DANIEL ŠUŠNJAR, PREDSEDAVAJUĆI ODBORA ZA TELEKOMUNIKACIJE I DIGITALNU EKONOMIJU U SAVETU STRANIH INVESTITORA

Sajber bezbednost treba da bude deo poslovne kulture

Pitanje bezbednosti podataka posebno je važno u situaciji kada se u okviru lanca snadbevanja ili zbog organizacije poslovnih procesa određeni poslovni podaci čine dostupnim trećoj strani. Tada se već u procesu nabavke usluga postavljaju zahtevi u pogledu čuvanja podataka u skladu sa standardima u određenoj industriji

Kakvi su novi trendovi kad je reč o proceni velikih kompanija gde investirati – kolika je uloga stepena digitalizacije i sajber bezbednosti neke države, i na koji način strani investitori mogu da utiču na pozitivne promene u toj oblasti? O tome za naše čitaoce govori Daniel Šušnjar, predsedavajući Odbora za telekomunikacije i digitalnu ekonomiju u Savetu stranih investitora.

Da li strani investitori, pre nego što odluče šta će i koliko investirati u nekoj državi, procenjuju i stepen digitalizacije u toj državi, i kakav je opšti utisak o Srbiji u tom kontekstu?

Apsolutno. Baš kao što se procenjuju uslovi poslovanja u pogledu infrastrukture, autoputeva ili dostupnosti i kvalifikacije radne snage. Razmatra se stepen digitalizacije, počevši od nivoa razvijenosti telekomunikacionih usluga, digitalnih veština i nivoa digitalne „osvešćenosti" stanovništva, preko razvijenosti inovativnih platnih usluga i uopšte pratećeg digitalnog ekosistema, pa sve do fleksibilnosti regulatornog okvira i usluga elektronske uprave koje olakšavaju poslovanje.

Značaj pojedinih kategorija zavisi od toga da li je strani investitor u Srbiji izvozno orijentisan, ili su usluge i proizvodi prvenstveno namenjeni domaćem i regionalnom tržištu. U svakom slučaju, u Savetu stranih investitora prepoznali smo da pouzdana i pravno relevantna identifikacija u digitalnom okruženju predstavlja okosnicu daljeg procesa digitalizacije u Srbiji, zajedno sa inovativnim i digitalizovanim finansijskim uslugama. Smatramo da postoji veliki potencijal u međusektorskoj saradnji telekomunikacionih operatora, banaka i osiguranja, ali, isto tako, i u partnerstvu i činjenici da se privatni sektor oslanja na dostignuća i digitalna rešenja razvijena od strane države. Primećujemo da našu ambiciju dele i druga poslovna udruženja, pa je tako Privredna komora Srbije pokrenula Centar za digitalnu transformaciju sa preduzećima različite veličine i iz različitih sektora. Ovakve i slične inicijative su i više nego dobrodošle.

Istraživanja pokazuju da su i dalje u najvišoj meri digitalizovane kompanije čija je delatnost u osnovi tehnološka, dok tradicionalne industrije poput poljoprivrede, mašinske i metalske kasne u tom procesu. Logistika i turizam, na primer, takođe su pokazali sposobnost za brzo prilagođavanje digitalnoj ekonomiji.

Ipak pandemija virusa Covid19 širom sveta naterala je na brzu reorganizaciju i digitalnu transformaciju i one kompanije koje to nisu planirale. Došlo je do promene u načinu komunikacije sa korisnicima i slično, čime se ovaj proces dodatno ubrzao. Stoga smatramo da će one kompanije koje nisu iskoristile ovaj trenutak, imati problem u poslovanju i komunikaciji sa klijentima i nakon što pandemija prođe. Mi zaista verujemo da je digitalna transfor-

macija opšta potreba i da to nije privilegija rezervisana samo za velike kompanije i sisteme.

Da li se prilikom odluke o investiranju ispituje i otpornost na sajber napade, i šta sve je tu uključeno?

Ispitivanje otpornosti na sajber napade podrazumeva nekoliko ključnih komponenti koje čine sajber bezbednost. U prvom redu, postavlja se pitanje postojanja adekvatnog regulatorno-pravnog okvira, kao i kapaciteta policije, tužilaštava i sudova da rade na suzbijanju i sankcionisanju visokotehnološkog kriminala. Sa druge strane, neophodno je da privatni sektor, zajedno sa civilnim društvom i akademskom zajednicom, uloži u stručnost i sticanje iskustva profesionalaca zaduženih za kontrolu i primenu tehničkih standarda u domenu korišćenja infrastrukture i pružanja digitalnih servisa, jer trenutno na tržištu rada postoji manjak kvalifikovanih stručnjaka iz oblasti informacione bezbednosti.

Sa manjim zakašnjenjem, Srbija uglavnom sledi regulativu Evropske unije u domenu sajber bezbednosti, a slično je i sa okvirom zaštite podataka o ličnosti. U prethodnom periodu napravljeni su značajni pomaci. U tom pravcu Usvojen je Zakon o informacionoj bezbednosti, kojim je uspostavljen bazični pravni okvir u ovoj oblasti kroz koji su implementirane odredbe Konvencije iz Budimpešte Saveta Evrope o borbi protiv sajber kriminala. U pogledu organizaciono-operativnih mehanizama, pri Ministarstvu unutrašnjih poslova uspostavljena je Služba za borbu protiv visokotehnološkog kriminala (VTK), zatim Posebno odeljenje Višeg javnog tužilaštva za borbu protiv VTK, dok je na nivou sudstva ustanovljena posebna nadležnost za VTK pri Višem sudu u Beogradu, odnosno posebno odeljenje Apelacionog suda u Beogradu kao drugostepena instanca. Takođe, pri Regulatornoj agenciji za elektronske komunikacije i poštanske usluge (RATEL) osnovan je i Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (CERT).

Naravno da je potrebno i u narednom periodu nastaviti rad na ovom polju, pa se tako očekuje operacionalizacija usvojenog Zakona o kritičnoj infrastrukturi kroz utvrđivanje kriterijuma za određivanje kritične infrastrukture u različitim oblastima, kao i preciziranje načina zaštite ove infrastrukture iz perspektive informacione bezbednosti.

Koliko strani investitori polažu na sajber bezbednost bankarskog sektora, platnog prometa u državi, snagu IT sektora, kvaliteta kompanija koje se bave sajber bezbednošću...?

Sigurnost i stabilnost bankarskog sektora i, uopšte, platnog prometa veoma je važna pri ukupnoj oceni uslova poslovanja u jednoj zemlji. S obzirom na to da dolazim iz telekomunikacionog sektora u kome je informa-

ciona bezbednost na visokom nivou, ono što mogu da primetim je da je ista situacija i u bankarskom sektoru, i da je i ovaj aspekt njihovog poslovanja pod punom kontrolom Narodne banke Srbije kao regulatora u ovoj oblasti. Što se tiče kvaliteta domaćih kompanija koje pružaju usluge iz ove oblasti, to nije jedan od ključnih kriterijuma, imajući u vidu da su pretnje na nivou informacione bezbednosti po svojoj prirodi međunarodnog karaktera. Shodno tome i rešenja koja se primenjuju za zaštitu nisu nužno vezana za države, i često su centralizovana kod kompanija koje su deo multinacionalnih grupacija.

Da li strane kompanije proveravaju sajber bezbednost stejkholdera, a posebno preduzeća sa kojima sarađuju – jer su i oni potencijalni kanal kroz koji mogu procuriti podaci iz same kompanije?

Pitanje bezbednosti podataka posebno je važno u situaciji kada se u okviru lanca snadbevanja ili zbog organizacije poslovnih procesa određeni poslovni podaci čine dostupnim trećoj strani. Tada se već u procesu nabavke usluga postavljaju zahtevi u pogledu čuvanja podataka u skladu sa standardima u određenoj industriji, na primer, postavlja se pitanje postojanja sertifikata kakav je ISO 27001/27701, zaključuju se prateći ugovori o poverljivosti i slično. Ovo posebno dolazi do značaja prilikom poveravanja podataka o ličnosti. Tada se preduzimaju posebne mere koje proizlaze iz našeg Zakona o zaštiti podataka o ličnosti, koje između ostalog podrazumevaju zaključenje sporazuma o obradi podataka, tzv. DPA sporazuma, čime se na precizan način definišu prava i obaveze obe strane.

Kada strane kompanije dolaze u Srbiju, da li traže za sebe osiguranje od sajber rizika ukoliko dođe do prekida poslovanja, i kako te polise obezbeđuju s obzirom na to da je ponuda na domaćem tržištu izuzetno slaba (samo jedna kompanija nudi te polise)?

Sa razvojem tehnologija i digitalnih poslovnih modela raste i potreba za sajber odgovornošću i to ne samo u smislu učestalosti rizika već i u smislu pratećih troškova.

Postoje dve vrste šteta kod IT osiguranja od sajber odgovornosti: direktne štete koje nastaju kao posledica sajber rizika i odražavaju se na poslovanje kompanije, dok drugu vrstu čine štete koje nastaju prema trećim licima. U prvom slučaju, cilj je da se klijentima olakšaju potencijalno veoma visoki troškovi u slučajevima povrede sopstvenih podataka. Kod osiguranja od rizika štete prema trećim licima, cilj je da se kompanije zaštite od rizika visokih odštetnih zahteva svojih klijenata čiji su podaci narušeni.

Foreign Investors Council

Čini se da je ova vrsta osiguranja u razvoju i da će u budućnosti imati veći značaj nego što je to trenutno slučaj.

Da li se od domaćih ponuđača očekuje da imaju polisu osiguranja od sajber rizika, kao uslov da bi se prijavili na tender?

Po našim saznanjima, to još nije praksa na srpskom tržištu.

Savet stranih investitora pokrenuo je krajem prošle godine inicijativu za digitalizaciju finansijskih usluga u Srbiji, i s tim u vezi Vladi Srbije predložio niz mera koje bi trebalo primeniti u funkciji ubrzanja dalje digitalizacije usluga u finansijskom sektoru. Koje predložene mere biste istakli kao najznačajnije/najurgentnije, i dokle se stiglo sa njihovom realizacijom?

Nakon nekoliko veoma uspešnih regulatornih promena tokom 2018/19. godine čime su uvedeni novi digitalni finansijski proizvodi i usluge, a imajući u vidu da je digitalizacija danas apsolutni prioritet, posebno kao posledica pandemije COVID-19 i socijalnog distanciranja, Savet je u saradnji sa svojim članovima pripremio inicijativu radi pune digitalizacije finansijskih usluga. Inicijativa sadrži 23 različita predloga, od kojih neki imaju značaj visokog prioriteta, primera radi digitalizacija menice, digitalna razmena podataka između finansijskih institucija i državnih organa, identifikacija klijenata na daljinu i dr. Sa zadovoljstvom možemo da istaknemo izvanrednu saradnju sa svim državnim organima radi realizacije inicijative, razumevanje i spremnost za implementaciju predloga. Neki od prioritetnih predloga Saveta su već u planu realizacije od strane Vlade RS i Narodne banke Srbije poput digitalne menice, prihvatanje dokaza o elektronskim transakcijama od strane javnih institucia i drugo, te ih možemo očekivati u primeni u bliskoj budućnosti. Verujemo i da je velikom broju građana u interesu da što veći broj usluga može da obavlja “iz fotelje”, pa nas posebno raduje sve veća mogućnost identifikacije klijenata na daljinu, o čemu će verujemo uskoro biti više reči u javnosti.

Da li postoji namera da se ubrza i proces unapređenja sajber bezbednosti – ako postoji, kakve mere se mogu kao predlog očekivati od Saveta stranih investitora?

Sajber bezbednost više ne može da se posmatra odvojeno od bezbednosti u realnom svetu. Šteta koja nastane kao rezultat sajber napada vrlo je realna i izaziva stvarne posledice i u fizičkom svetu. Ipak, zbog specifičnosti vezanih za tehnologiju, vrste, počinioce i žrtve ovakvih napada, pitanje sajber bezbednosti zahteva posebnu brigu svih koji se bave internetom.

Svedoci smo da ono što može da se upotrebi u korist društva, kao recimo tehnologija, može nažalost da se upotrebi i na njegovu štetu.

Kada pomenemo sajber bezbednost, obično pomislimo na neke krupnije stvari, kao što su skupi specijalizovani softveri. Često postoji nerazumevanje da povećanje budžeta za sajber bezbednost, ma koliko on bio velik, ne može da dovede do potpune sigurnosti kompanije od sajber napada, niti donosi brze rezultate.

Zato je bitno u vremenu pandemije, kada određene industrije beleže značajne gubitke, krenuti od rešenja koja ne zahtevaju velika ulaganja.

Kao što stručnjaci za bezbednost često ističu, ljudski faktor je jedan od najvećih sigurnosnih problema sa kojim se kompanije suočavaju. Stoga moramo da radimo na unapređenju sajber bezbednosti kroz edukaciju i podizanje svesti ljudi o pretnjama u sajber prostoru i merama prevencije, pogotovo prilikom rada od kuće, van kontrolisanog okruženja. Definisanje kompanijske politike u vezi sa radom od kuće u brojnim segmentima, kao što je politika upotrebe sopstvenih, privatnih, uređaja mobilnih telefona i laptopova, u odnosu na službene uređaje koji poseduju licencirani softver i antivirusne programe.

Svaka kompanija bi trebalo da razvija strategiju za zaštitu i oporavak podataka i sistema usled sajber napada. Prva 24 sata su ključna u sprečavanju gubitaka i zaštiti podataka i igraju ključnu ulogu u percepciji javnosti o brendu i njegovoj pouzdanosti. Zato je neophodno da kompanije uspostave timove za krizni menadžment i izrade planove za upravljanje kontinuitetom poslovanja i IT infrastrukturom u slučaju bezbednosnih incidenata, komunikacije, plan oporavka i reagovanje usled incidenata.

Sajber bezbednost u kompanijama ne treba da bude zadatak koji će se povremeno obavljati. Ona mora da bude utkana u poslovnu kulturu, a kompanije moraju da imaju strogo definisane politike.

Proaktivnost je ključni faktor, jer se ne sme čekati da se problem desi – tada je šteta već učinjena. Umesto toga, potrebno je učiniti sve da do nje ne dođe.