Evropa s skupnimi močmi v Cyber Europe 2012

Več kot 300 evropskih strokovnjakov za kibernetsko varnost danes v drugi vseevropski vaji Cyber Europe 2012, s skupnimi močmi preizkuša svoje sposobnosti odzivanja v simuliranem kibernetskem napadu. Vaja temelji na združevanju obsežnih aktivnosti, na nacionalnih in na evropski ravni, z namenom izboljšati odpornost najpomembnejše informacijske infrastrukture. Cyber Europe 2012 tako predstavlja pomemben mejnik v prizadevanjih za krepitev sodelovanja, pripravljenosti in odzivov po vsej Evropi v primeru kibernetske krize.

Vaja Cyber Europe 2012 je druga vseevropska vaja iz zaščite kritične informacijske infrastrukture. Namen vaje je povezati aktivnosti in vire na nacionalnem in nivoju Evropske unije, s ciljem izboljšati odpornost kritične informacijske infrastrukture. Cyber Europe 2012 se izvaja kot porazdeljena simulacijska (table-top) vaja, ki jo organizirajo države članice EU in EFTA, usklajuje jo Evropska agencija za varnost omrežij in informacij (European Network and Information Security Agency - ENISA), podporo pa ji zagotavlja Skupno raziskovalno središče Evropske komisije (the Joint Research Centre - JRC). V okviru vaje se generirajo navidezni incidenti in ne napadi na realna omrežja. V primerjavi z vajo iz leta 2010 pomeni projekt Cyber Europe 2012 velik napredek v smislu obsega, razširjenosti in kompleksnosti zadanih nalog.

Cilji vaje Cyber Europe 2012, so:

- **Preizkusiti učinkovitost obstoječih mehanizmov, postopkov in informacijskih tokov pri sodelovanju javnih inštitucij v Evropi v primeru kibernetskih incidentov velikih razsežnosti.**

- **Raziskati sodelovanje med javnimi in zasebnimi deležniki v Evropi v primeru kibernetskih incidentov velikih razsežnosti.**

- **Prepoznati pomanjkljivosti in razvojne izzive, da bi kibernetske incidente velikih razsežnosti v Evropi lahko obravnavali bolj učinkovito.**

Na vaji imajo štiri države vlogo opazovalk, medtem ko 25 držav v njej sodeluje aktivno, med njimi tudi Republika Slovenija. V vaji sodelujejo predstavniki e-uprav, po izkušnjah iz prve vseevropske vaje Cyber Europe 2010, pa so v vajo prvič vključena tudi zasebna podjetja iz finančnega sektorja in ponudniki internetnih storitev. V vaji udeleženci – igralci iz javnega in zasebnega sektorja izvajajo ukrepe na nacionalni ravni, hkrati udeleženci iz javnega sektorja sodelujejo prek meja.

V Republiki Sloveniji so v vajo vključeni naslednji igralci:

- Ministrstvo za pravosodje in javno upravo,
- Ministrstvo za izobraževanje, znanost, kulturo in šport,
- Ministrstvo za obrambo Republike Slovenije,
- Nacionalni odzivni center za omrežne incidente SI-CERT pri javnem zavodu Arnes,
- Javni zavod Arnes – Akademska in raziskovalna mreža Slovenije,
- Nova ljubljanska banka d.d.,
- Deželna banka Slovenije d.d.,
- Amis d.o.o.,
- T-2 d.o.o. in
- Telekom Slovenije d.d.

Scenarij vaje Cyber Europe 2012 predvideva kombinacijo več tehnično realnih groženj v okviru enega sočasno stopnjevanega porazdeljenega napada za zavrnitev dostopa (DDoS napad) do spletnih storitev v vseh udeleženih držav. Takšen scenarij bi povzročil motnje za milijone uporabnikov po vsej Evropi.

Kompleksnost scenarija omogoča izvedbo zadostnega števila kibernetskih napadov, da izzovejo več sto udeležencev iz javnega in zasebnega sektorja iz vse Evrope, hkrati pa sprožijo medsebojno sodelovanje. Do zaključka vaje se bodo udeleženci spopadli z več kot 1000 simuliranimi kibernetskimi napadi.

Profesor Udo Helmbrecht, izvršni direktor ENISE, je ob tej priložnosti dejal:
“ENISA si prizadeva, da bi skupnosti, ki se ukvarja s kibernetskimi krizami pomagala izboljšati odpornost najpomembnejše informacijske infrastrukture. Zato smo organizirali projekt Cyber Europe 2012.”

Ozadje

Leta 2010 je Evropska komisija izdala strategijo za varno informacijsko družbo, v kateri je posebej izpostavila pomen dialoga in sodelovanja pri krepitvi struktur za zagotavljanje informacijske varnosti v Evropi. V sporočilu o zaščiti kritične informacijske infrastrukture (CIIP Communication) je komisija predlagala aktivnosti za razvoj načel in navodil za zagotavljanje odpornosti interneta in predloge za izvedbo vseevropskih vaj o napadih na omrežno varnost velikih razsežnosti. S tem naj bi tudi vzpostavili okvir za evropsko sodelovanje v globalnih vajah. Na nivoju Evropske unije je jasno zavedanje, da je simulacija varnostnih incidentov in izvajanje vaj za testiranje sposobnosti odzivanja nanje, strateškega pomena, in da s tem lahko izboljšamo splošno varnost in odpornost kritične informacijske infrastrukture. V tem okviru je Evropska komisija države članice pozvala, da pripravijo ustrezne nacionalne področne strategije in organizirajo nacionalne vaje o odzivanju na incidente omrežne varnosti velikih razsežnosti, s čimer naj bi se članice usposobile za

tesnejše vseevropsko sodelovanje. Republika Slovenija bo nacionalno vajo o informacijski varnosti izvedla v prvi polovici leta 2013.

Leta 2009 je ENISA objavila priročnik dobrih praks za vaje na nacionalni ravni 'Good Practice Guide on National Exercises' in odtlej v pomoč pri načrtovanju tovrstnih vaj organizirala že vrsto delavnic po vsej Evropi. V kratkem bo objavila priročnik o nacionalnem načrtovanju izrednih ukrepov.

Obvestilo
Vaja ne vpliva na delovanje obstoječe kritične informacijske infrastrukture, sisteme ali storitve.

Sporočilo za medije na spletni strani:
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-i

Za intervjuje: Graeme Cooper, Vodja za javne zadeve, ENISA, GSM: +30 6951 782 268, Graeme.Cooper@enisa.europa.eu