



Datum: 23.07.2026

Medij: Profit

Rubrika: Info

Autori: redakcija

Teme: Evropska komisija

Napomena:

Površina: 1123



Naslov: Srbija na mapi globalnog sajber ekosistema

Strana: 10,11

PROFIT | Info

Da li prepoznamo našu šansu?

Srbija na mapi globalnog sajber ekosistema

Samo u prvim mesecima 2026. godine lista pogođenih čitala se kao spisak institucija koje bi trebalo da budu nedodirljive. Evropska komisija je u martu potvrdila sajber napad na cloud infrastrukturu svoje Europa platforme. Francuska državna agencija zadužena za izdavanje ličnih karata i pasoša priznala je u aprilu upad u kome su izvučeni lični podaci do 19 miliona građana. Eurail, servis kojim putuju milioni ljudi širom Evrope, ostao je bez podataka putnika, uključujući i brojeve pasoša, koji su potom ponuđeni na prodaju.

Ni ne moramo da gledamo ka Parizu ili Briselu da bismo videli istu sliku. Srbija nije izuzetak, Srbija prati trend. Prema podacima o visokotehnološkom kriminalu MUP-a Srbije, broj prijava raste oko 30 odsto godišnje, i to već nekoliko godina zaredom, a kao uzrok se navode upravo digitalizacija. Internet prevare i zloupotrebe platnih kartica danas čine oko polovine svih prijava, u toku 2025. u kriptovalutama je zamrznuto 1,3 miliona evra itd. Ovo nije pretnja koja se dešava negde drugde. Ona je već ovde, na našim nalogima, karticama i mejlovima.

Ono što povezuje većinu ovih napada nije nikakav tehnološki podvig. Nije bila potrebna nijedna linija sofisticiranog koda. U osnovi su najčešće pogrešno podešen sistem, propust u nadzoru ili jedan klik na pogrešan link. Drugim rečima, ljudska greška.

Ti slučajevi nisu izuzeci. Ovakvi napadi dešavaju se svakodnevno, u kompanijama svih veličina i u svim sektorima. I svaki put kada se dogode, javlja se ista potreba za timom koji mora da reaguje, sanira štetu i spreči sledeći talas. Potražnja za takvim timovima nikada nije bila veća, a ljudi koji to umeju nema dovoljno. Upravo tu vidim šansu za Srbiju.

Svetu su potrebni jaki i provereni igrači

Godišnji troškovi sajber kriminala na globalnom nivou premašuju desetine milijardi dolara. Da tu cifru stavim u kontekst: Da sajber kriminalci žive u jednoj državi, ona bi bila treća ekonomska sila sveta sa prihodima odmah iza SAD i Kine. To pokazuje koliko je snažna ova vrsta kriminala. Paralelno s tim,

u svetu nedostaje oko tri miliona stručnjaka za sajber bezbednost. Ne trideset hiljada. Tri miliona.

Briga o sajber bezbednosti odavno više nije izbor. Posle NIS2 direktive i novog Zakona o informacionoj bezbednosti, ona je postala zakonska obaveza. U prevodu, svaka kompanija koja ozbiljno shvata digitalni rizik traži ljude kojih jednostavno nema dovoljno.

Veštačka inteligencija je dodatno zakomplikovala sliku. Napadači je već koriste za automatizaciju i personalizaciju napada u razmerama koje pre samo nekoliko godina nisu bile moguće. Fišing mejl koji je nekada bilo lako prepoznati po nezgrapnoj gramatici danas zvuči kao da ga je napisao vaš direktor finansija, jer je AI analizirao njegovu prepisku i savršeno preuzeo njegov stil.

I to više nije daleka pretnja. Deepfake prevare su već prisutne i u Srbiji. Prevare koje kloniraju glas, pa čak i video, gde mislite da razgovarate sa poznatom osobom, a zapravo razgovarate sa njenom digitalnom kopijom kojom upravlja AI. Dovoljno je nekoliko sekundi pravog snimka da algoritam uhvati ton i boju glasa i da ga uspešno replicira u telefonskom napadu.

Odbrana mora da odgovori istom brzinom. A za to su potrebni i tehnologija i ljudi koji znaju da je primene.

Zašto baš Srbija?

Pitanje nije da li Srbija može da doprinese globalnom sajber ekosistemu. Pitanje je zašto to već ne radi u većoj meri. Imamo inženjerski kadar koji decenijama snabde-

va najveće svetske tehnološke kompanije. Imamo kvalitetno tehničko obrazovanje. Imamo IT sektor koji je rastao kroz praksu, a ne samo kroz teoriju. I imamo nešto što se teško kupuje novcem, kulturu tehničke radoznalosti i snalažljivosti koja se prenosi generacijama.

Brojke to potvrđuju. Izvoz IT usluga iz Srbije dostigao je u 2025. godini rekordnih 4,55 milijardi evra, što je deset odsto više nego godinu ranije. To je danas jedan od najbrže rastućih izvoznih sektora naše privrede i najbolji dokaz da svet već kupuje ono što ovde znamo da napravimo.

Region Centralne i Istočne Evrope sve više dolazi u fokus globalnih investitora i tehnoloških kompanija, koji ovde prepoznaju kvalitetne ljude. To nije nešto što treba uzeti zdravo za gotovo. To je prozor koji se otvara i koji se može zatvoriti jednako brzo ako propustimo trenutak.

U PULSEC-u, kao najvećoj kompaniji za sajber bezbednost u regionu, već godinama operativno dokazujemo da Srbija ima ozbiljan potencijal. Ali jedna kompanija, koliko god bila dobra, ne pravi ekosistem. Ona mu može dati podršku i pomoći da se razvije, ne i zameniti ga.

Zato već godinama organizujemo i konferenciju PULSE360, kroz koju prođe više od hiljadu učesnika. Iako je tema usko specifična, toliki odziv je jasan signal da je potreba za ovakvim mestom razmene znanja i iskustva velika. Koristim ovu priliku i da apelujem na naše obrazovne: na svim tehničkim fakultetima treba uvesti specijalizovane smerove za sajber





Datum: 23.07.2026

Medij: Profit

Rubrika: Info

Autori: redakcija

Teme: Evropska komisija

Napomena:

Površina: 1123



Naslov: Srbija na mapi globalnog sajber ekosistema

Strana: 10,11

bezbednost. Danas ih u najvećoj meri nemamo, pa se sve svodi na entuzijazam pojedinca, umesto da bude sistemski rešeno.

Talenat postoji. Sistem mora da ga podrži.

Deficit od tri miliona stručnjaka ne rešava se uvozom kadrova. Rešava se izgradnjom sistema koji neguje sopstvene ljude. U PULSEC-u smo to prepoznali kroz program CyberLab, koji obučava i razvija mlade stručnjake iz Srbije. Nije reč o kursovima koji se završavaju sertifikatom, već o konkretnom osposobljavanju za konkretne, deficitarne pozicije.

Kapital prati taj trend. Globalni investitori uložili su u 2025. godini blizu 14 milijardi dolara u sajber startape, gotovo 50 odsto više nego godinu ranije. Inovacija se sve češće dešava van velikih korporacija, u malim i agilnim timovima. Za ekosisteme koji imaju talenat, ali još nemaju kapital, to je još jedan prozor koji se otvara.

U Srbiji danas posluje skoro hiljadu aktivnih startapa. Mnogi imaju tehničku ideju, sposoban tim i stvaran problem koji pokušavaju da reše. Ono što im nedostaje nije talenat. Nedostaje im put od ideje do tržišta. Nedostaju im kontakti sa industrijskim partnerima koji bi rešenje testirali u realnom okruženju. Nedostaje im most između laboratorije i kancelarije direktora koji odlučuje o budžetu. Upravo taj raskorak pokušava da premosti HUB201, inovacioni hub za sajber bezbednost i primenu veštačke inteligencije, koji je za svega nekoliko meseci okupio više od 400 članova, među kojima su i naši inženjeri. Na prvom hakatonu u njihovoj organizaciji učestvovala su 53 tima sa 150 učesnika. To nije marketinška statistika. To je signal da u Srbiji postoji značajan broj inženjera, istraživača i mladih sa preduzetničkim duhom koji aktivno traže prostor da rade na ozbiljnim problemima.

Budimo iskreni i oko jedne stvari, trku za AI infrastrukturom nećemo dobiti onako kako je dobijaju globalni hyperscaler-i. Njihova igra su struja, voda i kapital na kontinentalnoj skali. U tu trku je i Evropa ušla kasno, a za naš region su ta vrata uglavnom zatvorena. Ali paralelno teče i druga trka, ona koju zaista možemo da dobijemo. Trka za ekspertizom. Za sajber bezbednošću. Za



Igor Pinter, direktor kompanije PULSEC

primenjenom veštačkom inteligencijom. Za poslovanjem u regulisanim industrijama. Za digitalnim suverenitetom kome se može verovati. Tu region već ima kredibilnu poziciju i tu bi ulaganje u ljude najbrže donelo rezultat.

Srbija ima realnu šansu da u narednoj deceniji postane prepoznatljiva tačka na mapi globalnog sajber ekosistema. Ali samo ako da-

nas donesemo prave izbore, ulaganje u ljude, a ne samo u infrastrukturu, partnerstva koja otvaraju tržišta, a ne samo vrata, programe koji proizvode profesionalce sa konkretnim veštinama, a ne samo sertifikate.

Talenat već imamo. Pitanje je samo hoćemo li prepoznati da imamo šta da ponudimo, pre nego što se prozor zatvori? ☹️

