekida pružanja usluga.

Analiza je također identificirala ključne ovisnosti pojedinih procesa o ljudskim resursima, informacijskim sustavima, laboratorijskoj opremi, vanjskim dobavljačima i infrastrukturi, čime je osigurana jasna osnova za planiranje mjera kontinuiteta poslovanja i oporavka (izradu planova kontinuiteta poslovanja te plana KT oporavka).

Zaključak

Provedena analiza utjecaja na poslovanje potvrđuje da je HAPIH sustavno identificirao ključne poslovne procese te procijenio posljedice njihovog prekida, uz jasno definirane ciljeve oporavka i potrebne resurse. Time je uspostavljena kvalitetna i dokumentirana osnova (**Izvješće_Analiza utjecaja prekida procesa_20251215**) za upravljanje kontinuitetom poslovanja u skladu sa zahtjevima kibernetičke sigurnosti.

BIA rezultati predstavljaju temelj za daljnje aktivnosti usklađivanja, osobito u dijelu formalizacije planova kontinuiteta poslovanja, planova oporavka od katastrofa i postupaka upravljanja kibernetičkim krizama, kako bi se osigurala potpuna usklađenost sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti.

5.3 Procjena sigurnosti fizičkih i digitalnih lokacija

Procjena sigurnosti fizičkih i digitalnih lokacija provedena je s ciljem utvrđivanja postojećih mjera zaštite na laboratorijskim lokacijama, lokacijama za obradu i pohranu podataka, uzorkovnim mjestima te skladištima uzoraka, uključujući zaštitu od fizičkih i digitalnih prijetnji. Procjena je obuhvatila mjere fizičke sigurnosti prostora i opreme, kao i mjere logičke sigurnosti informacijskih sustava i mrežne infrastrukture, s naglaskom na kontrolu pristupa i nadzor. Sve navedeno je provedeno u procesu GAP analize usklađenosti, prikupljanjem relevantnih informacija od odgovornih osoba HAPIH-a.

Sigurnost digitalnih lokacija i logička kontrola pristupa

Na razini informacijskih sustava i mrežne infrastrukture utvrđeno je da u HAPIH-u postoje uspostavljene operativne prakse upravljanja logičkim pristupom i korisničkim pravima. Dodjela i korištenje pristupnih prava provode se u praksi kroz postojeće informacijske sustave i organizacijske dogovore, a za dio sustava primjenjuju se i specifične procedure povezane s vanjskim regulatornim ili sektorskim zahtjevima.

Međutim, upravljanje logičkim pristupom nije objedinjeno u formaliziran i dokumentiran sustav na razini cijele organizacije. Ne postoji jedinstveni interni akt ili procedura koja bi jasno definirala pravila dodjele, izmjene i ukidanja korisničkih prava, razine pristupa, odgovornosti za odobravanje pristupa te obvezu redovitih revizija dodijeljenih prava. Upravljanje digitalnim identitetima i privilegiranim korisničkim računima provodi se parcijalno, bez jedinstvenog dokumentiranog okvira.

U području nadzora pristupa i sigurnosnih događaja, evidentiranje dnevničkih zapisa (logiranje) se provodi na razini pojedinih sustava i aplikacija, no ne postoji centralizirani sustav nadzora niti jedinstvena procedura koja definira opseg logiranja, razdoblja čuvanja zapisa, odgovornosti za pregled i postupanje po zabilježenim događajima. Ne postoji centralizirani sustav (SIEM) za korelaciju sigurnosnih događaja, što ograničava mogućnost cjelovitog nadzora i pravodobnog uočavanja složenijih sigurnosnih incidenata.

Analiza utjecaja na poslovanje dodatno potvrđuje da su ključne digitalne komponente i informacijska infrastruktura prepoznate kao kritične ovisnosti za kontinuitet rada većine poslovnih procesa, osobito u dijelu upravljanja identitetima, dostupnosti aplikacija, sigurnosnih kopija podataka i mrežne povezanosti.

Sigurnost fizičkih lokacija

U području fizičke sigurnosti utvrđeno je da HAPIH nema formalno uspostavljenu i objedinjenu politiku fizičke sigurnosti koja bi definirala razine zaštite po vrstama prostora, mjere fizičke kontrole pristupa, odgovornosti, način nadzora i periodiku provjere učinkovitosti primijenjenih mjera. Fizička sigurnost laboratorija, serverskih prostora, skladišta uzoraka i ostalih relevantnih prostora provodi se kroz pojedinačne mjere i praksu, ali bez jedinstvenog dokumentiranog okvira.

U praksi su prisutne mjere fizičke kontrole pristupa određenim prostorima, uključujući korištenje fizičkih i elektroničkih brava te ograničavanje pristupa ovlaštenim osobama. Zaduženja pristupnih sredstava evidentiraju se po osobama, no ne postoji centralizirana evidencija događaja fizičkog pristupa (dnevnički zapisi) koja bi omogućila naknadnu analizu ulazaka i izlazaka iz kritičnih prostora. Kao formalno uređen segment fizičke sigurnosti postoji pravilnik o video nadzoru, kojim su definirane uloge i odgovornosti, pravila pristupa snimkama i razdoblja čuvanja snimljenog materijala. Osim video nadzora, ostali sustavi tehničke zaštite (npr. protuprovalni sustavi) nisu obuhvaćeni jedinstvenim pravilnikom koji bi definirao njihovu primjenu, održavanje i nadzor. Evidentiranje događaja fizičkog pristupa putem tehničkih sustava nije u cijelosti uspostavljeno, a zapisi protuprovalnih sustava čuvaju se ograničeno vrijeme (. Protuprovalni/alarmni sustav je uspostavljen s čuvanjem zapisa približno 15 dana (sukladno procjeni rizika i raspoloživim resursima), dok je za sustav video nadzora navedena obveza čuvanja logova 5 godina, a snimke se čuvaju približno 10 dana).

Nalazi provedene analize utjecaja na poslovanje (BIA) dodatno naglašavaju važnost fizičke dostupnosti i sigurnosti infrastrukturnih resursa na više lokacija, uključujući serverske prostore i laboratorije, kao preduvjet za kontinuitet ključnih poslovnih procesa.

Zaključak

Na temelju provedene procjene zaključuje se da HAPIH ima implementirane pojedinačne mjere fizičke i logičke sigurnosti koje u praksi doprinose zaštiti laboratorijskih lokacija, digitalnih resursa i ključne infrastrukture. Istodobno je utvrđeno da sustav zaštite nije cjelovito formaliziran i dokumentiran na organizacijskoj razini.

Ključni nedostaci odnose se na izostanak jedinstvenih i formalno uspostavljenih politika i procedura za:

- kontrolu logičkog pristupa informacijskim sustavima i upravljanje digitalnim identitetima,
- centralizirano upravljanje i nadzor dnevničkih zapisa sigurnosnih događaja,
- fizičku sigurnost prostora, uključujući razine zaštite, protokole pristupa i evidenciju događaja fizičkog pristupa,
- sustavno upravljanje i dokumentiranje mjera tehničke zaštite na fizičkim lokacijama.

Utvrđeni nalazi ukazuju da je za postizanje potpune i dokazive usklađenosti potrebno uspostaviti i dokumentirati jedinstveni sustav kontrole fizičkog i logičkog pristupa te formalizirati politike i procedure fizičke sigurnosti za sve kritične lokacije i resurse HAPIH-a.

5.4 Analiza ugovora s trećim stranama i procjena sigurnosti dobavljačkog lanca

Analiza ugovornih odnosa HAPIH-a s trećim stranama provedena je s ciljem procjene u kojoj mjeri vanjski dobavljači IKT usluga i proizvoda, održavanja laboratorijskih sustava i digitalne infrastrukture doprinose ukupnoj razini kibernetičke sigurnosti HAPIH-a te koliko su ugovorni odnosi usklađeni s kibernetičkim sigurnosnim zahtjevima i otpornošću na incidente. Analiza je obuhvatila postojeće ugovorne i operativne odnose s vanjskim pružateljima usluga koji imaju pristup informacijskim sustavima, laboratorijskoj opremi, podacima ili infrastrukturi HAPIH-a, odnosno čiji rad ima izravan ili neizravan utjecaj na kontinuitet poslovanja.

Pregled postojećih ugovornih odnosa i prakse

Na temelju rezultata GAP analize utvrđeno je da HAPIH koristi usluge vanjskih dobavljača u području informacijsko-komunikacijske infrastrukture, aplikativne podrške, održavanja laboratorijskih sustava te telekomunikacijskih i infrastrukturnih usluga. Ovi dobavljači predstavljaju važnu vanjsku ovisnost, osobito za procese koji su identificirani kao ključni ili vremenski osjetljivi.

U praksi su ugovoreni odnosi usmjereni prvenstveno na dostupnost usluge, tehničku podršku i održavanje sustava, uz definirane razine usluge (SLA) za pojedine segmente. Međutim, GAP analiza pokazuje da ugovori s trećim stranama u pravilu ne sadrže sustavno i standardizirano definirane odredbe koje bi se odnosile na kibernetičku sigurnost u širem smislu, uključujući upravljanje sigurnosnim incidentima, obveze izvještavanja, zahtjeve za zaštitu podataka i pristupa, te provjeru usklađenosti dobavljača s relevantnim sigurnosnim standardima.

Usklađenost s kibernetičkim sigurnosnim zahtjevima

U dijelu usklađenosti s kibernetičkim sigurnosnim zahtjevima, utvrđeno je da ne postoji formalno uspostavljena i dokumentirana procedura za procjenu kibernetičkih rizika povezanih s trećim stranama prije sklapanja ugovora, niti tijekom trajanja ugovornog odnosa. Ne provodi se sustavna procjena sigurnosne zrelosti dobavljača, niti su definirani kriteriji prema kojima bi se dobavljači klasificirali s obzirom na razinu rizika za HAPIH.

Ugovori u pravilu ne sadrže jasno definirane obveze dobavljača u vezi s:

- primjenom minimalnih mjera kibernetičke sigurnosti,
- upravljanjem i prijavom kibernetičkih incidenata koji mogu utjecati na HAPIH,
- ograničavanjem i nadzorom logičkog i fizičkog pristupa sustavima i podacima HAPIH-a,
- osiguravanjem kontinuiteta usluge i oporavka u slučaju incidenta ili prekida rada.

Ovakvo stanje upućuje na to da se sigurnosni zahtjevi prema IKT dobavljačima trenutačno rješavaju fragmentirano, kroz tehničke i operativne dogovore, bez formalnog dokumentiranog okvira koji bi bio u potpunosti usklađen s kibernetičkim sigurnosnim zahtjevima.

Otpornost dobavljača na incidente i kontinuitet poslovanja

Nalazi analize utjecaja na poslovanje (BIA) pokazuju da su pojedini vanjski dobavljači ključne ovisnosti za kontinuitet rada HAPIH-a, osobito u dijelu IT podrške, aplikativnih rješenja, laboratorijskih informacijskih sustava i mrežne infrastrukture. Prekid ili nedostupnost usluga tih dobavljača može imati značajan utjecaj na sposobnost HAPIH-a da ispuni svoje regulatorne i operativne obveze unutar definiranih ciljeva oporavka.

Unatoč prepoznatoj važnosti dobavljača, u postojećim ugovornim odnosima nisu sustavno definirani zahtjevi vezani uz otpornost dobavljača na incidente, planove kontinuiteta poslovanja i oporavka od katastrofa, niti obveze sudjelovanja dobavljača u testiranjima kontinuiteta ili oporavka. Također, nisu jasno definirani postupci koordinacije i komunikacije u slučaju kibernetičkog incidenta koji uključuje ili pogađa vanjskog dobavljača.

Zaključak analize ugovora s trećim stranama

Na temelju provedene analize zaključuje se da HAPIH ima uspostavljene operativne ugovorne odnose s trećim stranama koje su nužne za funkcioniranje IT sustava, laboratorijskih procesa i digitalne infrastrukture, no ti odnosi nisu cjelovito uređeni s aspekta kibernetičke sigurnosti i zahtjeva koje propisuje Uredba o kibernetičkoj sigurnosti, Mjera 8.

Ključni nedostaci odnose se na izostanak:

- formalne i dokumentirane politike upravljanja sigurnošću u lancu opskrbe,
- sustavne procjene kibernetičkih rizika povezanih s trećim stranama,
- standardiziranih ugovornih odredbi o kibernetičkoj sigurnosti, incidentima, kontinuitetu i zaštiti pristupa,
- jasnih zahtjeva vezanih uz otpornost dobavljača na incidente i njihovu ulogu u oporavku poslovanja.

Utvrđeni nalazi ukazuju na potrebu uspostave strukturiranog pristupa upravljanju odnosima s trećim stranama, uključujući formalizaciju sigurnosnih zahtjeva u ugovorima, kako bi se osigurala usklađenost s Uredbom kibernetičke sigurnosti i smanjili rizici koji proizlaze iz ovisnosti HAPIH-a o vanjskim dobavljačima.

5.5 Analiza sektorskih specifičnosti

U kontekstu djelatnosti HAPIH-a, sektorske specifičnosti kibernetičke sigurnosti proizlaze iz činjenice da se velik dio poslovanja oslanja na laboratorijske i terensko-laboratorijske procese, na obradu i razmjenu rezultata analiza te na sustave i baze podataka koje podržavaju regulatorne obveze i javni interes, uključujući aspekte sigurnosti hrane i utjecaja na zdravlje ljudi. Zbog navedenog, prekidi rada ili kompromitacija podataka mogu imati izražen regulatorno-pravni i reputacijski utjecaj, osobito kod duljih prekida, što je potvrđeno kroz BIA rezultate (**Izvješće Analiza utjecaja prekida procesa_20251215**) za procese koji se u dokumentaciji opisuju kao regulatorno osjetljivi.

Osjetljivost podataka i zakonske obveze zaštite podataka

U poslovnim procesima obrađuju se elektronički podaci i rezultati laboratorijskih analiza pohranjeni u bazama podataka te se podaci razmjenjuju s vanjskim dionicima i sustavima. U pojedinim procesima eksplicitno su prepoznati ključni skupovi podataka (npr. rezultati analiza, baze podataka za provedbu nadzora i deklariranja, uključujući GMO relevantne podatke), uz definirane ciljeve povrata podataka (RPO) i režime sigurnosnih kopija. Ovakvi skupovi podataka zahtijevaju pojačanu zaštitu povjerljivosti, cjelovitosti i dostupnosti, kao i dokazivost postupanja u slučaju incidenta, s obzirom na moguće posljedice na ispunjenje regulatornih obveza i povjerenje javnosti.

Potreba za očuvanjem kontinuiteta laboratorijskih analiza

Kontinuitet laboratorijskih procesa je sektorski ključan zbog oslanjanja na specifičnu laboratorijsku opremu, povezane radne stanice, specijalizirani softver, aplikacije za evidenciju uzoraka i rezultate te centralizirane baze podataka. BIA je za više laboratorijskih i regulatorno osjetljivih procesa definirala ciljeve oporavka u rasponu od 48 do 72 sata (RTO), uz minimalne razine usluge (SDO) i maksimalno dopuštene zastoje (MAO), te je naglasila da se utjecaj prekida značajno povećava kod prekida duljih od 72 sata i posebno nakon tjedan dana. To upućuje da su otpornost infrastrukture, dostupnost laboratorijske opreme i stabilnost IT okruženja preduvjet za održavanje regulatorno važnih aktivnosti i pravodobnu isporuku rezultata.

Suradnja s nacionalnim i međunarodnim tijelima i vanjskim sustavima

Sektorska specifičnost očituje se i kroz povezanost poslovnih procesa s vanjskim sustavima i dionicima. U BIA nalazima su identificirane vanjske ovisnosti koje uključuju dvosmjernu razmjenu podataka s vanjskim informacijskim sustavima (npr. sustavi u domeni nadležnih tijela), kao i ovisnost o dobavljačima laboratorijskih kemikalija, održavanju laboratorijske opreme, aplikativnoj podršci i telekomunikacijskim uslugama sa SLA. Uz to, regulatorni okvir kibernetičke sigurnosti propisuje obveze pravodobnog obavještavanja o značajnim incidentima, uključujući procjenu prekograničnog i međusektorskog učinka kada je primjenjivo, što dodatno naglašava potrebu za jasnim postupcima koordinacije i komunikacije s nadležnim tijelima.

Zaključak

Sektorski specifični izazovi HAPIH-a usmjereni su na zaštitu i dostupnost laboratorijskih podataka i rezultata, očuvanje kontinuiteta laboratorijskih i regulatornih procesa te upravljanje ovisnostima o vanjskim sustavima i dobavljačima. Ovi izazovi zahtijevaju da mjere kibernetičke sigurnosti budu usmjerene na otpornost ključne infrastrukture, pouzdane mehanizme oporavka podataka i procesa te na učinkovite postupke upravljanja incidentima i komunikacije prema nadležnim tijelima i relevantnim dionicima.

5.6 Procjena prijetnji ključnim uslugama

Procjena kibernetičkih prijetnji ključnim uslugama HAPIH-a provedena je s ciljem identificiranja mogućih scenarija koji bi mogli ugroziti ključne laboratorijske funkcije, digitalno izvještavanje i sigurnosne protokole HAPIH-a te procjene njihovog potencijalnog utjecaja na stabilnost i kontinuitet pružanja usluga. Procjena se temelji na nalazima GAP analize i rezultatima analize utjecaja na poslovanje (BIA), pri čemu su u fokusu bile usluge i procesi koji su identificirani kao vremenski, regulatorno ili operativno osjetljivi.

Potencijalne ranjivosti i kibernetičke prijetnje

U kontekstu laboratorijskih i povezanih administrativnih procesa identificirani su sljedeći relevantni kritični scenariji - rizici:

- nedostupnost ili degradacija ključnih informacijskih sustava i aplikacija koje podržavaju laboratorijske analize, obradu uzoraka i digitalno izvještavanje,
- kompromitacija ili gubitak podataka o rezultatima analiza, bazama podataka i evidencijama koje se koriste u regulatornim i nadzornim postupcima,
- prekid rada ili oštećenje laboratorijske opreme i prateće IT infrastrukture zbog tehničkih kvarova, nestanka napajanja ili neadekvatnih uvjeta rada,
- kibernetički incidenti koji mogu dovesti do neovlaštenog pristupa, izmjene ili nedostupnosti podataka i sustava,
- ovisnost o vanjskim dobavljačima IT usluga, aplikativne podrške, laboratorijskih sustava i telekomunikacijskih veza, čiji prekid ili incident može uzrokovati lančane poremećaje u pružanju usluga,
- neadekvatna koordinacija i komunikacija u slučaju incidenta, što može produžiti vrijeme oporavka i povećati regulatorne i reputacijske posljedice.

Procjena utjecaja na stabilnost HAPIH usluga

Rezultati analize utjecaja na poslovanje (**Izvješće_Analiza utjecaja prekida procesa_20251215**) pokazuju da kratkotrajni prekidi pojedinih procesa u pravilu imaju ograničen utjecaj, dok se kod duljih prekida (posebno nakon 72 sata i nakon tjedan dana) utjecaj značajno povećava. U tim slučajevima dolazi do izraženih operativnih zastoja, povećanja zaostataka u obradi uzoraka, rasta regulatorno-pravnog i reputacijskog rizika te smanjenja sposobnosti HAPIH-a da pravodobno ispunjava svoje zakonske i javne obveze.

Za više ključnih laboratorijskih i administrativnih procesa definirani su ciljevi oporavka u rasponu od 48 do 72 sata, što ukazuje da prijetnje koje uzrokuju prekide dulje od navedenih rokova predstavljaju značajan rizik za stabilnost HAPIH usluga. Posebno su osjetljivi procesi koji ovise o centraliziranim bazama podataka, aplikacijama za evidenciju i izvještavanje te specijaliziranoj laboratorijskoj opremi, jer njihova nedostupnost ima neposredan učinak na više povezanih procesa istodobno.

Utjecaj na sigurnosne protokole i regulatorne obveze

U identificiranim rizičnim scenarijima prepoznat je i rizik od narušavanja sigurnosnih protokola, uključujući mogućnost otežanog nadzora, kašnjenja u otkrivanju sigurnosnih događaja i otežanog pravodobnog odgovora na incidente. Takvi scenariji mogu dovesti do neusklađenosti s regulatornim obvezama, osobito u pogledu zaštite podataka, izvještavanja i dokazivosti postupanja u slučaju značajnog incidenta.

Zaključak

Procjena prijetnji ključnim uslugama HAPIH-a pokazuje da su najveći rizici povezani s nedostupnošću i kompromitacijom informacijskih sustava, ovisnošću o vanjskim dobavljačima te produženim prekidima rada laboratorijske i digitalne infrastrukture. Identificirani rizični scenariji mogu imati značajan negativan utjecaj na stabilnost usluga, osobito kod duljih prekida, te naglašavaju potrebu za jačanjem otpornosti ključnih sustava, jasnim definiranim postupcima odgovora na incidente i osiguravanjem kontinuiteta laboratorijskih i digitalnih funkcija. Detaljan pregled i procjenu razine pojedinih rizika HAPIH će uspostaviti kroz Registar rizika kibernetičke sigurnosti“, a prethodno propisati „Metodologiju upravljanja rizicima kibernetičke sigurnosti“, što trenutno u HAPUH-u nedostaje.

5.7 Analiza postojećih planova i procedura

Provedenom GAP analizom je utvrđeno da su u HAPIH-u prisutne pojedine implementirane aktivnosti kontinuiteta i oporavka, ali bez cjelovitog, formalno usvojenog i dokumentiranog okvira BCP/DRP planova te bez sustavnog testiranja takvih planova. Kroz sustav kvalitete (ISO 9001) dokumentirani su određeni elementi organizacije rada i postupanja, a provedena analiza utjecaja na poslovanje (BIA) rezultirala je definiranjem ciljeva oporavka i kontinuiteta po ključnim procesima (RTO, RPO i SDO), što predstavlja temeljnu ulaznu podlogu za izradu BCP-a i DRP-a.

U dijelu operativne provedbe kontinuiteta i oporavka utvrđeno je da su u praksi implementirane aktivnosti koje podržavaju BC i DR, uključujući sigurnosne kopije i oporavak u skladu s definiranim ciljevima (npr. RTO 24 sata na razini ključnih IT funkcija, uz RPO utvrđen po procesima kroz BIA). Primjenjuje se i geografska dislociranost resursa i sigurnosnih kopija između lokacija (primarna uz sekundarne lokacije i distribuirane informacijske sustave), pri čemu se dio sustava vodi na jednoj lokaciji, a sigurnosne kopije na drugoj. Također su evidentirane mjere osiguranja napajanja na lokacijama (operativan agregat na primarnoj lokaciji te UPS sustavi na ostalim lokacijama s autonomijom približno 30 minuta). Za određene segmente podrške oslanja se i na ugovorne odnose s vanjskim dobavljačima, uz definirana vremena odziva.

Unatoč navedenim operativnim mjerama, utvrđeno je da ne postoje formalno definirani i usvojeni BCP i DRP planovi na razini organizacije, niti su definirane procedure aktivacije, koordinacije, oporavka i povratka na redovno stanje koje bi objedinjavale laboratorijske i IT potrebe. Dodatno, ne postoji jedinstveno dokumentirana procedura koja bi na razini cijelog HAPIH-a standardizirala zahtjeve, odgovornosti i korake vezane uz pričuvno kopiranje, oporavak i redundanciju (uključujući opis opsega, učestalosti, lokacija pohrane, kontrole ispravnosti pričuvnih kopija te postupke obnove).

U dijelu testiranja utvrđeno je da se zbog nepostojanja formalno usvojenih BCP i DRP planova posljedično ne provode ni planirana sustavna testiranja tih planova. Nakon izrade i usvajanja BCP-a i DRP-a potrebno je uspostaviti i dokumentirati procedure redovitog testiranja, uključujući evidenciju provedenih vježbi i poboljšanja temeljem rezultata testiranja, posebno za scenarije koji utječu na laboratorijske procese, baze podataka, aplikacije i ključnu infrastrukturu.

6. Zaključna ocjena

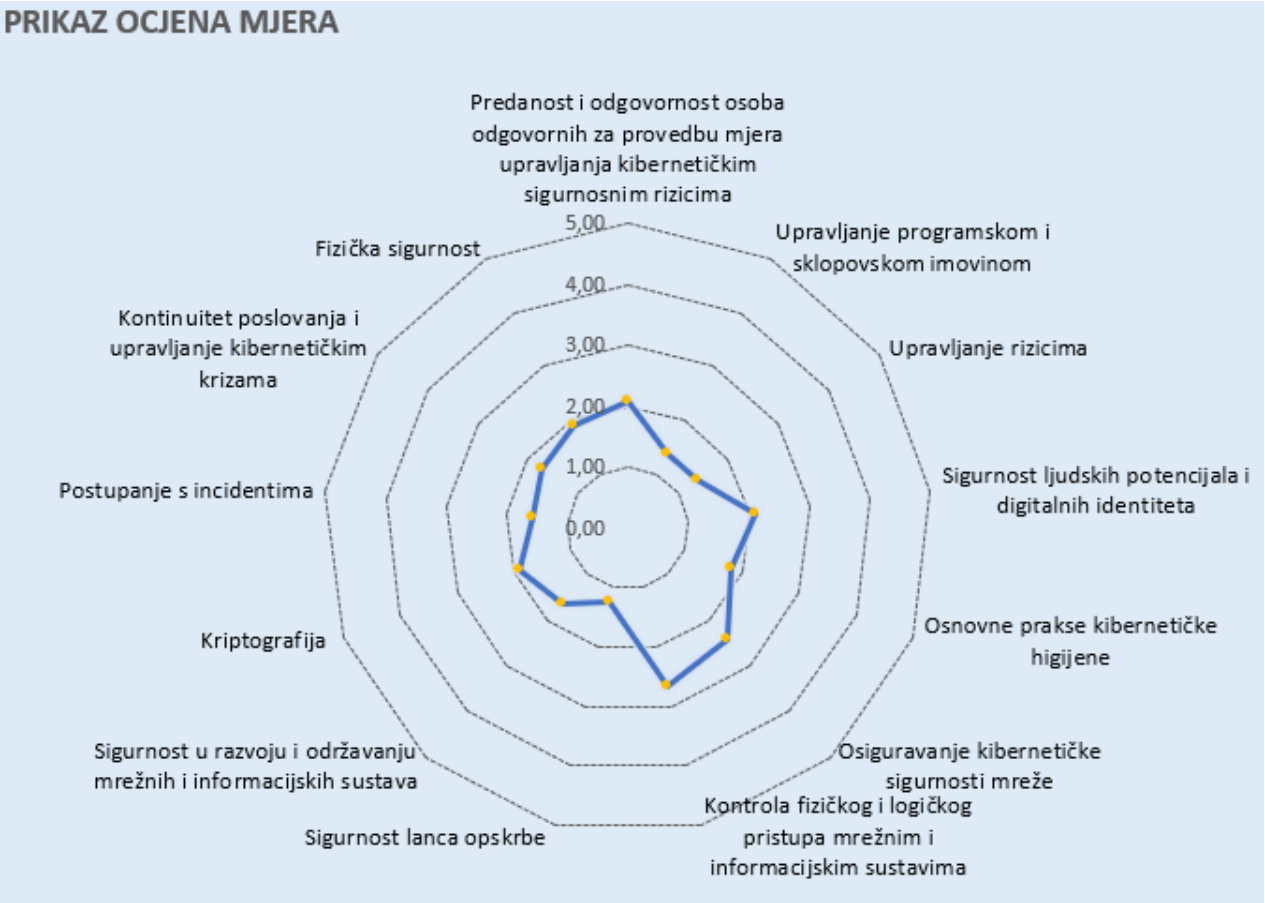
Provedenom analizom utvrđeno je da HAPIH u praksi ima implementiran značajan broj mjera kibernetičke sigurnosti koje operativno doprinose zaštiti informacijskih sustava, laboratorijskih procesa i digitalne infrastrukture. Te mjere uključuju tehničke i organizacijske kontrole u području upravljanja IT sustavima, sigurnosnih kopija i oporavka, osnovne kontrole pristupa, fizičku zaštitu pojedinih prostora te operativne mehanizme podrške i reakcije na poremećaje u radu.
Istodobno, GAP analiza je pokazala da kibernetička sigurnost u HAPIH-u trenutačno nije uspostavljena kao cjelovit, sustavno uređen i formalno dokumentiran sustav u smislu zahtjeva Zakona o kibernetičkoj sigurnosti i Uredbe o kibernetičkoj sigurnosti. Ključni nedostatak ne odnosi se primarno na izostanak tehničkih mjera, već na izostanak jedinstvenog upravljačkog okvira, formalizacije i međusobnog povezivanja postojećih praksi kroz jasno definiranu i usvojenu dokumentaciju sustava kibernetičke sigurnosti.
Kao ključna područja u kojima je potrebna daljnja formalizacija i jačanje sustavnog pristupa identificirana su, među ostalim:

- osiguravanje ljudskih resursa za upravljanje informacijskom sigurnošću, primarno kroz uspostavu funkcije „Voditelj informacijske sigurnosti“ za kontinuirano, sustavno provođenje politika i procedura kibernetičke sigurnosti za cijeli HAPIH te po potrebi i tima osposobljenih zaposlenika u ovom području,
- uspostava i usvajanje temeljnih politika i procedura kibernetičke sigurnosti (upravljanje rizicima, incidentima, kontinuitetom i oporavkom),
- formalno upravljanje kibernetičkim rizicima, uključujući dokumentiranu metodologiju i registar rizika,
- jasno definirani i dokumentirani postupci kontrole logičkog i fizičkog pristupa,
- sustavno upravljanje sigurnošću u odnosima s trećim stranama i dobavljačima,
- formalizacija planova kontinuiteta poslovanja i oporavka od ugroza, uz redovito testiranje, jačanje organizacijskih i administrativnih mjera, uključujući uloge, odgovornosti, edukaciju zaposlenika i postupke krizne komunikacije.

U okviru ove analize HAPIH je, kao važan subjekt prema nacionalnoj kategorizaciji, proveo samoprocjenu razine usklađenosti s mjerama kibernetičke sigurnosti sukladno propisanim pravilima i alatu regulatora (Zavod za sigurnost informacijskih sustava). Samoprocjena je provedena i dokumentirana kroz dokument **„Prilog A – Kalkulator samoprocjene_20251215“**.

Trenutačna razina usklađenosti kibernetičke sigurnosti po pojedinim područjima i mjerama Uredbe. Raspon usklađenosti od minimalnih „1“ do maksimalnih „5“.

#	MJERA	OCJENA	RAZINA
1	Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima	2,08	SREDNJA
2	Upravljanje programskom i sklopovskom imovinom	1,39	SREDNJA
3	Upravljanje rizicima	1,40	SREDNJA
4	Sigurnost ljudskih potencijala i digitalnih identiteta	2,11	SREDNJA
5	Osnovne prakse kibernetičke higijene	1,80	SREDNJA
6	Osiguravanje kibernetičke sigurnosti mreže	2,44	SREDNJA
7	Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima	2,65	SREDNJA
8	Sigurnost lanca opskrbe	1,25	SREDNJA
9	Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava	1,63	SREDNJA
10	Kriptografija	1,90	SREDNJA
11	Postupanje s incidentima	1,57	SREDNJA
12	Kontinuitet poslovanja i upravljanje kibernetičkim krizama	1,72	SREDNJA
13	Fizička sigurnost	1,90	SREDNJA
#	UKUPNI BODOVI STUPNJA USKLAĐENOSTI MJERA UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA HAPIH-a	**1,83**	



Rezultati prve samoprocjene predstavljaju početnu referentnu točku za daljnji razvoj sustava kibernetičke sigurnosti HAPIH-a. Sukladno regulatornim obvezama, HAPIH je dužan provoditi samoprocjenu najmanje jednom u dvije godine te kroz ponovljene procjene, koristeći propisani alat regulatora, sustavno pratiti napredak u jačanju kibernetičke sigurnosti, razinu usklađenosti i učinkovitost provedenih mjera kroz vrijeme.
Ovo izvješće predstavlja temeljni ulazni dokument za izradu **Akcijskog plana usklađivanja**, koji će biti izrađen temeljem sveobuhvatne analize identificiranih nalaza. Akcijski plan će definirati konkretne mjere i aktivnosti, potrebne resurse i odgovornosti, jasan vremenski okvir provedbe te prioritizaciju mjera prema razini identificiranog rizika i njihovom utjecaju na kontinuitet laboratorijskih i administrativnih funkcija.

7. Referentna dokumentacija

- Zakon o kibernetičkoj sigurnosti (NN 14/2024)
- Uredba o kibernetičkoj sigurnosti (135/2024)