Bezbednosni izazovi savremenog poslovanja

Piše: Prof. dr Miodrag Brzaković

Savremeni poslovni sistemi danas su uslovljeni da prate veoma širok spektar potencijalnih opasnosti i pretnji u odnosu na poslovanje i uspešnost organizacije.

Pored spoljnih faktora, kao što su neizvesna ekonomska situacija, na savremeno poslovanje veliki uticaj imaju i učestalost društvenih promena, problem izbora adekvatne, obrazovane radne snage, veliki broj zakonskih propisa, ali i bezbednosni rizici u poslovanju. Jedan od ključnih bezbednosnih rizika u savremenim uslovima poslovanja je i informaciona bezbednost.

Prateći efekat prihvatanja i primene interneta u skoro svim oblastima savremenog poslovanja jeste povećana ranjivost organizacija od mogućih sajber napada. Internet je postao deo kritične globalne infrastrukture. Tako se danas e-trgovina, e-bankarstvo, gotovo celo savremeno poslovanje, i globalno i lokalno, odvija na sajber platformama i internet servisima komunikacija. Isti taj sajber prostor, koji nam je omogućio brzinu, dostupnost, umreženost i trenutnu povezanost kakva je ranije bila nezamisliva, česta je meta sajber kriminala.

Kako odbraniti svoj sajber prostor od neželjenih upada i malverzacija koje u poslu dovode do gubitaka, a u privatnom prostoru do uzurpacije i zloupotrebe ličnih podataka? Sajber bezbednost se može razmotriti kroz tri kriterijuma. Prvi je vrsta akcije, i to su špijuniranje, sajber kriminal, presretanje podataka i ilegalni pristup, odnosno, ometanje i uništavanje podataka, te krađa identiteta. Drugi kriterijum je vrsta počinioca. Tu spadaju hakeri, sajber kriminalci, a poslednjih godina i sajber teroristi, odnosno grupacije koje na internetu izazivaju nemir i nanose štetu državama, remete opšti mir i stabilnost sveta. Treći kriterijum je vrsta cilja, i to mogu biti organizacije, pojedinci, državni organi, javne institucije, strateška infrastruktura.

Ni Srbija nije pošteđena bezbednosnih izazova i rizika u sajber prostoru. Uočeno je da su najčešći oblici neprikladnog delovanja na internetu kod nas: zloupotreba internet domena u svrhu lažnog predstavljanja, nepoštovanje postojećih regulativa u oblasti elektronske komunikacije, nepoštovanje zaštite privatnosti, različiti oblici zloupotreba nedovoljno opreznih korisnika interneta. Zbog specifičnosti primene savremenih tehnologija, kao i pristupa prema vrsti, počiniocima i žrtvama ovakvih napada, pitanje sajber bezbednosti zahteva posebnu brigu svih koji se bave internetom.

Uočeno je da su najčešći oblici neprikladnog delovanja na internetu kod nas: zloupotreba internet domena u svrhu lažnog predstavljanja, nepoštovanje postojećih regulativa u oblasti elektronske komunikacije, nepoštovanje zaštite privatnosti, različiti oblici zloupotreba nedovoljno opreznih korisnika interneta.

Na osnovu do sada rađenih istraživanja na ovu temu, pojedini relevantni analitičari smatraju da će popularnost društvenih mreža u budućnosti opasti upravo zbog problema rizika i već postojeće, sve češće, zloupotrebe ličnih podataka. Glavna tema mnogih grupa je prelazak na platforme koje garantuju veću privatnost.

Jedna od najugroženijih grupa danas jesu korisnici društvenih mreža. Zbog opasnosti koje prete korisnicima društvenih mreža, svako od nas trebalo bi da obrati pažnju na činjenicu da otkriva veliku količinu ličnih i poverljivih informacija. Korišćenjem društvenih mreža korisnik se svesno odriče dela svoje privatnosti, pa je važno kvalitetno oceniti da li bi ga neki podaci mogli ugroziti

Jedan od imperativa savremenog poslovanja je informaciono-bezbednosna kultura. Ona predstavlja ključ informacione bezbednosti u funkciji sprečavanja nepoželjnih događaja, i daje odgovore na najčešća pitanja: Kolika je mogućnost zloupotrebe? Koliko su naši lični podaci sigurni? Kakva je opasnost od korišćenja društvenih mreža? U koje se sve svrhe koriste naši lični podaci? Bezbednosna kultura je prevencija. A da bi se do nje došlo, mora se prepoznati nivo svesti o potencijalnim sajber rizicima, kako kod organizacija, tako i kod pojedinaca. Kod mnogih, jasna spoznaja o mogućoj ugroženosti još uvek nije na potrebnom nivou, pa podaci takvih organizacija i pojedinca ili nisu adekvatno zaštićeni, te su podložni budućoj zloupotrebi, ili su već ugroženi.

na neprihvatljiv način. Zato je, u cilju zaštite privatnosti, neophodno strogo voditi računa šta se objavljuje na društvenim mrežama. Na osnovu do sada rađenih istraživanja na ovu temu, pojedini relevantni analitičari smatraju da će popularnost društvenih mreža u budućnosti opasti upravo zbog problema rizika i već postojeće, sve češće, zloupotrebe ličnih podataka. Glavna tema mnogih grupa je prelazak na platforme koje

garantuju veću privatnost. Takođe, sve su brojniji i zahtevi za primenom preventivnih mera, sa ciljem podizanja lične i javne svesti o rizicima kojima su korisnici interneta i mobilnih društvenih mreža izloženi.

Kao jedan od odgovora na sajber rizike, u Evropskoj uniji je 25. maja 2018. godine stupila na snagu i u primeni je Opšta regulativa o zaštiti podataka o ličnosti, odnosno General Data Protection Regulation (GDPR). To je novi pravni okvir koji propisuje način korišćenja podataka o ličnosti građana EU. GDPR je stupio na snagu sa ciljem da zameni postojeće direktive koje se odnose na zaštitu podataka. Iz toga proizilazi da će svaka organizacija koja na bilo koji način obrađuje podatke građana EU morati da se pridržava novih pravila o zaštiti podataka o ličnosti, čak i ako joj je sedište izvan teritorije EU. Isto važi i za kompanije u Srbiji koje na bilo koji način obrađuju podatke građana EU. A kako je savremeni vid poslovanja vezan za aktuelne biznis modele digitalne ekonomije, neophodno je uskladiti se sa novim pravilima i kod nas. Ključni faktor za takvu aktivnost je kvalitetan IT kadar.

Na Fakultetu za primenjeni menadžment, ekonomiju i finansije – MEF i te kako se bavimo ovom temom. Studenti na našem odseku „Primenjenih informacionih tehnologija“, kao i naš fakultetski sistem, profesori i nastavni kadar u celini, polažu veliku pažnju na sva savremena dostignuća u svojim oblastima. Bezbednosni sajber rizici su, svakako, jedno od njih. Kako mi to rešavamo? Radimo ono što bismo savetovali da preduzme svaka organizacija, a to je: podizanje svesti o značaju primene mera informacione bezbednosti za održivost poslovanja, i to prvenstveno kroz edukaciju menadžmenta i zaposlenih, zatim radimo na mapiranju svih tokova podataka i usklađivanju poslovanja sa svim obavezama i regulativama, radimo kvalitetnu analizu rizika ciklično, ne zaboravljamo ni periodičnu optimizaciju sistema, a posebno smo posvećeni obezbeđivanju kvalitetnog kadra koji raspolaže odgovarajućim znanjem i kompetencijama.

Upravo prepoznajući potrebu za takvim kadrovima, koji će sutra znati da reše sve izazove sajber sveta, MEF je organizovao studijski program „Primenjene informacione tehnologije“. Tu naši mladi ljudi uče i stiču znanja i veštine iz oblasti programiranja, računarskih mreža, baza podataka, računarske grafike i simulacija, bezbednosti IS, kao i drugih srodnih oblasti, kroz samostalan i timski rad. Poseban akcenat se stavlja na razvoj analitičkog i kritičkog mišljenja koje je veoma bitno za budućeg inženjera informacionih tehnologija. Na ovaj način obezbeđuju se stručnjaci sposobni da odgovore na izazove

Radimo ono što bismo savetovali da preduzme svaka organizacija, a to je: podizanje svesti o značaju primene mera informacione bezbednosti za održivost poslovanja, i to prvenstveno kroz edukaciju menadžmenta i zaposlenih, zatim radimo na mapiranju svih tokova podataka i usklađivanju poslovanja sa svim obavezama i regulativama, radimo kvalitetnu analizu rizika ciklično, ne zaboravljamo ni periodičnu optimizaciju sistema, a posebno smo posvećeni obezbeđivanju kvalitetnog kadra koji raspolaže odgovarajućim znanjem i kompetencijama.

macione bezbednosti za održivost poslovanja, i to prvenstveno kroz edukaciju menadžmenta i zaposlenih, zatim radimo na mapiranju svih tokova podataka i usklađivanju poslovanja sa svim obavezama i regulativama, radimo kvalitetnu analizu rizika ciklično, ne zaboravljamo ni periodičnu optimizaciju sistema, a posebno smo posvećeni obezbeđivanju kvalitetnog kadra koji raspolaže odgovarajućim znanjem i kompetencijama.

različitih pristupa bezbednosti poslovanja, i proaktivno, i reaktivno. Ti mladi ljudi spremni su kad izađu sa MEF-a da vode procese optimizacije bezbednosti organa i organizacija u skladu sa njihovom veličinom, i osposobljeni su za jačanje informaciono-bezbednosne kulture, kao i primenu novih tehnologija u savremenom poslovanju.

U ovoj važnoj oblasti u kojoj će se naša budućnost odvijati Fakultet za primenjeni menadžment, ekonomiju i finansije – MEF daje svoj doprinos kroz osposobljavanje mladih ljudi, jačanje svesti o informacionoj bezbednosti, kao i kroz pomoć organizacijama i pojedincima da prihvate i primene važnost edukacije za bezbedno i uspešno poslovanje.

Prof. dr Miodrag Brzaković
Predsednik saveta
www.mef.edu.rs