

EUpravo zato/
Stefan Badža

Evropska komisija predstavila je početkom jula Akcioni plan za sajber bezbednost i veštačku inteligenciju, prvi dokument kojim se ove dve oblasti posmatraju kao jedinstven bezbednosni izazov. Plan dolazi u trenutku kada razvoj veštačke inteligencije istovremeno otvara nove mogućnosti za zaštitu informacionih sistema, ali i stvara prostor za sofisticiranije sajber napade.

Kako navodi Evropska komisija, veštačka inteligencija može da pomogne u otkrivanju i otklanjanju bezbednosnih propusta, ali ista tehnologija može biti iskorišćena za automatsko pronalaženje ranjivosti, ubrzavanje napada i izvođenje incidenata kakvi do sada nisu zabeleženi.

Potpredsednica Evropske komisije za tehnološki suverenitet, bezbednost i demokratiju Hena Virkunnen ocenila je da veštačka inteligencija menja samu prirodu sajber bezbednosti i da Evropa mora da razvije sopstvene kapacitete kako bi odgovorila na nove pretnje.

AI menja pravila

Poslednjih meseci sve je više primera koji potvrđuju da opasnost nije samo teorijska. Kompanija „Anthropic“ saopštila je da je njen eksperimentalni model Claude Mythos Preview tokom internih testiranja pokazao izuzetne sposobnosti u pronalaženju i iskorišćavanju softverskih ranjivosti, nadmašivši gotovo sve stručnjake, osim najboljih eksperata iz te oblasti. Isti model uspeo je da pronađe bezbednosni propust star čak 27 godina u operativnom sistemu OpenBSD, jednom od najbezbednijih na svetu.

To potvrđuje da tehnologija koja pomaže u otkrivanju i uklanjanju bezbednosnih propusta može biti iskorišćena i za njihovu zloupotrebu. U sajber bezbednosti taj odnos nije ravnopravan - odbrana mora da zaštiti svaki potencijalni propust, dok je napadaču dovoljan samo jedan.

Istovremeno, pitanje pristupa najnaprednijim AI modelima postaje i geopolitičko pitanje. O tome danas uglavnom odlučuju kompanije koje ih razvijaju, ali i države u kojima se oni stvaraju. Evropski

akcioni plan predstavlja prvi pokušaj da evropske institucije dobiju veću ulogu u određivanju pravila korišćenja ovih tehnologija.

Šta predviđa evropski plan

Akcioni plan zasniva se na tri ključna stuba.

Prvi se odnosi na razvoj i kontrolu najnaprednijih AI modela. Evropska unija planira da tokom 2027. formira stručne timove za njihovu procenu, dok bi do kraja ove godine Evropska agencija za sajber bezbednost (ENISA) i Zajednički istraživački centar Evropske komisije trebalo da uspostave bezbednu platformu za testiranje i pripreme smernice o tome ko i pod kojim uslovima može da koristi najnaprednije modele veštačke inteligencije.

Te smernice neće predstavljati novu zakonsku obavezu, već preporuke koje će biti usklađene s pravilima evropskog Akta o veštačkoj inteligenciji (AI Act).

Drugi deo plana usmeren je na unapređenje

osnovne sajber higijene kroz primenu postojećih evropskih propisa, poput NIS2 direktive, DORA uredbe i Akta o sajber otpornosti. Plan predviđa unapređenje evropske baze ranjivosti, kao i pokretanje programa za zaštitu ključnog softvera otvorenog koda, čije održavanje često zavisi od malih razvojnih timova, uprkos njegovom velikom značaju za digitalnu infrastrukturu.

Treći segment odnosi se na finansiranje. Evropska unija već je obezbedila ili planirala oko 200 miliona evra kroz programe „Horizont Evropa“ i „Di-

gitalna Evropa“, dok će kompanije koje razvijaju rešenja na preseku veštačke inteligencije i sajber bezbednosti moći da konkuriraju i za deo sredstava iz paketa Evropskog saveta za inovacije namenjenog strateškim tehnologijama. Najavljeno je i evropsko takmičenje u pronalaženju i otklanjanju softverskih ranjivosti pomoću veštačke inteligencije.

Značaj za Srbiju

Za Srbiju je ovaj plan značajniji nego što se na prvi pogled čini. Novi Zakon o informacionoj bezbednosti iz 2025. godine donet je upravo radi uskla-

divanja s principima evropske NIS2 direktive, zbog čega standardi predviđeni novim evropskim planom predstavljaju nastavak procesa kojem se domaći sistem već prilagođava.

Brojne srpske kompanije koje posluju s partnerima iz Evropske unije već se suočavaju sa zahtevima za procenu upravljanja sajber rizicima, a sve češće i s pitanjima o načinu korišćenja alata zasnovanih na veštačkoj inteligenciji. Ti zahtevi u praksi često dolaze kroz poslovne ugovore i tržišne standarde mnogo pre nego što postanu zakonska obaveza.

Srbija, kao pridružena članica programa „Horizont Evropa“ i „Digitalna Evropa“, ima mogućnost da učestvuje na konkursima koji će biti raspisivani u okviru ovog plana, u skladu sa uslovima pojedinačnih poziva. To otvara priliku domaćim istraživačima, kompanijama i startapima da obezbede evropsko finansiranje i razviju partnerstva sa institucijama iz država članica EU.

Poseban značaj plan može imati za zajednicu koja u Srbiji razvija rešenja iz oblasti sajber bezbednosti i veštačke inteligencije, naročito u Beogradu, gde se poslednjih godina formira sve snažniji inovacioni ekosistem.

Evropski plan ujedno pokazuje i koje će kompetencije biti najtraženije u narednim godinama - procena bezbednosti AI sistema, testiranje naprednih modela, upravljanje pristupom veštačkoj inteligenciji i unapređenje bezbednosti softvera otvorenog koda. Stručnjaci i organizacije koji razvijaju znanja u tim oblastima moći će da odgovore na potrebe evropskog tržišta i institucija.

Za razliku od brojnih strateških dokumenata, ovaj akcioni plan sadrži precizne rokove, jasno određene institucije zadužene za sprovođenje i obezbeđena finansijska sredstva. Već tokom naredne godine biće moguće proceniti u kojoj meri su planirane mere zaista sprovedene u praksi.

IZAZOV

EVROPA GRADI ODBRANU OD SAJBER NAPADA POMOĆU VEŠTAČKE INTELIGENCIJE

Evropska komisija prvi put objedinjuje veštačku inteligenciju i sajber bezbednost u jedinstveni akcioni plan, kojim želi da ojača digitalnu otpornost, reguliše pristup najnaprednijim AI modelima i smanji tehnološku zavisnost od drugih svetskih sila



ŠTA JE NIS2 DIREKTIVA

Stroži standardi sajber bezbednosti

● NIS2 je evropski propis kojim se uvode stroži standardi sajber bezbednosti za javni i privatni sektor. Srbija je donošenjem novog Zakona o informacionoj bezbednosti tokom 2025. godine započela usklađivanje sa ovim pravilima, zbog čega će veliki deo evropskih zahteva biti relevantan i za domaće institucije i privredu.

