Europska komisija

GOVOR O STANJU UNIJE 2018.

Izgradnja snažne kibersigurnosti u Europi

#SOTEU

12. rujna 2018.

„Kibernapadi ne poznaju granica, ali kapaciteti za odgovor na njih znatno se razlikuju među državama članicama, zbog čega nastaju slabe točke i ranjivosti koji još više privlače napade. EU-u su potrebne čvršće i učinkovitije strukture kako bi se osigurala snažna otpornost na kibernapade i na te napade odgovorilo. Ne želimo biti najslabija karika u toj globalnoj prijetnji."

Jean-Claude Juncker, sastanak na vrhu o digitalnim pitanjima u Tallinnu, 29. rujna 2017.

Kako bi Europa dobila primjerene instrumente za suočavanje s kiberprijetnjama koje se neprestano mijenjaju, Europska komisija i Visoka predstavnica predložile su 2017. niz mjera za izgradnju snažne kibersigurnosti u Europi. Ti se napori sada nadopunjuju prijedlogom mjera kojima bi se EU-u olakšalo udruživanje resursa i stručnog znanja u području istraživanja i inovacija te omogućilo da postane predvodnik u tehnologijama kibersigurnosti i digitalnim tehnologijama sljedeće generacije.

Današnje kiberprijetnje

Zabilježeno je **više od 4000 napada ucjenjivačkim softverima** dnevno u 2016.

80 % europskih poduzeća prošle je godine bilo izloženo barem jednom kiberincidentu.

Sigurnosni incidenti u svim industrijama **povećali su se za 38 %**, što je najveće povećanje u zadnjih 12 godina.

U nekim državama članicama **50 % svih počinjenih kaznenih djela** odnosi se na kiberkriminalitet.

Više od 150 zemalja i više od 230 000 sustava u različitim sektorima i zemljama u svibnju 2017. pogođeno je napadom programa WannyCry, sa znatnim posljedicama na ključne usluge povezane s internetom, uključujući bolnice i službe hitne pomoći.

Jačanje otpornosti na kibernapade

Komisija već podupire jačanje otpornosti, odvraćanja i odgovora EU-a na kibernapade, među ostalim:

potporom učinkovitoj provedbi prvog zakona EU-a o kibersigurnosti (Direktiva o sigurnosti mrežnih i informacijskih sustava) radi:

JAČANJA SPOSOBNOSTI

Države članice trebaju poboljšati svoje kibersigurnosne sposobnosti.

SURADNJE

Pojačana suradnja na razini EU-a

SPRJEČAVANJA RIZIKA

Poduzeća u ključnim sektorima (kao što su energetika, promet, zdravstvo) dužna su uspostaviti mjere za sprječavanje rizika i odgovore na kiberincidente

suradnjom s državama članicama u sljedećim područjima:

AGENCIJA EU-A ZA KIBERSIGURNOST

Jačanje Agencije EU-a za kibersigurnost radi bolje podrške državama članicama

OKVIR CERTIFICIRANJA NA RAZINI EU-A

Okvir certificiranja na razini EU-a kojim se jamči da su proizvodi i usluge kibersigurni

KOORDINIRANI ODGOVOR

Osiguravanje brzog i koordiniranog odgovora na kibernapade velikih razmjera

Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA) pomaže tijelima država članica nadležnima za kibersigurnost da bolje štite EU od kibernapada.

Udruživanje resursa i stručnog znanja u području kibersigurnosnih tehnologija

Uz postojeće inicijative EU-a u području kibersigurnosti, Komisija danas predlaže da se ti napori pojačaju uspostavom mreže centara za kompetencije i Europskog centra za kompetencije u industriji, tehnologiji i istraživanjima u području kibersigurnosti u cilju razvoja i uvođenja alata i tehnologije potrebnih za praćenje prijetnji koje se neprestano mijenjaju.

Zajedno s državama članicama Europski centar bit će zadužen za koordinaciju sredstava predviđenih za kibersigurnost u sljedećem dugoročnom proračunu EU-a i njihovu najprimjereniju upotrebu. To će pridonijeti stvaranju novih europskih kiberkapaciteta.

Europa raspolaže velikim stručnim znanjem, a u EU-u postoji više od **660 centara za kompetencije** u području kibersigurnosti. Kako bi se njihovo stručno znanje učinkovito iskoristilo, Komisija predlaže mehanizam kojim će se:

- postojeće stručno znanje prikupljati i dijeliti te osigurati pristup tom znanju
- poticati uvođenje kibersigurnosnih proizvoda i rješenja u EU-u
- osigurati dugoročna strateška suradnja industrije, istraživačke zajednice i vlada
- zajednički ulagati u skupu strukturu i koristiti se njome

Europski centar za kompetencije:

koordinirat će upotrebu sredstava predviđenih za područje kibersigurnosti u okviru sljedećeg dugoročnog proračuna EU-a za razdoblje 2021.–2027. u okviru programa Digitalna Europa i Obzor Europa. Centar će podupirati rad mreže i zajednice u provedbi istraživanja i razvoja u području **kibersigurnosti**. Uz to će organizirati **zajednička ulaganja** EU-a, država članica i industrije. Na primjer, u okviru programa Digitalna Europa **2 milijarde EUR** uložit će se u zaštitu digitalnog gospodarstva, društva i demokracija EU-a jačanjem njegove industrije kibersigurnosti, financiranjem najsuvremenije opreme i infrastrukture za kibersigurnost.

Mreža nacionalnih koordinacijskih centara:

svaka država članica imenovat će jedan nacionalni koordinacijski centar koji će rukovoditi radom i sudjelovati u razvoju novih kibersigurnosnih sposobnosti i jačanju širih kompetencija. Ta mreža pomoći će otkriti najvažnije projekte u području kibersigurnosti u državama članicama i pružati im potporu.

Zajednica stručnjaka:

široka, otvorena i raznovrsna skupina dionika u području kibersigurnosti, od istraživača do privatnog i javnog sektora, koja uključuje civilna i vojna tijela.

Kakva se poboljšanja očekuju?

- bolja koordinacija rada
- pristup stručnom znanju
- pristup infrastrukturi za testiranje i eksperimentiranje
- ocjenjivanje kibersigurnosti proizvoda
- pristup inovativnim kibersigurnosnim proizvodima i rješenjima
- potpora tržišnom uvođenju proizvoda i rješenja
- poboljšana vidljivost prema potencijalnim ulagateljima i poslovnim partnerima
- snižavanje troškova zajedničkim ulaganjima s drugim državama članicama
- EU stječe sposobnost da samostalno osigura svoje gospodarstvo i demokratski poredak
- EU postaje svjetski predvodnik u području kibersigurnosti

Tko će od toga imati koristi?

Ured za publikacije

Print ISBN 978-92-79-92462-0 doi:10.2775/95720 NA-04-18-693-HR-C
PDF ISBN 978-92-79-92500-9 doi:10.2775/18829 NA-04-18-693-HR-N