Evropska komisija

STANJE V UNIJI 2018

Okrepitev kibernetske varnosti v Evropi

#SOTEU

12. septembra 2018

„Kibernetski napadi ne poznajo meja, vendar se odzivne zmogljivosti od ene države do druge zelo razlikujejo. Tako nastajajo vrzeli, ki povzročajo ranljivosti in še več napadov. EU potrebuje trdne in učinkovite strukture za zagotavljanje močne kibernetske odpornosti in odziva na kibernetske napade. Pri tej svetovni grožnji nočemo biti najšibkejši člen.“

Jean-Claude Juncker, digitalni vrh v Talinu, 29. septembra 2017

Evropska komisija in visoka predstavnica sta leta 2017 predlagali obsežen sklop ukrepov za okrepljeno kibernetsko varnost v EU, da bi imela Evropa na voljo prava orodja, s katerimi bi se lahko branila pred vseskozi spreminjajočimi se kibernetskimi grožnjami. Ta prizadevanja zdaj dopolnjuje predlog, ki bo EU pomagal združiti vire in strokovno znanje o raziskavah in inovacijah ter postati vodilna sila na področju kibernetskovarnostnih in digitalnih tehnologij naslednje generacije.

Današnje kibernetske grožnje

Leta 2016 se je v Evropi vsak dan zgodilo **več kot 4 000 napadov z izsiljevalskim programjem**.

Lani je **80 % evropskih podjetij** doživelo vsaj en kibernetski incident.

Število varnostnih incidentov se je v vseh panogah **povečalo za 38 %**, kar je največje povečanje v zadnjih 12 letih.

V nekaterih državah članicah kibernetska kazniva dejanja predstavljajo **50 % vseh kaznivih dejanj**.

Napad Wannycry maja 2017 je čezmejno in čezsektorsko prizadel **več kot 150 držav in 230 000 sistemov**, kar je znatno vplivalo na bistvene storitve, povezane z internetom, vključno z bolnišnicami in reševalnimi službami.

Krepitev odpornosti na kibernetske napade

Komisija že podpira krepitev odvračanja kibernetskih napadov ter odpornosti in odzivanja na njih, vključno z naslednjim:

Podpiranje učinkovitega izvajanja prve zakonodaje EU o kibernetski varnosti (direktive o varnosti omrežij in informacijskih sistemov) na podlagi:

VEČJIH ZMOGLJIVOSTI

države članice morajo izboljšati svoje zmogljivosti na področju kibernetske varnosti

SODELOVANJA

krepitev sodelovanja na ravni EU

PREPREČEVANJA TVEGANJA

akterji v ključnih sektorjih (kot so energija, prevoz, zdravje) morajo vzpostaviti ukrepe za preprečevanje tveganja in obvladovanje kibernetskih incidentov

Sodelovanje z državami članicami na področju:

AGENCIJE EU ZA KIBERNETSKO VARNOST

krepitev Agencije EU za kibernetsko varnost za učinkovitejšo pomoč državam članicam

CERTIFIKACIJSKEGA OKVIRA EU

vseevropski certifikacijski okvir za zagotovitev kibernetsko varnih proizvodov in storitev

USKLAJENEGA ODZIVA

zagotavljanje hitrega in usklajenega odziva na obsežne kibernetske napade

Agencija Evropske unije za varnost omrežij in informacij (ENISA) organom držav članic za kibernetsko varnost pomaga bolje zaščititi EU pred kibernetskimi napadi.

Združevanje virov in strokovnega znanja na področju kibernetskovarnostne tehnologije

Komisija kot dopolnitev že obstoječih pobud EU za kibernetsko varnost danes predlaga, da se navedena prizadevanja dopolnijo z vzpostavitvijo mreže strokovnih centrov in Evropskega industrijskega, tehnološkega in raziskovalnega centra za kibernetsko varnost ter da se tako podpre razvoj in uvajanje orodij in tehnologij, brez katerih ni mogoče iti v korak z grožnjami, ki se ves čas spreminjajo.

Evropski center bo z državami članicami čim bolj usmerjeno usklajeval sredstva, predvidena za kibernetsko varnost v naslednjem dolgoročnem proračunu EU. Tako bo prispeval k ustvarjanju novih evropskih kibernetskih zmogljivosti.

Evropa ima bogato strokovno znanje – v EU je več kot **660 strokovnih centrov za kibernetsko varnost**. Za učinkovito izkoriščanje njihovega strokovnega znanja Komisija predlaga mehanizem za:

združevanje, izmenjavo in dostop do obstoječega strokovnega znanja

pomoč pri uvajanju izdelkov in rešitev za kibernetsko varnosti

zagotavljanje dolgoročnega strateškega sodelovanja med panogami, raziskovalnimi skupnostmi in vladami

sovlaganje in souporabo drage infrastrukture

Evropski strokovni center:

Upravljal bo porabo sredstev za kibernetsko varnost, predvidenih v naslednjem dolgoročnem proračunu EU za obdobje 2021–2027 v okviru programa za digitalno Evropo in programa Obzorje Evropa. Podpiral bo mrežo in skupnost pri spodbujanju raziskav in inovacij na področju **kibernetske varnosti**. Organiziral bo tudi **skupne naložbe** EU, držav članic in industrije. V okviru programa za digitalno Evropo bo na primer zagotovljena naložba v višini **2 milijard evrov** za zaščito digitalnega gospodarstva, družbe in demokracij EU s pospeševanjem panoge kibernetske varnosti v EU in financiranjem najsodobnejše opreme in infrastrukture za kibernetsko varnost.

Mreža nacionalnih koordinacijskih centrov:

Vsaka država članica bo imenovala en nacionalni koordinacijski center, ki bo vodil mrežo in sodeloval pri razvoju novih zmogljivosti kibernetske varnosti in krepitvi širših kompetenc. Mreža bo pomagala opredeliti in podpreti najpomembnejše projekte s področja kibernetske varnosti v državah članicah.

Strokovna skupnost:

Velika, odprta in raznolika skupina zainteresiranih strani na področju kibernetske varnosti tako iz raziskovalne skupnosti kot iz zasebnega in javnega sektorja, vključno s civilnimi in obrambnimi organi.

Kaj se bo izboljšalo?

- boljše usklajevanje dela;
- dostop do strokovnega znanja;
- dostop do zmogljivosti za preizkušanje in eksperimentiranje;
- ocenjevanje kibernetske varnosti izdelka;
- dostop do inovativnih izdelkov in rešitev za kibernetsko varnost;
- podpora pri uvajanju izdelkov in storitev na trg;
- večja prepoznavnost za potencialne vlagatelje in poslovne partnerje;
- prihranek stroškov zaradi sovlaganja z drugimi državami članicami;
- EU bo zmožna samostojno zaščititi svoje gospodarstvo in demokracijo;
- EU bo postala vodilna v svetu na področju kibernetske varnosti.

Kdo bo imel koristi?

Urad za publikacije

Print ISBN 978-92-79-92503-0 doi:10.2775/65460 NA-04-18-693-SL-C
PDF ISBN 978-92-79-92466-8 doi:10.2775/84333 NA-04-18-693-SL-N