

# Potrebno djelovanje

## **Što je problem i zašto?**

Digitalne tehnologije i internet okosnica su gospodarstva i društva EU-a. Funkcioniranje glavnih djelatnosti u kritičnim gospodarskim sektorima, primjerice prijevozu, energetici, zdravstvu ili financijama, sve više ovisi o mrežnim i informacijskim sustavima. Internet stvari putem komunikacijskih mreža povezuje predmete i ljude. Ta nova stvarnost donosi jedinstvene mogućnosti, ali i opasnosti. Kiberincidenti su zaista sve češća pojava te je vjerojatno da će se njihova složenost, učestalost i opseg utjecaja – od pristupa osnovnim uslugama do demokratskih procesa – i dalje povećavati.

U tom su kontekstu utvrđeni sljedeći međusobno povezani problemi:

* fragmentacija politika i pristupa kibersigurnosti u državama članicama;
* raspršenost resursa i pristupa kibersigurnosti u institucijama, agencijama i tijelima EU-a;
* nedovoljna osviještenost građana i poduzeća o kiberprijetnjama i nedovoljna informiranost o sigurnosnim značajkama proizvoda i usluga informacijskih i komunikacijskih tehnologija (IKT) koje kupuju, uz sve veći broj različitih nacionalnih i sektorskih programa certificiranja.

Ti problemi utječu na ukupnu kiberotpornost EU-a i učinkovito funkcioniranje unutarnjeg tržišta.

## **Što bi trebalo postići?**

Ovom se inicijativom posebno nastoji:

1. povećati sposobnost i pripremnost država članica i poduzeća, posebno u pogledu kritične infrastrukture;
2. poboljšati suradnju i koordinaciju među državama članicama i institucijama, agencijama i tijelima EU-a;
3. povećati razinu sposobnosti EU-a kako bi se dopunilo djelovanje država članica, posebno u slučaju prekograničnih kiberkriza;
4. povećati osviještenost građana i poduzeća o pitanjima kibersigurnosti;
5. povećati opću transparentnost u pogledu kibersigurnosti IKT proizvoda i usluga radi jačanja povjerenja u jedinstveno digitalno tržište i digitalne inovacije;
6. izbjegavanje fragmentiranja programa certifikacije u EU-u i povezanih sigurnosnih zahtjeva i evaluacijskih kriterija po državama članicama i sektorima.

## **Koja je dodana vrijednost djelovanja na razini EU-a?**

Budući da digitalizacija i međupovezanost gospodarstva i društva imaju globalni domet, dimenzije problema znatno nadilaze državno područje jedne države članice. Zbog toga je potrebno djelovanje na razini Unije. Uzimajući u obzir postojeći kontekst i buduće scenarije, može se zaključiti da pojedinačna djelovanja država članica i fragmentirani pristup kibersigurnosti, posebno njegova snažna prekogranična dimenzija, ne mogu povećati kolektivnu kiberotpornost Unije.

# Rješenja

## **Koje su opcije za postizanje ciljeva? Daje li se prednost određenoj opciji?**

U ovoj se procjeni učinka razmatraju posebne opcije politike, uključujući preispitivanje Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA) i sigurnosne certifikacije u području IKT-a.

***Preispitivanje ENISA-e***

**Opcija 0** – **Polazni scenarij** – podrazumijeva zadržavanje *statusa quo*. ENISA-in mandat bi se produljio, dok bi njezini ciljevi i zadaće ostali uglavnom nepromijenjeni, pri čemu bi se uzele u obzir zadaće koje bi se ENISA-i povjerile naknadnim zakonodavstvom EU-a (npr. Direktivom o sigurnosti mrežnih i informacijskih sustava).

**Opcija 1** – **Istek ENISA-ina mandata** (zatvaranje ENISA-e). Ta bi opcija dovela do zatvaranja ENISA-e na kraju njezina mandata (lipanj 2020.) i možda do redistribucije nadležnosti/aktivnosti na razini EU-a i/ili na nacionalnoj razini.

**Opcija 2** – **„Reformirana ENISA”**. Ta bi se opcija temeljila na postojećem mandatu ENISA-e, koji bi se dopunjavao pojedinačnim izmjenama kako bi se uzeo u obzir razvoj situacije u području kibersigurnosti. Agencija bi stekla stalni mandat, koji bi se temeljio na sljedećim ključnim elementima: potpora razvoju i provedbi politike EU-a; izgradnja kapaciteta; znanje i informacije; zadaće povezane s tržištem; istraživanje i inovacije; operativna suradnja i upravljanje krizama.

**Opcija 3** – **EU-ova agencija za kibersigurnost s punom operativnom sposobnošću**. Ta opcija podrazumijeva reformu ENISA-e objedinjenjem triju glavnih funkcija: 1. funkcije kreatora politike / savjetodavne funkcije; 2. funkcije centra za informacije i stručnost; i 3. funkcije tima za hitne računalne intervencije (CERT). Ta bi opcija u velikoj mjeri podrazumijevala istu promjenu opsega mandata kao i opcija 2. No uvele bi se nove zadaće u području odgovora na incidente i upravljanja krizama tako da bi Agencija pokrivala sve faze kibersigurnosnog ciklusa i bavila se sprječavanjem i otkrivanjem kiberincidenata te odgovorima na njih.

***Certificiranje***

**Opcija 0 –** **Polazni scenarij - bez promjena**. U skladu s tom opcijom Komisija bi zadržala *status quo* bez poduzimanja mjera politike ili zakonodavnih mjera.

**Opcija 1** – **Nezakonodavne (neobvezujuće) mjere**. U skladu s tom opcijom Komisija bi iskoristila neobvezujuće instrumente politike (npr. komunikacije o tumačenju, potpora samoregulatornim inicijativama i aktivnostima normizacije na razini EU-a) kako bi se povećala transparentnost i smanjila fragmentacija.

**Opcija 2 –** **zakonodavni akt EU-a o proširenju sporazuma Skupine viših dužnosnika za sigurnost informacijskih sustava (SOG-IS) na sve države članice**. U okviru te opcije Komisija bi predložila zakonodavni akt kojim bi se članstvo zakonski proširilo na sve države članice.

**Opcija 3** – **EU-ov opći okvir za sigurnosnu certifikaciju u području IKT-a**. Ta opcija podrazumijeva uspostavu Europskog okvira za sigurnosnu certifikaciju u području IKT-a (uključujući skupinu stručnjaka koju bi činila nacionalna tijela) što je više moguće na temelju postojećih programa sigurnosne certifikacije u području IKT-a. Uspostavom okvira omogućilo bi se uvođenje EU-ovih certifikacijskih programa koji će biti prihvaćeni u svim državama članicama.

Najprihvatljivija opcija jest kombinacija opcije 2 u pogledu ENISA-e i opcije 3 u pogledu certificiranja.

## **Tko su dionici? Tko podržava koju opciju?**

Može se zaključiti da velika većina dionika iz svih kategorija (države članice, industrija, institucije EU-a, istraživačka zajednica) koji su sudjelovali u savjetovanju pozdravljaju najprihvatljiviju opciju jer podržavaju jačanje ENISA-e i stvaranje Europskog okvira za sigurnosnu certifikaciju u području IKT-a.

Konkretno, postoji konsenzus o tome da je (kao minimum) potrebna agencija EU-a koja će imati stalni mandat, dobro funkcionirati, raspolagati dostatnim resursima i imati ovlasti za suočavanje s postojećim i budućim izazovima u području kibersigurnosti. Dionici se općenito slažu i oko stvaranja dobrovoljnog nadogradivog europskog okvira.

Kad je riječ o industriji, to rješenje za certificiranje podržavaju poduzeća koja već podliježu zahtjevima za certificiranje i koja bi imala koristi od EU-ova mehanizma utemeljenog na uzajamnom priznavanju certifikata. Podržavaju ga i MSP-ovi, koji snose ili bi snosili najteži teret u slučaju da u različitim državama članicama moraju proći različite certifikacijske postupke. Neke države članice, posebno one s manjim resursima, i pojedini predstavnici industrije i institucija EU-a izrazili su pozitivno mišljenje i za opciju 3 u pogledu ENISA-e.

# Učinci najprihvatljivije opcije

## **Koje su prednosti najprihvatljivije opcije (odnosno glavnih opcija ako ne postoji najprihvatljivija opcija)?**

U skladu s najprihvatljivijom opcijom, EU bi imao agenciju koja bi pružala pomoć državama članicama, institucijama EU-a i poduzećima u područjima u kojima bi to donijelo najveću dodanu vrijednost. Ta područja obuhvaćaju: potporu provedbi Direktive o sigurnosti mrežnih i informacijskih sustava; razvoj i provedbu politika; informacijsko znanje i osviještenost; istraživanje; operativnu suradnju i krize; tržište. Konkretno, ENISA bi podupirala politike EU-a povezane sa sigurnosnom certifikacijom u području IKT-a tako što bi osiguravala administrativno održavanje i tehničko upravljanje za europski okvir u tom području. Tim će se okvirom zapravo uspostaviti pravila za upravljanje sigurnosnom certifikacijom u području IKT-a u EU-u, kojima bi se promicao sustav uzajamnog priznavanja certifikata izdanih u državama članicama. Kombinacija tih opcija smatra se najprihvatljivijim rješenjem za EU u cilju postizanja sljedećih utvrđenih ciljeva: povećanja sposobnosti u području kibersigurnosti; pripremnosti; suradnje; osviještenosti; transparentnosti i izbjegavanja fragmentacije tržišta. Ta je opcija ujedno i najusklađenija s prioritetima politika jer se temelji na strategiji za kibersigurnost i povezanim politikama (npr. Direktiva o sigurnosti mrežnih i informacijskih sustava) i sa strategijom jedinstvenog digitalnog tržišta. Nadalje, ta opcija omogućuje postizanje ciljeva iskorištavanjem razumne količine resursa.

## **Kolike troškove podrazumijeva najprihvatljivija opcija (odnosno glavne opcije ako ne postoji najprihvatljivija opcija)?**

Iako bi dobila nove zadaće, „reformirana ENISA” i dalje bi bila agilna organizacija. Potrebni financijski doprinos iz proračuna EU-a bio bi veći od sadašnjeg, ali još znatno manji od onoga drugih agencija koje djeluju u kritičnim područjima.

Stvaranje Europskog okvira za sigurnosnu certifikaciju u području IKT-a ne bi podrazumijevalo dodatne početne troškove industrije (uključujući MSP-ove). Dapače, omogućio bi znatne uštede za poduzeća koja već certificiraju svoje proizvode ili koja su spremna provoditi sigurnosno certificiranje te bi pozitivno utjecao na njihovu konkurentnost u cijelom svijetu. S druge strane, bile bi potrebne određene proračunske obveze kako bi se osiguralo održavanje okvira, što bi se, kad je riječ o tehničkim i tajničkim poslovima, uglavnom osiguralo modelom „reformirane ENISA-e”.

## **Hoće li to znatno utjecati na nacionalne proračune i uprave?**

Ne. Troškovi povezani s jačanjem ENISA-e pokrili bi se uglavnom iz proračuna EU-a, dok bi države članice i dalje imale mogućnost pružanja dobrovoljnog financijskog doprinosa Agenciji. Kad je riječ o certificiranju, glavni utjecaj na nacionalne proračune i uprave proizlazio bi iz osnivanja tijela za certificiranje, gdje je to primjereno.

## **Hoće li biti drugih bitnih učinaka?**

Ne.

## **Proporcionalnost**

Najprihvatljivija opcija uključuje uravnotežene mjere koje se smatraju potrebnima za postizanje predmetnog cilja i ne uzrokuju prekomjerno opterećenje za relevantne dionike. U tom svjetlu smatra se da je ova inicijativa u skladu s načelom proporcionalnosti.

# Daljnji koraci

## **Kad će se politika preispitati?**

Predloženo je da se prva evaluacija provede pet godina nakon što pravni instrument stupi na snagu. Komisija će Europskom parlamentu i Vijeću podnijeti izvješće o svojoj evaluaciji, zajedno s prijedlogom njegova preispitivanja bude li to potrebno. Daljnje evaluacije provodit će se svakih pet godina.