Koja je uloga akademskog sektora u informacijskoj sigurnosti?

Informacijska sigurnost

Informacijska sigurnost predstavlja multidisciplinarno područje koje čini temelje razvoja suvremenog informacijskog društva, na sličan način kao što je sigurnost temelj tradicionalnog društva i odnosa u njemu. Upravo zbog toga svi segmenti društva imaju svoju ulogu, bilo u razvoju, bilo u provedbi informacijske sigurnosti. Akademski sektor svoju ulogu oblikuje kao dio javnog sektora u smislu odgovarajuće primjene informacijske sigurnosti, ali primarna uloga akademskog sektora, kao znanstveno-stručnog potencijala države, jeste sudjelovanje u razvoju informacijske sigurnosti i profiliranje tog razvoja u nacionalnom, ali i međunarodnom okruženju.

Informacijska sigurnost proizlazi iz tradicionalnih zahtjeva zaštite tajnih podataka u državnom sektoru. Razvojem i globalizacijom društva, informacije i informacijski sustavi postali su vrijednosni potencijal ne samo državnog sektora i ne samo u uskom okviru tajnih podataka. Tako je danas u sklopu informacijske sigurnosti nužno promatrati cjelokupno društvo i informacijski prostor u cjelini, usklađujući razlike i potrebe informacijske sigurnosti u različitim sektorima društva (standardi informacijske sigurnosti državnog sektora, pojedinih gospodarskih sektora, nacionalne i međunarodne norme informacijske sigurnosti).

Suvremena paradigma „umreženog društva" ili „informacijskog društva" mora se temeljiti na uređenosti i sigurnosti kakva vlada u tradicionalnom društvu. Preventiva, istražni (forenzički) postupci, ili kazneno i prekršajno procesuiranje, moraju biti u jednakoj mjeri razvijeni kao i u tradicionalnom društvu, jer primjerice pravna država mora jednako funkcionirati i u slučaju elektroničke i fizičke usluge kupovine, kao što jednako mora funkcionirati i u slučaju elektroničke komunikacije podataka ili fizičkog transporta roba. Naravno, specifičnosti globalizacije moraju se uzeti u obzir, zbog čega je nužno razviti drugačije oblike međunarodne suradnje, jer za razliku od tradicionalnog društva, ugroze informacijskog društva ne poznaju državne granice.

Zaštita (svih) podataka

Jedan od tipičnih razloga nerazumijevanja informacijske sigurnosti jest taj da se informacijska sigurnost povezuje isključivo s tajnim podacima. Takvo viđenje je netočno, jer se informacijska sigurnost bavi informacijskim prostorom u cjelini, te uvijek postavlja u kontekst sva tri ključna sigurnosna svojstva podataka: povjerljivost, cjelovitost i raspoloživost. Tajnost je pri tome samo jedna potkategorija svojstva povjerljivosti. Cjelovitost podataka i njihova raspoloživost ciljanoj skupini korisnika, vrijedi za sve podatke pa i za one javno objavljene, jer i takvi podaci moraju imati vlasnika, ili onoga tko vodi brigu o tim podacima u ime vlasnika. Svojstvo povjerljivosti danas se promatra u širokom opsegu pojavnosti, od tajnosti (državne, poslovne ili profesionalne

tajne), do privatnosti u smislu fizičkih osoba (osobni podaci) ili pravnih osoba (službeni ili interni podaci).

Zakonski okvir informacijske sigurnosti u Republici Hrvatskoj

Zakon o sigurnosnim službama prvi puta je 2002. godine u RH uveo pojam informacijske sigurnosti na nacionalnoj razini, ali primarno u uskom kontekstu NATO-a i u određenoj koliziji s važećim, iako uvelike zastarjelim, Zakonom o zaštiti tajnosti podataka iz 1996 godine. Koncept tajnosti podataka, propisan ovim Zakonom 1996. godine, potpuno je neusklađen sa suvremenim standardima razvijenih zemalja svijeta.

Nacionalni program informacijske sigurnosti u RH (NPIS) iz 2005. godine (www.e-hrvatska.hr) izrađen je s ciljem kako bi se proanalizirao širi kontekst bitan za uvođenje informacijske sigurnosti u RH. Informacijska sigurnost se tako, s jedne strane, postavlja kao integralni dio sustava nacionalne sigurnosti, a s druge strane kao temelj razvoja suvremenog umreženog društva. Izmjene spomenuta dva zakona, početni su korak koji treba omogućiti donošenje Zakona o informacijskoj sigurnosti. Spomenuti zakoni čine paket zakona vezan za područje nacionalne sigurnosti, nalaze se u službenoj proceduri i njihovo donošenje očekuje se u drugoj polovini 2006. godine.

Suvremeni demokratski standardi doveli su u prošlom desetljeću do visokih zahtjeva za zaštitom osobnih podataka, u okviru čega je i RH, prateći ove standarde, donijela Zakon o zaštiti osobnih podataka te Uredbu o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka. Zaštita osobnih podataka, na ovaj način propisana, obvezuje sve fizičke i pravne osobe (dakle i privatni i državni, odnosno javni sektor) pa se ova kategorija osobnih podataka ne apostrofira posebno u Zakonu o informacijskoj sigurnosti, već spada u širu državnu kategoriju neklasificiranih podataka u čijoj osnovi je privatnost kao svojstvo povjerljivosti podataka.

Zakon o informacijskoj sigurnosti

Tijela javne vlasti u današnje vrijeme nije moguće promatrati izvan šireg društvenog konteksta, jer se i koncepti e-Governmenta i informacijskog društva odnose na društvo u cjelini. U tom smislu Zakon o informacijskoj sigurnosti (ZoIS) pruža temelje za koordinaciju nacionalnog normizacijskog procesa u području informacijske sigurnosti, kao i za poticanje primjene relevantnih međunarodnih normi. Procesima nacionalne normizacije i poticanja primjene normi informacijske sigurnosti u različitim gospodarskim sektorima, ali i javnim institucijama, te procesima javno-privatnog partnerstva u području informacijske sigurnosti, stvara se dobrobit za najširu društvenu zajednicu (državni i privatni sektor te građanstvo u cjelini).

U cjelokupnom kontekstu važno je napomenuti i telekomunikacijski regulativni

okvir propisan Zakonom o telekomunikacijama i njegovim podzakonskim aktima, čime je uređen segment javnih telekomunikacijskih mreža i usluga na kojem se temelji čitav niz informacijsko-komunikacijskih sustava državnog i privatnog sektora. Utjecaj sustavno uređenog regulativnog okvira informacijske sigurnosti u tijelima javne vlasti neminovno će vremenom utjecati na uvođenje dodatnih pravila za telekomunikacijske operatore, mrežne operatore i davatelje usluga, odnosno na uvođenje nekih „mainstream" mjera informacijske sigurnosti u telekomunikacijski regulativni okvir.

Upravo u ovom širokom društvenom kontekstu trebalo bi promatrati institucionalni okvir ZoIS-a, odnosno stvaranje ili reformiranje nadležnih tijela informacijske sigurnosti. Tako ZoIS postavlja Ured Vijeća nacionalne sigurnosti kao vršno koordinacijsko tijelo RH u području informacijske sigurnosti, Zavod za sigurnost informacijskih sustava - ZSIS (prije Zavod za informacijsku sigurnost i kripto-zaštitnu tehniku) kao specijalizirano tehničko koordinacijsko tijelo u području informacijske sigurnosti, te stvara pretpostavke za ustroj nacionalnog CERT-a u CARNetu, na temeljima i iskustvu dosadašnjeg akademskog CERT-a. Dobrom koordinacijom ova tri tijela, te još nekih tijela u segmentu implementacije i nadzora informacijske sigurnosti, svi opisani procesi trebali bi se moći realizirati u RH tijekom četverogodišnjeg perioda predviđenog NPIS-om.

Izazovi informacijske sigurnosti za akademsku zajednicu

Akademski sektor, kao dio javnog sektora, ne koristi klasificirane podatke u svom redovnom radu te stoga u redovnom radu i ne primjenjuje posebne mjere i standarde informacijske sigurnosti namijenjene zaštiti klasificiranih (tajnih) podataka. Akademski sektor, kao i širi skup tijela javne vlasti, koristi u svom radu osobne podatke (zaposlenika ili građana), a pored toga u dijelu tijela javne vlasti koriste se i podaci koji će po novoj državnoj kategorizaciji pripadati neklasificiranim podacima (službeni ili interni). Općenito rečeno, neklasificirane mreže i informacijski sustavi obrađuju, pohranjuju ili prenose neklasificirane podatke sa zahtjevima cjelovitosti i dostupnosti, dok se povjerljivost takvih podataka tretira na razini privatnosti (osobni podaci fizičkih osoba ili interni podaci pravnih osoba koji nisu namijenjeni javnosti već određenim poslovnim procesima). Drugim riječima, zahtjevi koji se postavljaju na zaštitu osobnih podataka kroz Zakon o zaštiti osobnih podataka i oni koji će se postavljati na neklasificirane mreže i informacijske sustave kroz ZoIS, u osnovi su vrlo slični i međusobno sukladni, iako je pojam neklasificiranih podataka širi od osobnih pa su u tom smislu i zaštitne mjere koje se primjenjuju u državnom sektoru uobičajeno nešto kompleksnije.

Javno djelovanje akademskog sektora, ali i državne uprave u cjelini, nameće nužnost odgovarajućeg povezivanja privatnih i javnih mreža i informacijskih sustava. Upravo zbog nužnosti doticaja javnih i privatnih mreža te javnih i privatnih podataka, uobičajena je „mekša" regulacija područja informacijske sigurnosti neklasificirane domene, u odnosu na klasificiranu domenu podataka kod koje po definiciji nema doticaja javnosti. Naravno, to dovodi do velikih

razlika u konceptu povjerenja u tim sigurnosnim domenama i zabrane međusobnog povezivanja mreža i informacijskih sustava iz klasificirane i neklasificirane domene („air gap"). Međunarodna normizacija pruža danas dobro rješenje za neklasificirano područje standardima ISO/IEC 17799 i 27001, odnosno paletom standarda informacijske sigurnosti koji će se dalje nadograđivati na ova dva. Pristup koji razvijene zemlje provode u ovom području (npr. UK, Njemačka), ali i institucije EU, ide za tim da se koriste međunarodni standardi jer u velikoj mjeri olakšavaju uspostavu međusobnog povjerenja kod interkonekcije mreža i informacijskih sustava, bilo u nacionalnim ili u međunarodnim okvirima, jer su i jedni i drugi nužnost suvremenog društva. Uobičajeno je također da nadležno državno tijelo za sigurnosnu akreditaciju mreža i sustava, zajedno s drugim nacionalnim tijelima nadležnim za informacijsku sigurnost, izdaje dodatne preporuke i smjernice za provedbu međunarodnih normi u području tijela javne vlasti (primjerice u Njemačkoj www.bsi.bund.de). Za očekivati je da i RH, razradom podzakonskih akata ZoIS-a, preuzme ovakav smjer razvoja, jer je on, između ostalog, dio standarda koje RH treba usvojiti u okviru pristupa u EU i NATO.

Iz rečenog je razvidno da je upravo segment zaštite osobnih podataka najrelevantniji u okviru primjene informacijske sigurnosti u akademskom sektoru. No, zaštitu digniteta pojedinca (svakoga od nas) nikako ne smijemo zanemarivati, jer je ona u kontekstu razvoja informacijskog društva u stvari najvažniji dio prakse koju treba razvijati. Važno je napomenuti da je zanemarivanje ove prakse u akademskom sektoru razvijenih zemalja svijeta, već dovelo do slučajeva masovnih krađa „zaboravljenih" baza s osobnim podacima građana, jer je jedan od čestih znanstvenih procesa statistička obrada različitih masovnih podataka u kojima su sadržani određeni osobni podaci građana. Nadalje, tu su arhive studenata, kao jedne od masovnih kategorija stanovništva svake zemlje, i to sve traži ozbiljan i sustavan pristup informacijskoj sigurnosti.

U području certifikata spomenutog standarda ISO/IEC 27001, potrebno je razlikovati dvije vrste procesa koji će se događati. S jedne strane, radi se o potrebi obučavanja (certificiranja) stručnih kadrova za tzv. interne auditore (provjeravatelje standarda), za što je ZoIS predvidio model koordinatora informacijske sigurnosti koji će se morati odrediti u tijelima javne vlasti. Ovakav model uobičajen je u EU i s pozicije državne uprave koristi se u nešto širem kontekstu od spomenutog standarda. Razlog tome je da ovisno o nacionalnoj politici informacijske sigurnosti, ciljevi i dosezi informacijske sigurnosti u pojedinim skupinama tijela javne vlasti mogu biti različito postavljeni, a samim tim i uloga ovih koordinatora može biti šira od okvira standarda. S druge strane radi se o potrebi prilagodbe (certificiranja) poslovnih procesa i informacijskih sustava tijela javne vlasti (ili akademske institucije) prema standardu ISO/IEC 27001. U ovom dijelu ZoIS je predvidio model sigurnosne akreditacije sustava koji će provoditi ZSIS, u suradnji s Hrvatskom akreditacijskom agencijom, odnosno ovlaštenim pravnim osobama za poslove certificiranja ovog standarda. I ovdje je potrebno napomenuti da proces sigurnosnog akreditiranja iz ZoIS-a može biti šire postavljen od certificiranja standarda ISO/IEC 27001, iz prethodno pojašnjenih razloga.

Područje osobnih podataka, kao što je rečeno, u potpunosti je regulirano u RH i kao takvo obvezujuće za sve pravne i fizičke osobe u RH. Regulativni okvir informacijske sigurnosti, kakav je opisan u tekstu, tek treba stvarati i to se očekuje u periodu idućih nekoliko godina. No, kako je pojašnjeno u tekstu zahtjevi informacijske sigurnosti bi trebali biti sukladni pa u tom smislu Zakon o zaštiti osobnih podataka i Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka, pružaju dobru podlogu za početak rada u području informacijske sigurnosti već danas.

Pored opisanog participiranja akademskog sektora u primjeni informacijske sigurnosti, bitno je istaknuti stratešku ulogu akademskog sektora u razvoju informacijske sigurnosti i profiliranju tog razvoja u nacionalnom, ali i međunarodnom okruženju. Takva uloga trebala bi počivati na prilagodbi postojećih visokoškolskih obrazovnih programa, prvenstveno u području informacijskih tehnologija i znanosti, ali isto tako i u pravnim znanostima i menadžmentu. Promjena pristupa trebala bi se rukovoditi izazovima i zahtjevima koje pred nas stavlja izgradnja „kulture sigurnosti", što je moto suvremenog svijeta, kojemu kao zemlja težimo. Zanimljivo je spomenuti da je na jednoj od najvećih specijaliziranih kongresno-izložbenih manifestacija u području informacijske sigurnosti - Infosecurity Europe 2006, održanoj u Londonu u travnju ove godine, bilo prisutno gotovo desetak britanskih sveučilišta s ponudom specijaliziranih poslijediplomskih studija iz područja informacijske sigurnosti.

Praktični značaj informacijske sigurnosti za IT struku

Informacijska sigurnost na niz načina pozitivno utječe na radne procese i stručne kadrove u IT području. Na određeni način uvodi se „red, rad i disciplina". Pojednostavljeno rečeno: „Red" se odnosi na organizacijske zahtjeve, odnosno na realno predviđen i stvarno popunjen broj IT djelatnika odgovarajućeg profila, te kvalitetne i ujednačene radno-pravne uvjete; „Rad" se odnosi na zahtjeve, ali i uvjete za stalno praćenje struke i cjeloživotno obrazovanje; „Disciplina" se odnosi na sve zaposlenike u određenoj instituciji i uobičajeno se provodi dokumentom koji donosi uprava institucije i koji se naziva „politika" te se donosi za različite aspekte poslovnog ili tehnološkog okruženja.

Zašto je ovo važno? U praksi, osobito u državnim službama, ali često i puno šire, djelatnost IT-a, koja se vrlo brzo razvija u tehnološkom segmentu, a naročito po broju korisnika, stagnira u strukovnom segmentu, gdje broj i uvjeti IT osoblja gotovo ničim ne prate ovaj trend brzog razvoja. Na potpuno nerazumljiv način, upravljački segmenti organizacija pretpostavljaju da primjerice „IT osoblje koje je održavalo prvih stotinu računala solidno informatički obrazovanih korisnika, može i današnjih tisuću ili više korisnika koje ćemo sami obrazovati u hodu", naravno uz nepromijenjeni brojčani i radno-pravni status IT osoblja. Tzv. „outsourcing" obično predstavlja dugo traženo organizacijsko rješenje, koje, najčešće nedefiniranim parametrima i

kriterijima nabave, održavanja, poslovnog odnosa i svega drugog, samo dodatno produbljuje opisani početni problem.

Informacijska sigurnost ne nudi „instant rješenja" ovih problema, ali zahtjeva uređenost poslovnih procesa i cjeloživotni proces praćenja i upravljanja svim bitnim segmentima jedne organizacije pa i IT infrastrukturom. To uključuje puno drugačiju brigu o ovim opisanim aspektima IT prakse u RH, ali i puno više od toga, osobito u segmentu odgovornosti onih koji upravljaju organizacijom.