C/2024/1049

9.2.2024.

Mišljenje Europskog odbora regija – Akt EU-a o kibersolidarnosti i digitalna otpornost

(C/2024/1049)

Izvjestitelj: Pehr GRANFALK (SE/EPP), član Općinskog vijeća Općine Solna

Referentni dokument: Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih

COM(2023) 209 final

I. PREPORUKE ZA IZMJENE

COM(2023) 209

Amandman 1.

Uvodna izjava 1.

Prijedlog Komisije	Amandman OR-a
Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora gospodarstva jer su javne uprave, poduzeća i građani međusobno povezani i ovisni jedni o drugima u svim sektorima i prekogranično više nego ikada prije.	Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora gospodarstva***, ali su ujedno iznijeli na vidjelo i slabosti,*** jer su javne uprave, poduzeća i građani međusobno povezani i ovisni jedni o drugima u svim sektorima i prekogranično više nego ikada prije.

Obrazloženje

Razumljivo samo po sebi.

Amandman 2.

Uvodna izjava 3.

Prijedlog Komisije	Amandman OR-a
Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe, potrebno je povećati otpornost građana, poduzeća i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. […]	Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe, potrebno je povećati otpornost građana, poduzeća***, javne uprave na nacionalnoj, regionalnoj i lokalnoj razini*** i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. […]

Obrazloženje

Lokalna i regionalna uprava pružaju usluge bliske građanima koje su ključne za društvo te su jedan od najvažnijih elemenata dinamičnog europskog tržišta.

Amandman 3.

Uvodna izjava 29.

Prijedlog Komisije	Amandman OR-a
U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti"). Koordinirane vježbe testiranja […]	U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi***, kao i tijela javne uprave na regionalnoj i lokalnoj razini, neovisno o tome smatraju li se visokokritičnima prema nacionalnom pravu,*** odabrati iz Priloga I. Direktivi (EU) 2022/2555 („sektori visoke kritičnosti"). Koordinirane vježbe testiranja […]

Obrazloženje

Budući da države članice imaju mogućnost isključiti lokalne i regionalne vlasti iz provedbe Direktive NIS 2 ([1]), trebalo bi osigurati da one budu obuhvaćene Aktom o kibersolidarnosti.

Amandman 4.

Uvodna izjava 30.

Prijedlog Komisije	Amandman OR-a
Osim toga, mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružati potpora drugim mjerama pripravnosti i podupirati pripravnost u drugim sektorima koji nisu obuhvaćeni koordiniranim testiranjem subjekata koji djeluju u ***visokokritičnim*** sektorima. Te bi mjere mogle uključivati različite vrste aktivnosti za nacionalnu pripravnost.	Osim toga, mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružati potpora drugim mjerama pripravnosti i podupirati pripravnost u drugim sektorima koji nisu obuhvaćeni koordiniranim testiranjem subjekata koji djeluju u ***kritičnim*** sektorima. ***Isto bi se trebalo primjenjivati na javnu upravu, bez obzira na to smatra li se ona kritičnom prema nacionalnom pravu.*** Te bi mjere mogle uključivati različite vrste aktivnosti za nacionalnu pripravnost.

([1]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

Obrazloženje

Lokalnim i regionalnim vlastima trebalo bi omogućiti da iskoriste potporu u okviru mehanizma za izvanredne kibersigurnosne situacije.

Amandman 5.

Uvodna izjava 33.

Prijedlog Komisije	Amandman OR-a
Na razini Unije trebalo bi postupno uspostaviti kibersigurnosnu pričuvu koja bi se sastojala od usluga privatnih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i hitne mjere oporavka u slučajevima značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera. Kibersigurnosna pričuva EU-a trebala bi osigurati dostupnost i spremnost usluga. Usluge iz kibersigurnosne pričuve EU-a trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima ***koji djeluju u kritičnim ili visokokritičnim sektorima*** te nadopunjavati njihovo djelovanje na nacionalnoj razini. Pri podnošenju zahtjeva za potporu iz kibersigurnosne pričuve EU-a države članice trebale bi navesti vrstu potpore pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni zahtjeva države članice. Usluge iz kibersigurnosne pričuve EU-a mogu služiti i za potporu institucijama, tijelima i agencijama Unije pod sličnim uvjetima.	Na razini Unije trebalo bi postupno uspostaviti kibersigurnosnu pričuvu koja bi se sastojala od usluga privatnih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i hitne mjere oporavka u slučajevima značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera. Kibersigurnosna pričuva EU-a trebala bi osigurati dostupnost i spremnost usluga. Usluge iz kibersigurnosne pričuve EU-a trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima te nadopunjavati njihovo djelovanje na nacionalnoj razini. Pri podnošenju zahtjeva za potporu iz kibersigurnosne pričuve EU-a države članice trebale bi navesti vrstu potpore pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni zahtjeva države članice. Usluge iz kibersigurnosne pričuve EU-a mogu služiti i za potporu institucijama, tijelima i agencijama Unije pod sličnim uvjetima.

Obrazloženje

Potpora iz kibersigurnosne pričuve EU-a ne ni smjela stajati na raspolaganju samo subjektima iz kritičnog ili visokokritičnog sektora.

Amandman 6.

Članak 1. stavak 2. točka (b)

Prijedlog Komisije	Amandman OR-a
podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa („DEP”);	podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji***, kao i javne uprave na nacionalnoj i podnacionalnoj razini*** i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa („DEP”);

Obrazloženje

Podnacionalna tijela također bi trebala biti obuhvaćena područjem primjene predmetne uredbe.

Amandman 7.

Članak 4. stavak 1., drugi podstavak

Prijedlog Komisije	Amandman OR-a
Mora moći služiti drugim javnim i privatnim organizacijama na nacionalnoj razini kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. […]	Mora moći služiti drugim javnim i privatnim organizacijama na nacionalnoj ***i podnacionalnoj*** razini kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. […]

Obrazloženje

Nacionalni centri za sigurnosne operacije (SOC-ovi) trebali bi prikupljati i analizirati informacije i regionalnih i lokalnih tijela.

Amandman 8.

Članak 5. stavak 2.

Prijedlog Komisije	Amandman OR-a
Nakon poziva na iskaz interesa ECCC odabire konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski doprinos Unije pokriva do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva konzorcij domaćin. Prije pokretanja postupka nabave alata i infrastrukture ECCC i konzorcij domaćin sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.	Nakon poziva na iskaz interesa ECCC odabire konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski doprinos Unije pokriva do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva konzorcij domaćin ***sredstvima koja nisu obuhvaćena Uredbom (EU) 2021/1060 (Uredba o zajedničkim odredbama)***. Prije pokretanja postupka nabave alata i infrastrukture ECCC i konzorcij domaćin sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.

Obrazloženje

Mjere u okviru Akta o kibersolidarnosti ne bi se trebale financirati iz programa kohezijske politike.

Amandman 9.

Članak 9. stavak 1.

Prijedlog Komisije	Amandman OR-a
Uspostavlja se mehanizam za izvanredne kibersigurnosne situacije radi povećanja otpornosti Unije na ***velike*** kibersigurnosne prijetnje te radi pripreme za kratkoročne posljedice značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera i njegovo ublažavanje u duhu solidarnosti („mehanizam”).	Uspostavlja se mehanizam za izvanredne kibersigurnosne situacije radi povećanja otpornosti Unije na kibersigurnosne prijetnje te radi pripreme za kratkoročne posljedice značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera i njegovo ublažavanje u duhu solidarnosti („mehanizam”).

Obrazloženje

Mehanizam za izvanredne kibersigurnosne situacije trebao bi služiti kao priprema za kratkoročne učinke svih vrsta kibersigurnosnih incidenata i ublažiti ih.

Amandman 10.

Članak 10. stavak 2. (novi)

Prijedlog Komisije	Amandman OR-a
	2. Komisija sastavlja godišnje izvješće u kojem ocjenjuje funkcioniranje mehanizma i moguću potrebu za dodatnim zahtjevima u pogledu suradnje i osposobljavanja.

Obrazloženje

Komisija bi trebala podnositi redovita izvješća jer se područje kibersigurnosti stalno razvija, a zahtjeve je potrebno pravodobno prilagođavati aktualnom stanju.

Amandman 11.

Članak 11. stavak 1.

Prijedlog Komisije	Amandman OR-a
Za potrebe podupiranja koordiniranog testiranja pripravnosti subjekata iz članka 10. stavka 1. točke (a) u cijeloj Uniji Komisija, nakon savjetovanja sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava i ENISA-om, među sektorima visokog stupnja kritičnosti navedenima u Prilogu I. Direktivi (EU) 2022/2555 utvrđuje relevantne sektore ili podsektore iz kojih se subjekti mogu podvrgavati koordiniranom testiranju pripravnosti, uzimajući u obzir postojeće i planirane koordinirane procjene rizika i testiranja otpornosti na razini Unije.	Za potrebe podupiranja koordiniranog testiranja pripravnosti subjekata iz članka 10. stavka 1. točke (a) u cijeloj Uniji Komisija, nakon savjetovanja sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava i ENISA-om, među sektorima visokog stupnja kritičnosti navedenima u Prilogu I. Direktivi (EU) 2022/2555***, uključujući javnu upravu na lokalnoj razini,*** utvrđuje relevantne sektore ili podsektore iz kojih se subjekti mogu podvrgavati koordiniranom testiranju pripravnosti, uzimajući u obzir postojeće i planirane koordinirane procjene rizika i testiranja otpornosti na razini Unije.

Obrazloženje

Lokalnim i regionalnim vlastima trebalo bi omogućiti da koriste mehanizam za izvanredne kibersigurnosne situacije. Amandmanom se u Prijedlog uredbe unosi zahtjev izvjestitelja iz amandmana 3. (u vezi s uvodnom izjavom 30.).

Amandman 12.

Članak 14. stavak 2. točka (b)

Prijedlog Komisije	Amandman OR-a
vrsta pogođenog subjekta, pri čemu se veća prednost daje incidentima koji utječu na ključne subjekte kako su definirani u članku 3. stavku 1. Direktive (EU) 2022/2555;	vrsta pogođenog subjekta, ***uključujući javne uprave na regionalnoj i lokalnoj razini,*** pri čemu se veća prednost daje incidentima koji utječu na ključne subjekte kako su definirani u članku 3. stavku 1. Direktive (EU) 2022/2555;

Obrazloženje

Pojašnjava se da područje primjene uključuje podnacionalna tijela.

Amandman 13.

Članak 18. stavak 1.

Prijedlog Komisije	Amandman OR-a
Na zahtjev Komisije, mreže EU-CyCLONe ili mreže CSIRT-ova ENISA istražuje i procjenjuje prijetnje, ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibersigurnosni incident ili kibersigurnosni incident velikih razmjera. Nakon završetka istraživanja i procjenjivanja incidenta ENISA mreži CSIRT-ova, mreži EU-CyCLONe i Komisiji dostavlja izvješće o istraživanju incidenta kako bi im pomogla u obavljanju njihovih zadaća, osobito u pogledu onih utvrđenih u člancima 15. i 16. Direktive (EU) 2022/2555. Komisija prema potrebi izvješće šalje Visokom predstavniku.	Na zahtjev Komisije, mreže EU-CyCLONe ili mreže CSIRT-ova ENISA istražuje i procjenjuje prijetnje, ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibersigurnosni incident ili kibersigurnosni incident velikih razmjera. Nakon završetka istraživanja i procjenjivanja incidenta ENISA mreži CSIRT-ova, mreži EU-CyCLONe i Komisiji dostavlja izvješće o istraživanju incidenta kako bi im pomogla u obavljanju njihovih zadaća, osobito u pogledu onih utvrđenih u člancima 15. i 16. Direktive (EU) 2022/2555. ***Ako je to moguće, mreža CSIRT-ova izvješće dostavlja i javnim upravama na podnacionalnoj razini.*** Komisija prema potrebi izvješće šalje Visokom predstavniku.

Obrazloženje

Pojašnjava se da područje primjene uključuje podnacionalna tijela.

II. **PREPORUKE O POLITIKAMA**

STAJALIŠTE EUROPSKOG ODBORA REGIJA

Europski odbor regija (OR) pozdravlja Prijedlog uredbe Europske komisije o jačanju europske suradnje u području kibersigurnosti. Države članice EU-a danas su usko povezane i umrežene, a u budućnosti će to biti još više. Odbor stoga pozdravlja inicijativu Komisije za zajedničko rješavanje kiberprijetnji koje proizlaze iz povećane digitalizacije. Prijedlog ukazuje na sve veći broj kiberincidenata, osobito u područjima odgovornosti gradova i regija, i naglašava da se treba pripremiti na sigurnosne incidente u kritičnim područjima društva, odgovoriti na njih i iz njih učiti. OR smatra da prijedlozi Komisije mogu doprinijeti povećanju digitalne otpornosti u Uniji.

1. Da bi se postigao cilj digitalno otporne Europe, političari i građani moraju postati svjesni potrebe za udruživanjem snaga u području kibersigurnosti. OR stoga poziva države članice, Komisiju i sve lokalne vlasti da zajedno podignu razinu osviještenosti o potrebi za djelovanjem, uključujući potrebu za povećanjem ulaganja u digitalnu otpornost, posebno na lokalnoj i regionalnoj razini, te da razmotre mogućnost razvoja zaštitnih instrumenata politike usmjerenih na napade financijskim ucjenjivačkim softverom. Za to su potrebne odgovarajuće financijske i tehničke mjere odnosno mjere povećanja kompetencija.

2. Odbor napominje da se Prijedlog u mnogim aspektima odnosi na Direktivu NIS 2 i da se na njoj temelji. Pri prenošenju Direktive NIS 2 u nacionalno pravo svaka država članica određuje trebaju li lokalna tijela biti obuhvaćena područjem primjene Direktive NIS 2 ([2]). Budući da svaka država članica može odlučiti hoće li općine biti ključni ili važni subjekti u provedbi Direktive NIS 2, eventualne razlike među zemljama odrazit će se u načinu na koji zemlje pristupaju Aktu o kibersolidarnosti kako je trenutačno predložen. Kako lokalne vlasti nadležne za osnovne usluge u nekim državama članicama ne bi bile isključene iz područja primjene Akta o kibersolidarnosti, u normativnom dijelu Prijedloga uredbe trebalo bi pojasniti da se ta tijela smatraju obuhvaćenima, neovisno o tome jesu li uključena u Direktivu NIS 2 ili ne.

3. S obzirom na to da je kibersigurnost jedan od temelja digitalne interoperabilnosti, nužno je da se napori za poboljšanje interoperabilnosti diljem regija podupru snažnim kibersigurnosnim mjerama kako kiberprijetnje ne bi ometale interoperabilnost regija diljem Europe.

4. Gradovi i regije moraju od struktura koje će se osnovati dobiti konkretnu potporu, a ne da im se samo nameće obveza izvješćivanja. Odbor stoga poziva na pojašnjenje načina na koje će se regijama pružati potpora, posebno kako bi se povećala razina kibersigurnosti u malim zajednicama.

Stajališta o područjima djelovanja iz Prijedloga

Europski kiberštit

Uspostava paneuropske infrastrukture centara za sigurnosne operacije kako bi se razvili i poboljšali zajednički kapaciteti za otkrivanje, analizu i obradu podataka o kiberprijetnjama i kiberincidentima.

5. Da bi se dobila sveobuhvatna slika trenutačnog stanja kibersigurnosti u EU-u, potrebno je objediniti informacije, procjene rizika, prijetnje i incidente, među ostalim od lokalnih i nacionalnih pružatelja sustava. OR smatra problematičnim činjenicu da ne postoje jasni poticaji i postupci koji se odnose na načine na koje gradovi i regije mogu aktivno doprinijeti jačanju digitalne otpornosti. Uključenost lokalne i regionalne razine iznimno je važna jer upravo ta razina posjeduje digitalna rješenja koja su izložena napadima. Stoga je potrebno stvoriti okruženje u koje gradovi i regije mogu i moraju biti uključeni kao partneri u okviru napora za povećanje kibersigurnosti u Uniji.

6. Odbor je utvrdio da među zemljama postoje velike razlike u stupnju razvijenosti u pogledu poduzetih mjera zaštite i sigurnosti. Znatne razlike postoje čak i unutar zemalja, primjerice, između nacionalnih tijela i manjih lokalnih tijela, kao i u pogledu kapaciteta i ciljeva u području kibersigurnosti. Odbor stoga smatra da bi predmetna uredba trebala doprinijeti smanjenju tih razlika i osigurati da svi dionici imaju relativno jednake mogućnosti i ciljeve.

7. Odbor skreće pozornost na rizik da će se zadaće nove mreže nacionalnih i prekograničnih centara za sigurnosne operacije preklapati sa zadaćama mreže timova za odgovor na računalne sigurnosne incidente (CSIRT) ([3]). Ako se osim timova za odgovor na računalne sigurnosne incidente uspostave i centri za nacionalnu sigurnost, potrebno je jasno definirati funkcioniranje suradnje i odgovornosti nacionalnog centra za sigurnosne operacije i CSIRT-ova u slučaju incidenta.

([2]) Članak 2. stavak 5. Direktive NIS 2.: „Države članice mogu predvidjeti da se ova Direktiva primjenjuje na: (a) subjekte javne uprave na lokalnoj razini.

([3]) U skladu s člankom 11. stavkom 3. Direktive NIS 2, CSIRT-ovi obavljaju sljedeće zadaće:
(a) praćenje i analiziranje kiberprijetnji, ranjivosti i incidenata na nacionalnoj razini i, na zahtjev, pružanje pomoći predmetnim ključnim i važnim subjektima u vezi s praćenjem njihovih mrežnih i informacijskih sustava u stvarnom ili gotovo stvarnom vremenu;
(b) pružanje ranih upozorenja i najava te informiranje predmetnih ključnih i važnih subjekata, kao i nadležnih tijela i drugih relevantnih dionika o kiberprijetnjama, ranjivostima i incidentima, ako je moguće u gotovo stvarnom vremenu;
(c) odgovaranje na incidente i, ako je to primjenjivo, pružanje pomoći predmetnim ključnim i važnim subjektima;
(d) prikupljanje i analiziranje forenzičkih podataka te osiguravanje dinamičke analize rizika i incidenata te informiranosti o stanju u pogledu kibersigurnosti;
(e) osiguravanje, na zahtjev predmetnog ključnog ili važnog subjekta, proaktivnog skeniranja mrežnih i informacijskih sustava predmetnog subjekta radi otkrivanja ranjivosti s potencijalno znatnim učinkom;
(f) sudjelovanje u mreži CSIRT-ova i pružanje uzajamne pomoći u skladu sa svojim kapacitetima i kompetencijama drugim članovima mreže CSIRT-ova na njihov zahtjev;
(g) ako je to primjenjivo, djelovanje u svojstvu koordinatora za potrebe postupka koordiniranog otkrivanja ranjivosti iz članka 12. stavka 1.;
(h) doprinošenje korištenju alata za sigurnu razmjenu informacija na temelju članka 10. stavka 3.

8. Odbor pozdravlja posebne ciljeve iz Prijedloga uredbe i predložene mjere, no istodobno izražava žaljenje zbog toga što, unatoč sve većem broju kibernapada, lokalne i regionalne vlasti nisu u dovoljnoj mjeri obuhvaćene Prijedlogom te stoga predlaže niz zakonodavnih izmjena za uklanjanje tih nedostataka;

9. Trenutačno nema dovoljno podataka i jasnih referentnih vrijednosti o incidentima, prijetnjama i rizicima za općine i regije. U okviru europskog kiberštita trebalo bi razviti pokazatelje za procjenu razvoja i zrelosti provedbe predmetne uredbe. Pokazatelji se dugoročno mogu uključiti u kartu rizika koja se temelji na podacima i pokazuje područja u kojima je potrebno najviše djelovanja.

Mehanizam za izvanredne kibersigurnosne situacije

Cilj je ojačati pripravnost, testirati pripravnost u kritičnim sektorima, ojačati kapacitete za oporavak nakon incidenata i uspostaviti kibersigurnosnu pričuvu.

10. Kiberincidenti velikih razmjera mogu biti posljedica lokalnih događanja, pa u Prijedlogu treba pokazati na koji način centri za sigurnosne operacije i kibersigurnosna pričuva mogu obuhvatiti ozbiljne lokalne poremećaje, a ne samo ozbiljne incidente i incidente velikih razmjera koji su se već dogodili. Razmjena informacija ne bi smjela biti ograničena na incidente velikih razmjera, već bi trebala uključivati i potencijalne rizike.

11. Informacije povezane s kiberincidentima često su vrlo osjetljive i mogu sadržavati tehničke pojedinosti ili osobne podatke koji se zasad ne mogu dijeliti bez ugovora i sporazuma među partnerima. Trenutačno postoje poteškoće u razmjeni informacija na nacionalnoj razini. Pitanje prekogranične razmjene stoga je vrlo složeno. Kako bi mehanizam za izvanredne kibersigurnosne situacije funkcionirao, Komisija mora osigurati da svi dionici – javni i privatni u okviru kibersigurnosne pričuve EU-a – imaju pravne i tehničke uvjete za razmjenu i primanje informacija. Odbor smatra da je glavni cilj razmjene informacija rješavanje incidenata, odnosno način na koji se napadnuti subjekti mogu najbolje nositi s ozbiljnim incidentom.

12. OR pozdravlja visoku razinu zahtjeva koje moraju ispunjavati pružatelji usluga iz privatnog sektora uključeni u predloženu kibersigurnosnu pričuvu. Međutim, ti zahtjevi ne bi smjeli biti formulirani tako da dovedu do isključivanja određenih vještina ili znanja o sustavu zato jer samo nekoliko vrlo velikih aktera može ispuniti zahtjeve koje moraju ispunjavati pružatelji sigurnosnih usluga. EU treba pokriti širok raspon sigurnosnih aktivnosti kako bi bio što otporniji.

13. Prijedlogom se predviđa da će se kibersigurnosna pričuva sastojati od usluga koje pružaju pouzdani pružatelji usluga, koji će biti certificirani u skladu s Aktom o kibersigurnosti ([4]). Agencija Europske unije za kibersigurnost (ENISA) odgovorna je za osiguravanje usklađenosti proizvoda i usluga s utvrđenim kibersigurnosnim zahtjevima. OR naglašava potrebu da ENISA brzo razvije programe certifikacije kako bi se pružatelje usluga moglo certificirati s pomoću modernih tehnologija ([5]).

14. Kod stvaranja kibersigurnosne pričuve potrebno je pripaziti da se ne ometa tržišno natjecanje i da se ne isključuju pružatelji usluga koji djeluju samo u dijelovima Unije. Za uspostavu kibersigurnosne pričuve i certifikaciju potrebni su brzi i jasni postupci kako bi se utvrdili najkompetentniji i najvažniji akteri u tom kontekstu.

([4]) Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

([5]) ENISA trenutačno razvija tri postupka certifikacije – IKT, 5G i usluge računalstva u oblaku. https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq

15. OR smatra da bi trebalo identificirati nacionalne pružatelje tehnologija i usluga za kritične sustave i registrirati ih u bazi podataka. Ti podaci mogu biti vrlo vrijedni u kontekstu mjera koje zahtijevaju mobilizaciju lokalnih aktera, a mogli bi se upotrebljavati i u okviru rada Akademije za kibersigurnost.

16. U slučaju incidenta učinak protumjera ovisi o brzini odgovora. Složene informacije o sigurnosnim incidentima i rizicima koje se razmjenjuju moraju u kratkom roku doprijeti do pravih ciljnih skupina. Prijedlogom je predviđeno stvaranje nove organizacije i strukture za razmjenu informacija. Međutim, OR naglašava potrebu za upotrebom i razvojem postojećih informacijskih kanala kao što su CyCLONe ([6]) i CSIRT pri uspostavi nacionalnih i prekograničnih sigurnosnih centara.

Mehanizam za istraživanje kibersigurnosnih incidenata

Funkcija mu je istraživanje kibersigurnosnih incidenata, posebno incidenata koji su imali znatan učinak.

17. Potreba za vještinama u području kibersigurnosti i njihovim financiranjem povezana je s brzim razvojem digitalizacije. OR pozdravlja činjenicu da je Komisija osnovala akademiju za vještine u području kibersigurnosti. S obzirom na nedostatak kvalificirane radne snage u EU-u poziva na donošenje jasne strategije za jačanje manjih i financijski slabijih gradova i regija.

18. Odbor naglašava da snažna digitalna otpornost zahtijeva suradnju različitih aktera, u koju moraju biti uključeni javni i privatni subjekti sa svojim stručnim znanjem, iskustvom i osobljem. Ističe ulogu lokalnih i regionalnih vlasti u izgradnji digitalne otpornosti. One se mogu međusobno podupirati putem kampanja za podizanje svijesti, razmjena primjera najbolje prakse i razmjene stručnog znanja. Naime, što poduzeća više ulažu u svoju digitalnu otpornost, to će trošak napada za njihove protivnike biti veći, što bi također moglo imati odvraćajući učinak.

19. Trenutačno europski gradovi i regije sami snose troškove održavanja visoke razine kibersigurnosti, kao i troškove incidenata. OR smatra da postoji rizik da će predmetna uredba dodatno opteretiti već oskudne resurse. Uredba stoga ne smije stvoriti opterećenje, već doprinijeti jačanju kapaciteta svih subjekata s pomoću konkretnih alata, postupaka i potpore.

20. OR se pita zašto se izvješća o istraživanjima ne mogu razmjenjivati unutar mreže nacionalnih i prekograničnih centara za sigurnosne operacije. Naime, u Prijedlogu se predviđa da pristup javnim informacijama imaju samo nacionalni centri za sigurnosne operacije. Kako bi akteri poboljšali i dalje razvijali kibersigurnost, od iznimne je važnosti izvući pouke iz incidenata. Stoga bi sve pojedinosti o informacijama trebale biti dostupne svim sudionicima u mreži.

21. U Prijedlogu se o financiranju govori preopćenito. OR se zalaže za to da se detaljnije pojasni kako će se sredstva koristiti i koji se udio izravno dodjeljuje regijama i općinama.

([6]) Direktiva NIS 2, članak 16. stavci 1. i 3.
Europska mreža organizacija za vezu za kiberkrize (mreža EU-CyCLONe)
1. Mreža EU-CyCLONe osniva se kako bi se poduprlo koordinirano upravljanje kibersigurnosnim incidentima velikih razmjera i krizama na operativnoj razini i osigurala redovita razmjena relevantnih informacija među državama članicama te institucijama, tijelima, uredima i agencijama Unije.
3. Mreža EU-CyCLONe ima sljedeće zadaće:
(a) povećanje razine pripravnosti za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama;
(b) poboljšanje zajedničke informiranosti o kibersigurnosnim incidentima velikih razmjera i krizama;
(c) procjena posljedica i učinka relevantnih kibersigurnosnih incidenata velikih razmjera i kriza te predlaganje mogućih mjera ublažavanja;
(d) koordinacija upravljanja kibersigurnosnim incidentima velikih razmjera i krizama te pomoć pri odlučivanju na političkoj razini u pogledu takvih incidenata i kriza;
(e) rasprava, na zahtjev dotične države članice, o nacionalnim planovima za odgovor na kibersigurnosne incidente velikih razmjera i krize iz članka 9. stavka 4.

22. Naposljetku, Odbor naglašava da je Prijedlog u skladu s načelima supsidijarnosti i proporcionalnosti.

Bruxelles, 30. studenoga 2023.

Predsjednik
Europskog odbora regija

Vasco ALVES CORDEIRO