Panel „Preparations for the NIS2 directive“ - Izvješće

Panel je održan na konferenciji DEEP u Zadru, 25. listopada 2023. od 14:30 do 16:10. Panel je vodio Stjepan Groš, a na njemu su sudjelovali:

- Ana Balaško (HEP ODS d.o.o.)
- Marko Grbić (LNG Hrvatska d.o.o.)
- Ivan Kalinić (Diverto d.o.o.)
- Aleksandar Klaić (Centar za kibernetičku sigurnost SOA-e)
- Mario Kozina (Hrvatska narodna banka)
- Dario Rajn (Podravka d.d.)

Izvješće s panela sastavio je moderator Stjepan Groš.

Sažetak i Zaključak

Tijekom panela utvrđeno je kako za uspješno usklađivanje za novim ZKS-om treba prvo imati uspostavljenu upravljačku strukturu u organizaciji. Dakle, svi koji nemaju funkciju voditelja sigurnosti ili nešto slično, prvo bi trebali nju uspostaviti.

Novi ZKS, kao i pripadajuća uredba, neće uvjetovati korištenje neke specifične norme za upravljanje informacijskom sigurnošću, a neće ni biti s njima u konfliktu. S obzirom na to, zaključak panela je da se predlaže organizacijama usklađivati sa ISO27001, a ako imaju OT sustave onda i sa ISA62443. Usklađivanjem s bar jednom od tih normi, ili obje, značajno će približiti svaku organizaciju usklađenosti i sa novim ZKS-om.

Posebno značajan izazov koji će donijeti nova regulativa je nadzor dobavljača. To je nešto novo o čemu treba razmišljati što ranije. Naime, s dobavljačima se obično dogovaraju višegodišnji ugovori te je teško te ugovore mijenjati nakon što se potpišu. S obzirom da u ovom trenutku nema modela koji bi se mogao koristiti po pitanju informacijske sigurnosti, na panelu je istaknuto kako prehrambena industrija ima već dulji niz godina regulativu s kojom im je nametnuta obaveza kontrole dobavljača. Svakako se čini oportunim proučiti taj sustav i vidjeti na koji način bi se znanja i iskustva mogla prenijeti na područje informacijske sigurnosti.

Usklađivanje zahtjeva i ulaganje će vrlo vjerojatno biti izazov mnogima. Trebat će uvjeriti svoje uprave da investiraju, iako nemaju direktnog povrata investicije. Kao mogućnost olakšavanja te situacije istaknuto je postojanje Europskih fondova.

Kroz buduće panele svaka od ovih tema može se dodatno razraditi.

Svrha i ciljevi panela

S obzirom na značaj direktive NIS2 za Republiku Hrvatsku i dionike u RH, a čija transpozicija u zakonodavni sustav RH je u tijeku, na raznim konferencijama raspravlja se o toj problematici. Organizatori konferencije DEEP su uočili kako se dosta raspravlja o raznim aspektima uvođenja i budućeg provođenja direktive NIS2 u RH, ali da nema nikakvih aktivnosti koje bi pomogle obveznicima budućeg Zakona o kibernetičkoj sigurnosti da se započnu pripremati za prilagodbu odredbama Zakona i pripadajućih akata. Iz tog razloga svrha panela bila je pomoći budućim obveznicima da se što ranije započnu pripremati za novu regulativu kako bi što bezbolnije prošli kroz to razdoblje uvođenja i prilagodbe. Pri tome je temeljni izazov za početak usklađivanja činjenica da nije još u potpunosti poznat cijeli pravni okvir, što se svakako mora uzeti u obzir. Nadalje, odlučeno je kako rezultat panela mora biti takav da svima onima koji ga budu poslušali da konkretne smjernice za daljnje postupanje.

Kroz konzultacije s panelistima te uz poznavanje najboljih praksi upravljanja informacijskom sigurnošću u organizacijama definirani su sljedeći ciljevi panela:

1. Prisutnoj publici na panelu skrenuti pozornost kako je organizacijski i upravljački okvir ključan.

2. Odrediti je li usklađivanje po ISO27001 i ISA62443 normama moguć korak prema usklađenosti sa budućim Zakonom o kibernetičkoj sigurnosti.

3. Kako pristupiti nadzoru dobavljača kao vrlo bitne komponente direktive NIS2.

4. Koje su mogućnosti financiranja procesa usklađivanja.o

Organizacija panela

S obzirom na definiranu svrhu i ciljeve panela, pristupilo se odabiru panelista. Pri odabiru panelista vodilo se sljedećim načelima:

- U panelu trebaju sudjelovati predstavnici postojećih obveznika, kao i oni za koje se pretpostavlja da će to tek biti.
- Sudjelovati bi morao i predstavnik regulatora.
- Trebalo bi imati predstavnika dobro uređenog sektora, kao što je primjerice bankarski sektor.
- S obzirom na pretpostavku da se može usklađivati sa ISO27001, trebao bi sudjelovati i netko s puno iskustva u usklađivanju s tom normom.

Na temelju toga odabrani su sudionici panela navedeni na početku ovog dokumenta.

Tijek panela

Kako bi panel bilo lakše pratiti, a uzevši u obzir svrhu i ciljeve panela, panel se odvijao u segmentima trajanja 15 ili 20 minuta. Pretpostavka je bila da će lakše biti pratiti panel ako se o pojedinim ciljevima govori ograničeno i relativno kratko vrijeme te ako se nakon svakog segmenta da sažetak ili zaključak.

Panel se sastojao od segmenata opisanih u nastavku.

Uvod – 15min

U uvodnom dijelu predstavili su se svi sudionici panela te je također svaki sudionik panela rekao nešto kratko rekao o organizaciji u kojoj radi, tj. koju predstavlja. Nakon toga uslijedio je prvi set pitanja koja su bila upućena Aleksandru Klaiću iz Centra za kibernetičku sigurnost koji ima značajnu ulogu u transpoziciji direktive NIS2.

Na prvo pitanje, koje su ključne razlike između NIS1 i NIS2, saznali smo da su to:

- NIS2 je sveobuhvatniji te će uključiti daleko veći broj obveznika nego što je to bio slučaj s NIS1, procjena je otprilike tri do četiri puta više.
- Druga razlika je što se mjere kibernetičke sigurnosti moraju provoditi u sveukupnom poslovanju, a ne samo u određenim segmentima usko vezanima uz ključne usluge.
- NIS2 je temelj za buduće akte koje će EU donijeti, kao primjerice Cyber Resilience Act, Cyber Solidarity Act koji su već u procesu donošenja.

Drugo pitanje se odnosilo na hodogram aktivnosti koji će trebati pratiti tijekom usklađivanja. Za usklađivanje ima puno vremena, a pogrešnim se smatra da će obveze nastupiti s trenutkom donošenja novog zakona, dakle preko noći. U tom smislu, rokovi su sljedeći:

Procijenjeno trajanje	Tko	Što
Do početka 2024. godine	Zakonodavac	Donošenje Zakona o kibernetičkoj sigurnosti
2024. godina	Nacionalni centar za kibernetičku sigurnost i druga nadležna tijela u različitim sektorima prema prilogu III. Zakona o kibernetičkoj sigurnosti	Donošenje podzakonskih akata
2025. godina	Obveznici ZKS-a	Provođenje mjera
2026. i 2027. godina	Obveznici ZKS-a	Izrada internih provjera, procjena učinkovitosti
Kraj 2027. godine	Obveznici ZKS-a	Provedba ocjene sukladnosti, tj. nezavisne revizije (ključni subjekti) Samoproocjena (važni subjekti)
2028. i 2029. godina	Nadležna tijela u različitim sektorima prema prilogu III. Zakona o kibernetičkoj sigurnosti	Prvi krug periodičnog stručnog nadzora koji će se provoditi svakih 3 do 5 godina

Zadnje pitanje sudioniku iz Centra za kibernetičku sigurnost je koja je razlika između ocjene sukladnosti i nadzora. Ocjena sukladnosti je revizija zahtjeva ZKS-a, može biti dio neke šire revizije, primjerice, ISO27001 ili druge vrste poslovne revizije. To će obavljati privatne tvrtke (revizori) odobrene za tu uslugu. Nadzor podrazumijeva stručni nadzor nadležnih tijela iz priloga III. Zakona o kibernetičkoj sigurnosti. Tijekom tog procesa će se kontrolirati cjelokupni proces koji provode subjekti obveznici, uključujući i rezultate revizije. Nadzor će se provoditi svakih tri do pet godina.

Nakon toga, uslijedilo je pitanje Mariu Kozini iz HNB-a o iskustvima uspostave regulatornog okvira u području informacijske sigurnosti. HNB je regulirao ovo područje već 2006. godine kada su objavljene smjernice a zatim i 2008. godine kada je objavljena obvezujuća Odluka o primjerenom upravljanju informacijskim sustavom. U tih, više od 17 godina, provedeni su brojni nadzori te su stečena iskustva koja mogu pomoći i kod NIS2 direktive, a koja također mogu pokazati kako će se stvari odvijati u narednom periodu.

Od njega smo čuli kako usklađivanje bankarskog sektora nije bilo bezbolno i trajalo je. HNB je imao inkrementalni pristup, očekivalo se da banke primjene postepeno nova pravila u roku od dvije

godine (do 2010.). U prvoj fazi fokus je bio na uspostavi upravljanja (governance), uspostavi procesa upravljanja rizicima te definiranju politika informacijske sigurnosti. U drugoj fazi se očekivala uspostava tehničkih rješenja. Zadnja faza je bila uspostava kontinuiteta poslovanja i pričuvnog podatkovnog centra. Nakon toga su krenuli nadzori. Sve se stabiliziralo oko 2012. ili 2013. godine. U konačnici, dolaskom prvog ZKS-a, banke su bile spremne. U zaključku, treba planirati na vrijeme i postepeno ići u provedbu.

Zaključak ovog segmenta je da vremena ima, ali da svakako s pripremom treba krenuti što prije.

Organizacijski i upravljački zahtjevi za provođenje usklađivanja – 20min

Nakon uvodnog dijela uslijedio je segment koji se bavi organizacijskim i upravljačkim zahtjevima za provođenje usklađivanja po NIS2. Naime, iz informacijske sigurnosti poznato je kako se bez odgovarajuće upravljačke strukture ne može se podići informacijska sigurnost organizacije.

U tom smislu, prvo je postavljeno pitanje Dariu Rajnu iz Podravke. Naime, u Podravci – koja će tek biti obveznik novog ZKS-a – uspostavili su upravljanje sigurnošću, odnosno implementirali su ISO27001, te je bilo zanimljivo čuti kako su krenuli u to, što su naučili i kako su uspjeli pridobiti Upravu. Po njihovom iskustvu, vrlo je bitno imati podršku uprave budući da su imali dva neuspješna pokušaja uvođenja upravljanja sigurnošću koja su krenula iz nižih organizacijskih jedinica – bez eksplicitne podrške uprave. Konačni pokušaj kada su uspjeli je krenuo tako da su iskoristili GDPR 2018. godine i pripadajuće kazne kako bi uvjerili Upravu da se u informacijsku sigurnost mora uložiti te su odjel informacijske sigurnosti izdvojili iz IT-ja u posebnu organizacijsku jedinicu. Odlučili su se na ISO27001, a imali su već iskustva s ISO9001, to im je olakšalo stvar i uspjeli su implementirati ISO27001.

Drugo pitanje išlo je Ivanu Kaliniću, kao osobi s puno iskustva u implementaciji ISO27001 norme, od koga smo željeli saznati kako bi trebalo izgledati upravljanje sigurnošću u organizaciji te kako doći do tog stanja? Prema njegovom iskustvu, sve kreće od svijesti Uprave, bez obzira na motiv – regulatorni, izloženost riziku, ili bilo što drugo. Oni kao konzultanti potom savjetuju da se cjelokupni sustav upravljanja sigurnošću postavi na način da se osnaže poslovni vlasnici, direktori organizacijskih jedinica, koji bi trebali biti svjesni da su oni odgovorni za svoje procese i imovinu te da su oni prva linija obrane od bilo kakvih napada. Kao drugu liniju obrane preporučaju stručne osobe u obliku voditelja informacijske sigurnosti koja ima savjetodavnu ulogu te će biti na dispoziciji svima. Dodatno, ta uloga ima i nadzornu ulogu da periodički provjeri je li sve u redu i opet savjetodavno djeluje. Na taj način se postiže da sigurnost nije izolirani otok već da se sigurnost ugradi u sve poslovne procese. Kada organizacija sazrije i ako je dovoljno velika tada preporučuju i treću liniju obrane u obliku revizije, odnosno u novom ZKS-u će to biti ocjena sukladnosti ili redovan nadzor koji dodatno pružaju uvjerenje da se stvari rade ispravno. Bez obzira na linije obrane, kreće se s drugom linijom obrane, tj. voditeljem sigurnosti iz razloga osvještavanja svih.

S obzirom da se stalno spominje preustroj kako bi se uvelo upravljanje sigurnošću, to znači i potrebu za odgovarajućim kadrom. S obzirom na poznate probleme s kadrovima, dodatno je bilo zanimljivo čuti od Daria Rajna, kako su riješili taj problem u Podravci. U njihovom slučaju problem ljudi je prisutan na svim razinama i svim radnim mjestima, a posebno je to istaknuto u

informacijskoj sigurnosti. Dio ljudi su angažirali iz IT-ja, a dio zapošljavaju pri čemu imaju poteškoća naći educirane ljude.

Konačno, u ovom segmentu je bilo pitanje HEP ODS d.o.o. kako upravljaju sigurnošću s obzirom da su oni već obveznici postojećeg ZKS-a i morali su se pozabaviti s tim. Ana Balaško je izložila kako su se stvari odvijale u HEP ODS po donošenju postojećeg ZKS-a. U tom trenutku nisu imali posebnu organizacijsku jedinicu za informacijsku sigurnost, nisu imali nova zapošljavanja. Problem im je prvenstveno bio ljudski, jer su došle nove obaveze koje je netko trebao preuzeti. Zahvaljujući svojoj postojećoj poslovnoj organizaciji imali su olakšanu implementaciju postojećeg ZKS-a. Dodatno su imali veliku pomoć od HEP d.d. u kojemu je pozicionirana odjel korporativne sigurnosti certificiran po ISO27001. I po njima je bitno da se uspostavi organizacijska struktura te da se definiraju odgovornosti.

U zaključku, svi sudionici su isticali važnost organizacijskog aspekta i nužnost da se prvo to odredi pri čemu je vrlo značajno dobiti podršku uprava. Kako bi se dobila podrška uprave, sudionici su istaknuli sljedeće mogućnosti:

Obveza usklađivanja s regulativom

- Mogućnost sankcija, posebno ako su kazne točno određene i jasno je tko će ih dobiti
- I možda najbitnije, kvantificiranje rizika u Eurima što uprave vrlo dobro razumiju
- Pozivanje na istraživanja koje pokazuju što druge uprave brine (djelovanje na ego)

Usklađivanje s ISO27001 i ISA62443 kao model za usklađivanje sa novim ZKS-om – 20min

Ovaj segment bavio se idejom da je moguće započeti usklađivanje sa novim ZKS-om i prije nego što su on i odgovarajući podzakonski akti doneseni i to na način da se usklađuje sa relevantnim normama ISO27001 i ISA62443.

U tom smislu, prvo pitanje je išlo Aleksandru Klaiću, od koga se tražilo da rastumači odnos tih normi i novog ZKS-a. Saznali smo tako da je direktiva NIS2 relativno neutralna što se tiče normi s kojima se mogu rješavati zahtjevi direktive. Razlog za to je jednostavan, heterogenost sustava je takva da nije moguće pronaći jednu normu s kojom bi se postigao pristup postizanja kibernetičke sigurnosti koji bi odgovarao svima. Ipak, treba obratiti pozornost da je ISO27001 vrlo prisutan u RH, ali na različite načine – kao najbolja praksa, kao vlastita revizija, vanjska certifikacija. Pri tome ISO27001, sve do zadnje inačice, nije postavljao zahtjev između opsega i konteksta certifikacije. U tom smislu je tek zadnja verzija potpuno uskladiva s pristupom koji ima direktiva NIS2.

Nakon toga Dario Rajn je pojasnio proces usklađivanja sa ISO27001 u Podravci koji je uslijedio nakon uspostavljanja upravljačke strukture u organizaciji. Sama implementacija je trajala oko godinu i po uz pomoć vanjskog partnera – što on smatra optimalnim trajanjem za organizaciju veličine Podravke. Pri tome je bitno istaknuti da je uključenost ljudi unutar kompanije bila na visokoj razini što je omogućilo da uvođenje bude suštinsko te je trajalo toliko. Formalno uvođenje, s druge strane, bi bilo puno kraće, par mjeseci. Samo usklađivanje sa ISO27001 normom može se podijeliti u tri segmenta:

1. Dokumentacija.
2. Edukacija (podizanje svijesti) u cijeloj organizaciji.
3. Tehnička (podizanje SOC-a i druge tehničke mjere).

S obzirom na iskustvo s usklađivanjem prema ISO27001 normi, od Ivana Kalinića se tražio komentar koliko su ta usklađivanja trajala, koji izazovi su se javljali, koja su iskustva stekli? On je počeo svoj komentar tako što je konstatirao da su u Podravci cijeli proces napravili po svim pravilima. Po njemu, ako nije uloženo vrijeme i sredstva u edukaciju kao i ugrađivanje tih mjera u procese i svakodnevne postupke ljudi, dolazi do problema i upravljanje sigurnošću se ne provodi suštinski. Najkraća implementacija koju je on vidio, bila je šest mjeseci za malu tvrtku od 15-tak ljudi. Takvo trajanje je posljedica činjenice da se ljudi moraju educirati i uključivati u cijeli proces.

Dodatno pitanje je bilo što tvrtke mogu očekivati od konzultanata, i što oni kao konzultanti očekuju od klijenata? Prema njemu, prva stvar koju očekuju je zainteresiranost klijenta, te potporu nalogodavca da mogu isporučiti sve što im je zadaća.

Nakon toga prešlo se na pitanje OT sustava i norme ISA62443, s obzirom da će velik broj obveznika novog ZKS-a imati OT sustave koji nisu dobro pokriveni s normom ISO27001. U tom smislu, pitanje je bilo upućeno Marku Grbiću iz LNG Hrvatska d.o.o. da kaže koja je specifičnost norme ISA62443 te kako su oni pristupili usklađivanju s tom normom. Prema njemu, ISA62443 je specifično za OT sustave te su oni radili procjenu rizika po toj normi. Njihovo iskustvo je da je to proces koji traje, sveobuhvatan je te kreće s pregledom dokumentacije. Za provedbu tog procesa trebalo im je pola godine i oni su to napravili za interne potrebe jer još ne postoji mogućnost certificiranja prema toj normi u RH.

Zaključak je da se može odabrati ISO27001, ISA62443 ili neku drugu sličnu normu kao smjer usklađivanja sa novim ZKS-om, uz napomenu da se katalog prijetnji i ugroza mora čitati iz novog ZKS-a.

Nadzor dobavljača – 20min

S obzirom da jedna od ključnih novosti direktive NIS2 je sigurnost dobavljačkog lanca, pitanje je kako pristupiti tom problemu te se ovaj segment bavio tim pitanjem. Zanimljivo je pri tome kako neki sektori već imaju obvezu nadzora svojih dobavljača, konkretno u prehrambenoj industriji i može li se što od tih metoda preslikati na kibernetičku sigurnost. Pitanje Dariu Rajnu bilo je kako oni kontroliraju svoje dobavljače?

Oni s kontrolom kvalitete hrane kod dobavljača imaju višegodišnje iskustvo, a namjeravaju ta iskustva preslikati i na IT dio. Oni svoje dobavljače kategoriziraju po vrsti robe koje od njih dobavljaju, sirovine, ambalaže, usluge, „outsourcing“ partneri koji rade nešto pod njihovim brendom. Godišnje, oni rade procjenu rizika dobavljača na temelju šest kriterija, primjerice, veličina, broj reklamacija, itd. Na temelju tih kriterija iz svake grupe dobavljača izvuku pet do deset partnera te rade revizije kod tih partnera na temelju internih standarada. Interni standardi su načinjeni na temelju međunarodnih retail standarada. Pri tome nastoje u svakih tri do pet godina pokriti sve ključne partnere. Na temelju revizije ocjenjuju, tj. boduju partnere, a to potom daju Odjelu nabave kao preporuku treba li s tim partnerom radili ili ne, treba li tražiti od partnera da nešto promijene, i slično.

Preslikavanje navedenog mehanizma planiraju napraviti za informacijsku sigurnost, ali im je jasno da će postojati određeni izazovi koje će trebati riješiti. Primjerice, pregledavanje kompletnog informacijskog sustava partnera nije moguće zbog kompleksnosti informacijskih sustava općenito. Iduće pitanje je bilo Aleksandru Klaiću, a odnosilo se na moguće smjernice u vezi sigurnosti dobavljača u Uredbi temeljenoj na novom ZKS-u. Ono što smo saznali je da će Uredba svakako morati razraditi sve mjere definirane novim ZKS-om pa tako i sigurnost dobavljača. Za sada je plan da se sve provodi temeljem SLA ugovora, iako su svjesni da je tu prisutan priličan broj izazova u praksi. Ideja je da će biti definiran skup kriterija temeljem kojih će svaki subjekt moći kontrolirati dobavljače i na temelju njih znati da li su pojedini dobavljači odgovarajuće razine sigurnosti.

Tu se otvorilo i pitanje javnih nabava, tj. kako se zahtjevi javnih nabava potiču ili sukobljavaju sa zahtjevima za informacijskom sigurnošću. Istaknuto je da postoje određeni izazovi, u smislu da javni natječaji ne smiju favorizirati nikoga te iz tog razloga se može desiti da dođe do iznenadne promjene dobavljača što onda povlači i niz operativnih posljedica. Iz HEP ODS-a su istaknuli kako oni nemaju problema s javnom nabavom pod uvjetom da se iskoriste mehanizmi koje javna nabava omogućava. Prvenstveno se tu radi o kriteriju ekonomski najpovoljnije ponude koja omogućava vrednovanje i drugih parametara osim same cijene.

Ana Balaško je istaknula kako novi ZKS govori o certificiranju dobavljača što u HEP ODS-u namjeravaju koristiti tijekom javne nabave i zahtijevati određene certifikate kako bi osigurali sigurnost dobavljača – što je isto jedan mogući pristup indirektnog nadzora dobavljača. Dodatno je pitanje kako će to utjecati na dobavljače, ali to je u ovom trenutku nepoznato.

U LNG Hrvatska rade na konkretnom problemu kontrole pristupa dobavljača sustavima uvođenjem primjerenog tehničkog sustava kibernetičke zaštite putem kojega se dobavljači spajaju na sustav za potrebe pružanja usluga. To je otvorilo dodatno pitanje kontrole na tehničkoj razini s kojom se nismo bavili, ali je svakako bitno za ukupni proces nadzora.

Zaključak je da će izazov nadzora dobavljača vjerojatno biti riješen s više istovremenih pristupa. Prvo je tu svakako proces certifikacije o kojemu nije bilo dublje rasprave, ali se radi o značajnoj komponenti. Potom će trebati nekako definirati ugovorne odnose, a svakako će trebati definirati kriterije za ispunjavanje ugovornih odnosa. Konačno, trebat će primijeniti i odgovarajuća tehnička rješenja kako bi se provodile proaktivne mjere kontrole dobavljača. Svakako će biti zanimljivo koristiti iskustva iz drugih područja, u ovom slučaju bankarskog sektora te prehrambene industrije.

Razno – 15min

Ova točka se dominantno bavi pitanjem kako financirati sve aktivnosti usklađivanja sa ZKS-om i sigurnosnim normama. Pri tome se htjelo istaknuti mogućnost korištenja EU fondova u tu svrhu. Od Ane Balaško je zatražen komentar o CEF/DEP fondovima, kao jednoj mogućnosti financiranja koji je korišten i u RH. HEP ODS nije direktno koristio te fondove, ali su tijekom provođenja drugih projekata uključivali kibernetičku sigurnost kao jedan značajan element projekta s čime su postizali financiranje podizanja kibernetičke sigurnosti organizacije. EU je prepoznala značaj kibernetičke sigurnosti te je uvela program DEP koji pokriva i kibernetičku sigurnost. Također, stupanjem na snagu ZKS-a vrlo vjerojatno će se otvoriti razne mogućnosti financiranja kibernetičke sigurnosti.

Također je istaknuto kako je najbolje za prijave na EU natječaje razgovarati s konzultantima specijaliziranima za to koji mogu puno pomoći i olakšati stvari. Dodatno, prva prijava može biti vrlo izazovna, ali stečeno iskustvo kao i materijali onda mogu značajno olakšati iduće prijave.

Tu je istaknuto i Nacionalno koordinacijsko središte za industriju, tehnologiju i istraživanje u kibernetičkoj sigurnosti. Od Aleksandra Klaića je zatražen komentar o tom središtu i cijeloj infrastrukturi. To središte će, prema njemu, pokrivati širok raspon aktivnosti namijenjenih korištenju EU sredstava u području kibernetičke sigurnosti. U Republici Hrvatskoj bi to središte trebalo biti u CARNET-u. Aleksandar Klaić je istaknuo i neke druge modele financiranja, kao što su primjerice digitalni vaučeri za digitalizaciju Ministarstva zaštite okoliša i gospodarstva.

Dodatno su istaknute i druge mogućnosti kroz istraživačke, Horizon i EDF pozive i projekte..

Zaključne riječi – 15min

U zaključnoj riječi svaki od sudionika panela kratko je sažeo svoja iznesena stajališta tijekom panela, ali i dao i neka dodatna viđenja.