Evropska komisija priporočila skupen pristop EU k varnostnim tveganjem za omrežja 5G

Strasbourg, 26. marca 2019

Komisija je danes priporočila sklop operativnih ukrepov in ukrepov za zagotovitev visoke ravni kibernetske varnosti omrežij 5G po vsej EU.

Omrežja pete generacije (5G) bodo prihodnja hrbtenica naših družb in gospodarstev, ki bo povezovala milijarde objektov in sistemov, tudi v kritičnih sektorjih, kot so energija, promet, bančništvo in zdravstvo, ter sisteme za industrijsko kontrolo, ki bodo prenašali občutljive informacije in podpirali varnostne sisteme. Demokratični procesi, kot so volitve, so vse bolj odvisni od digitalnih infrastruktur in omrežij 5G, zato v ospredje prihaja potreba po odpravljanju morebitnih šibkih točk, priporočila Komisije pa so pred majskimi volitvami v Evropski parlament vse aktualnejša.

Po podpori usklajenemu pristopu k varnosti omrežij 5G, ki so jo voditeljice in voditelji držav in vlad izrazili na zasedanju Evropskega sveta 22. marca, Komisija danes priporoča sklop konkretnih ukrepov za oceno tveganj za kibernetsko varnost omrežij 5G in okrepitev preventivnih ukrepov. Priporočila so kombinacija zakonodajnih in političnih instrumentov za zaščito naših gospodarstev, družb in demokratičnih sistemov. S prihodki 5G, ki naj bi po oceni leta 2025 na svetovni ravni znašali 225 milijard EUR, je 5G ključ do konkurenčnosti Evrope na svetovnem trgu, njena kibernetska varnost pa je bistvena za zagotavljanje strateške avtonomije Unije.

Podpredsednik Komisije Andrus **Ansip**, pristojen za enotni digitalni trg, je dejal: *„Tehnologija 5G bo preoblikovala naše gospodarstvo in družbo ter prinesla ogromne priložnosti za ljudi in podjetja. A to se ne sme zgoditi, ne da bi bilo ob tem poskrbljeno za popolno varnost. Zato je bistveno, da je infrastruktura 5G v EU odporna in v celoti zavarovana pred tehničnimi ali pravnimi vrzelmi.*"

Komisar Julian **King**, pristojen za varnostno unijo, je dejal: *„Odpornost naše digitalne infrastrukture je ključnega pomena za vlade, podjetja, varnost naših osebnih podatkov in delovanje naših demokratičnih institucij. Razviti moramo evropski pristop k zaščiti celovitosti omrežja 5G, ki bo digitalno življenje naših prepletenih življenj.*"

Komisarka Marija **Gabriel**, pristojna za digitalno gospodarstvo in družbo, je dodala: *„Zaščita omrežij 5G je namenjena zaščiti infrastrukture, ki bo podpirala bistvene družbene in gospodarske funkcije, kot so energija, promet, bančništvo in zdravje, pa tudi veliko bolj avtomatizirane tovarne prihodnosti. Pomeni tudi zaščito demokratičnih procesov, kot so volitve, pred vmešavanjem in širjenjem dezinformacij.*"

Vsaka šibka točka v omrežjih 5G ali kibernetski napad, usmerjen v prihodnja omrežja v eni državi članici, bi prizadela Unijo kot celoto. Zato morajo usklajeni ukrepi, sprejeti na nacionalni in evropski ravni, zagotoviti visoko raven kibernetske varnosti.

Današnje priporočilo razgrinja vrsto **operativnih ukrepov**:

1. Na nacionalni ravni

Vsaka država članica bi morala do konca junija 2019 dokončati nacionalno oceno tveganja za omrežno infrastrukturo omrežja 5G. Na podlagi tega bi morale države članice posodobiti obstoječe varnostne zahteve za ponudnike dostopa do omrežja in vključiti pogoje za zagotavljanje varnosti javnih omrežij, zlasti pri podeljevanju pravic uporabe radijskih frekvenc v pasovih 5G. Ti ukrepi bi morali vključevati okrepljene obveznosti za dobavitelje in operaterje, da se zagotovi varnost omrežij. Pri nacionalnih ocenah tveganja in ukrepih bi bilo treba upoštevati različne dejavnike tveganja, kot so tehnična tveganja in tveganja, povezana z ravnanjem dobaviteljev ali operaterjev, tudi tistih iz tretjih držav. Nacionalne ocene tveganja bodo osrednji element za pripravo ocene tveganja na ravni EU.

Države članice EU imajo pravico, da podjetja iz nacionalnovarnostnih razlogov izključijo iz svojih trgov, če ne izpolnjujejo standardov in pravnega okvira države.

2. Na ravni EU

Države članice bi si morale med seboj izmenjevati informacije ter bodo ob podpori Komisije in Evropske agencije za kibernetsko varnost (ENISA) dokončale usklajeno oceno tveganja do 1. oktobra 2019. Na tej podlagi se bodo države članice dogovorile o sklopu ukrepov za zmanjšanje tveganja, ki se lahko

uporabijo na nacionalni ravni. Ti lahko vključujejo zahteve po certificiranju, preskuse, nadzore in določanje izdelkov ali dobaviteljev, ki veljajo za potencialno tvegane. To delo bo s pomočjo Komisije in agencije ENISA opravila skupina pristojnih organov za sodelovanje, kakor je določeno v direktivi o varnosti omrežij in informacijskih sistemov. To usklajeno delo bi moralo podpirati ukrepe držav članic na nacionalni ravni in Komisiji zagotoviti smernice za morebitne nadaljnje ukrepe na ravni EU. Poleg tega bi morale države članice oblikovati posebne varnostne zahteve, ki bi se lahko uporabljale v okviru javnih naročil, povezanih z omrežji 5G, vključno z obveznimi zahtevami po izvajanju certifikacijskih shem za kibernetsko varnost.

Z današnjim priporočilom se izkorišča **širok nabor instrumentov**, ki se že uporabljajo oziroma je o njih že bil dosežen dogovor, za okrepitev sodelovanja na področju kibernetskih napadov in omogoči skupno delovanje EU na področju zaščite njenega gospodarstva in družbe, vključno s prvim vseevropskim aktom o kibernetski varnosti (direktivo o varnosti omrežij in informacijskih sistemov), uredbo o kibernetski varnosti, ki jo je pred kratkim odobril Evropski parlament, in novimi telekomunikacijskimi pravili. Priporočilo bo državam članicam pomagalo pri skladnem izvajanju teh novih instrumentov v zvezi z varnostjo 5G.

Na področju kibernetske varnosti bi moral prihodnji evropski certifikacijski okvir za kibernetsko varnost za digitalne izdelke, postopke in storitve, predviden v aktu o kibernetski varnosti, vzpostaviti bistveno podporno orodje za spodbujanje enako visokih ravni varnosti. Pri njegovem izvajanju bi morale države članice prav tako nemudoma in dejavno sodelovati z vsemi drugimi deležniki pri razvoju namenskih certifikacijskih shem na ravni EU, ki se nanašajo na 5G. Ko bodo na voljo, bi morale države članice certificiranje na tem področju z nacionalnimi tehničnimi predpisi predpisati kot obvezno.

Na področju telekomunikacij morajo države članice zagotoviti ohranjanje integritete in varnosti javnih komunikacijskih omrežij, hkrati pa morajo z obveznostmi poskrbeti, da operaterji sprejmejo tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganj za varnost omrežij in storitev.

Naslednji koraki

- Države članice bi morale dokončati svoje nacionalne ocene tveganja do **30. junija 2019** in posodobiti potrebne varnostne ukrepe. Nacionalna ocena tveganja bi morala biti posredovana Komisiji in Evropski agenciji za kibernetsko varnost do **15. julija 2019**.
- Vzporedno bodo države članice in Komisija začele usklajevati prizadevanja v skupini za sodelovanje na področju VOI. Agencija ENISA bo dokončala kartiranje groženj za omrežja 5G, s katerim bo države članice podprla pri izvedbi ocene tveganja na ravni EU do **1. oktobra 2019**.
- Skupina za sodelovanje na področju VOI bi se morala do **31. decembra 2019** dogovoriti o ukrepih za zmanjševanje tveganj, ki bi omogočili obravnavo tveganja za kibernetsko varnost, ugotovljena na nacionalni ravni in ravni EU.
- Ko bo akt o kibernetski varnosti, ki ga je nedavno odobril Evropski parlament, v prihodnjih tednih začel veljati, bosta Komisija in Agencija ENISA vzpostavili vseevropski certifikacijski okvir. Države članice se spodbuja, naj sodelujejo s Komisijo in Agencijo ENISA pri dajanju prednosti certifikacijski shemi, ki zajema omrežja in opremo 5G.
- Države članice bi morale do **1. oktobra 2020** v sodelovanju s Komisijo oceniti učinke priporočila, da se ugotovi, ali je potrebno nadaljnje ukrepanje. Pri tej oceni bi bilo treba upoštevati rezultate usklajene evropske ocene tveganja in učinkovitost nabora orodij.

Ozadje

Evropski svet je v svojih sklepih z dne 22. marca izrazil podporo priporočilu Komisije o usklajenem pristopu k varnosti omrežij 5G. Resolucija Evropskega parlamenta, izglasovana 12. marca, o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU prav tako poziva Komisijo in države članice, naj ukrepajo na ravni Unije.

Poleg tega je kibernetska varnost omrežij 5G je ključna za zagotavljanje strateške avtonomije Unije, kar je poudarjeno tudi v skupnem sporočilu „EU-Kitajska: strateška vizija". Zato je bistveno in nujno, da se obstoječa varnostna pravila na tem področju pregledajo in okrepijo, s čimer se zagotovi, da odražajo strateški pomen omrežij 5G in razvoj groženj, vključno z vse večjim številom in izpopolnjenostjo kibernetskih napadov. 5G je ključ do konkurenčnosti Evrope na svetovnem trgu. Na svetovni ravni naj bi v letu 2025 prihodki 5G dosegli 225 milijard evrov. Drug vir navaja, da koristi uvedbe 5G v štirih ključnih industrijskih sektorjih, in sicer avtomobilskem, zdravstvenem, prometnem in energetskem, lahko dosežejo 114 milijard evrov na leto.

Več informacij

Priporočilo o kibernetski varnosti omrežij 5G

Vprašanja in odgovori

Varnostna unija: dogovor doslej dosežen o 15 od 22 zakonodajnih pobud

Sporočilo za medije: Pogajalci EU dosegli dogovor o okrepitvi kibernetske varnosti v Evropi

Sporočilo za medije: Skupno sporočilo „EU-Kitajska: strateška vizija“

IP/19/1832

Kontakti za stike z mediji:

Nathalie VANDYSTADT (+32 2 296 70 83)
Marietta GRAMMENOU (+32 2 298 35 83)

Za vprašanja širše javnosti: Europe Direct po telefonu 00 800 67 89 10 11 ali e-pošti