Avtor: izr. prof. dr. Denis Čaleta / Institut za korporativne varnostne študije

INTERVJU
mag. Mojca Kunšek, direktorica Agencije Republike Slovenije za javnopravne evidence in storitve (AJPES)*

INFORMACIJSKA VARNOST JE KLJUČNEGA POMENA ZA PREDVIDLJIVOST IN TOČNOST PODATKOV

Moderna informacijska družba zahteva nove pristope tudi na področju upravljanja z javnimi evidencami podatkov, ki morajo biti dostopni različnim ciljnim uporabnikom v Republiki Sloveniji. O izzivih, ki se pojavljajo pri zagotavljanju varnosti in točnosti javnih podatkov, smo se pogovarjali z gospo Mojco Kunšek.

Spoštovana vodite izredno pomembno Agencijo Republike Slovenije za javnopravne evidence in storitve. Prosimo, če nam lahko na kratko opredelite glavna težišča vaših pristojnosti.

AJPES je osrednja nacionalna institucija na področju registracije poslovnih subjektov ter zbiranja, objavljanja in posredovanja podatkov in informacij za zagotavljanje preglednega nacionalnega in evropskega poslovnega okolja. Tako je AJPES tudi aktivno vključen v izvajanje številnih predpisov in sodeluje s številnimi resorno pristojnimi ministrstvi in drugimi državnimi organi. V okviru izvajanja nalog točk SPOT, na dvanajstih lokacijah po Sloveniji, je AJPES osrednja informativna in vstopna točka za registriranje gospodarskih subjektov, saj registrira preko 50 % vseh poslovnih subjektov v državi in je odgovoren za registracijo s.p.. Ena osrednjih nalog je tudi upravljanje Poslovnega registra Slovenije, ki se povezuje v mrežo evropskih poslovnih registrov, tako preko interesne platforme EBR, kot tudi preko platforme e-justice pri Evropski komisiji. Pristojnosti AJPES zajemajo tudi upravljanje informacijskega sistema sodnega registra, zagotavljanje rešitev, preko katerih poslovni subjekti in sodišča objavljajo podatke in dokumente na spletnem portalu AJPES, zbiranje in javna objava letnih poročil družb in podjetnikov, ter vodenje prekrškovnih postopkov ob opustitvi predložitve. AJPES je zadolžen tudi za zbiranje vrste drugih informacij in vodenje drugih registrov, ki povečujejo varnost v pravnem prometu poslovnih subjektov ali na drug način pripomorejo k preglednemu poslovnemu okolju, ter hkrati omogočajo učinkovito poslovanje poslovnih subjektov in institucij javne uprave. Tržne storitve AJPES obsegajo zlasti izdelavo bonitetnih informacij, izvajanje večstranskega pobota medsebojnih obveznosti poslovnih subjektov in zagotavljanje podjetniško usmerjenih orodij in informacij.

V AJPES si prizadevamo narediti največ, kar je trenutno glede na razmere mogoče, da zagotavljamo varnost in neprekinjenost poslovanja za izvajanje poslovnih procesov javne službe.

Ključni del vašega delovanja zajema predvidljivost in točnost podatkov, ki jih zagotavljate za različni se-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

gment končnih uporabnikov. Kako vplivajo vedno močnejši procesi digitalizacije in informatizacije na vašo organizacijo?

AJPES je digitalno dokaj napredna institucija. Krajevno pristojnost izpostav smo namreč odpravili že pred 10 leti, s čemer poslovne primere, ne glede na lokalni izvor, lahko rešuje katerakoli izmed izpostav v 12 regijah. Prav tako omogočamo uporabnikom dostopnost do podatkov preko 10 spletnih servisov ter zagotavljamo pravno varnost s predhodnim preverjanjem potencialnih podjetnikov z interoperabilnostjo spletnih mest v državi (FURS, MNZ, IRSD, MRVL). Prav tako tudi sledimo tehnologijam in trendom digitalizacije in informatizacije ter skušamo zagotoviti ustrezna investicijska sredstva za stabilno informacijsko infrastrukturo in informacijske sisteme ter izvedbe projektov državnega pomena s pogodbenimi partnerji.

Kako močno na to področje vplivajo spremembe, ki se dogajajo na področju evropskih in posledično nacionalnih podlag za varovanje osebnih podatkov?

Pri AJPES se pomena varovanja osebnih podatkov zavedamo še iz časov pred Splošno uredbo o varstvu podatkov (v nadaljevanju GDPR), zato z njenim sprejemom ni bilo posebnih presenečenj. Seveda smo morali imenovati pooblaščeno osebo za varstvo osebnih podatkov, ki je pri nas zunanja, in prilagoditi katerega izmed procesov; kljub temu pa tu do sedaj ni bilo kakih večjih pretresov. Več izzivov smo imeli z nacionalno zakonodajo npr. z zadnjo spremembo Zakona o gospodarskih družbah (ZGD-1), saj smo zaradi zavezujoče objave e-poštnih naslovov pravnih subjektov, med katerimi so tudi naslovi posameznikov, zaznali več nejevolje med našimi podjetji in samostojnimi podjetniki, pa še to predvsem zaradi povečane količine neželene e-pošte. Ob sprejemu GDPR smo na tržnem delu dejavnosti AJPES vpeljali nove rešitve za področje neposrednega trženja storitev, na javnem delu pa uredili ustrezne pravne podlage ter prilagodili procesno dokumentacijo za zagotavljanje zakonite obdelave osebnih podatkov, ki jih ima AJPES v upravljanju. Prilagoditev poslovanja v skladu z zahtevanimi standardi in normativno regulacijo z GDPR je nedvomno pomenila določene spremembe v poslovnih procesih, v katerih se podatki obdelujejo, saj smo jih morali prilagoditi tako iz tehničnega kot tudi iz procesnega vidika.

Z uvajanjem novih tehnologij je tesno povezano tudi spreminjanje organizacijske kulture organizacije. Kako uspete zagotavljati to transformacijo pri zaposlenih v Agenciji?

V AJPES zagovarjamo načelo vseživljenjskega učenja, saj le strokovno dovolj kompetentni zaposleni lahko suvereno izvajajo storitve. Koncept vseživljenjskega učenja širimo ne le na vsebinska področja, temveč tudi v zagotavljanje ustreznega nivoja digitalnih kompetenc ob vsesplošnem zagotavljanju varnosti. Visok nivo digitalnih kompetenc, zavzemanje za neprekinjeno poslovanje in povezanost med zaposlenimi, ne glede na mesto opravljanja dela, pa je bila tudi ena ključnih prednosti pri hitrem prehodu na delo od doma tudi ob pojavu epidemije v marcu 2020, tako da so lahko nadaljevali z enakim tempom in obsegom dela na daljavo z uporabo sodobnih komunikacijskih naprav kot v času pred epidemijo.

Čeprav se AJPES srečuje tudi s kadrovskimi izzivi, kot je težje nadomeščanje odhodov v pokoj kot tudi pridobivanje kadrov, pa skuša novo zaposlene sodelavce z mentorskim pristopom čim prej usposobiti za samostojno opravljanje dela ob poznavanju konteksta delovanja agencije. Ob omejenih mož-

nostih nagrajevanja zaposlenih v javnem sektorju pa skuša vendarle prepoznavati tudi najboljše kadre. Svoje zavzemanje za dobro organizacijsko energijo pa AJPES izkazuje tudi s prejemom certifikata v okviru projekta Nacionalno merjenje organizacijske energije v letih 2021 in 2022.

Novi varnostni izzivi med katerimi so najbolj izpostavljena ravno kibernetska tveganja vplivajo na delovanje vseh organizacij. Verjetno se tem izzivom težko izogibate tudi pri delovanju vaše organizacije. Kako pomembno mesto namenjate razvoju tega področja?

Skladno s strateško usmeritvijo AJPES – nuditi napredne informacijske rešitve z visoko stopnjo razpoložljivosti – je kot strateški cilj AJPES opredeljeno tudi zagotavljanje varnosti, zaupnosti, celovitosti in razpoložljivosti informacijskega sistema ter zagotavljanje neprekinjenega delovanja ključnih poslovnih procesov v primeru izrednih dogodkov. Na področju informacijske varnosti AJPES sledi strateškim usmeritvam države, Nacionalni strategiji kibernetske varnosti in usklajuje svoje delovanje z Zakonom o informacijski varnosti in Uredbo o informacijski varnosti v državni upravi. Prav tako pa AJPES zaradi globalne situacije na področju kibernetske varnosti izvaja tudi priporočila pristojnih institucij za izvedbo ukrepov za zagotovitev visoke stopnje varnosti omrežij in informacijskih sistemov, za kar ima oblikovano tudi posebno delovno skupino za zagotavljanje ustreznih varnostnih politik ter obravnavo morebitnih varnostnih incidentov, v katerih delujejo vsi ključni deležniki, od pravne službe, preko IT, informacijske varnosti in neprekinjenega poslovanja, do pooblaščene osebe za varstvo osebnih podatkov, ki poročajo direktno meni oz. moji namestnici.

Prav tako pa se izvajajo tudi kontinuirana izobraževanja, ki združujejo tako kibernetska tveganja, varovanje informacij, varstvo osebnih podatkov, kot tudi s področja neprekinjenega poslovanja. Zavedamo se namreč, da je kibernetska tveganja mogoče zmanjšati samo s celostnim pristopom.

Dodatno izobraževanje in usposabljanje je verjetno postala stalnica modernega organizacijskega delovanja. Ali vašim zaposlenim namenjate tudi izobraževanja in usposabljanja iz varnostnih vsebin, ki so pomembna za dvigovanje varnostnega zavedanja?

AJPES za zaposlene obdobno organizira tudi izobraževanja in usposabljanja iz varnostnih vsebin, predvsem s ciljem ustreznega informiranja ter pravočasnega zaznavanja in prepoznavanja morebitnih varnostnih groženj. V AJPES se zavedamo, da je pomembne cilje mogoče izvajati le s kompetentnimi in predvsem motivirani kadri v zdravem delovnem okolju. Zato si AJPES prizadeva za stalno in redno strokovno usposabljanje in izpopolnjevanje zaposlenih, pravočasno in učinkovito vključevanje novih nalog v poslovne procese in izboljševanje kakovosti izvajanja storitev. Prav tako AJPES spodbuja tudi redni interni prenos znanja, veščin, vrednot in primerov dobrih praks med zaposlenimi tudi preko internega sistema e-izobraževanj, ki jih pripravljajo zaposleni. Izboljšanje varnostnega zavedanja pa izboljšuje tudi z rednim testiranjem odziva zaposlenih za primere različnih varnostnih incidentov v različnih organizacijskih enotah, ki se izvaja enkrat letno. V kratkem pripravljamo še preverjanje, pri katerem bomo način izvedbe usmerili predvsem v zaznavanje ribarjenja (phishinga). Zavedamo se, da je tako preverjanje za naše zaposlene lahko stres, zato gledamo dolgoročno in se predvsem trudimo poudarjati dobre odzive.

Kje kot strateška voditeljica javne organizacije vidite glavne varnostne izzive za nemoteno delovanje zakonitega, strokovnega, preglednega in družbeno odgovornega poslovanja vaše organizacije?

V AJPES si prizadevamo narediti največ, kar je trenutno glede na razmere mogoče, da zagotavljamo varnost in neprekinjenost poslovanja za izvajanje poslovnih procesov javne službe. V AJPES imamo vzpostavljen register tveganja, da zagotavljamo obvladljivost prepoznavnih dejavnikov tveganja v organi-

zaciji. Kot strateška voditeljica javne organizacije menim, da je za obvladovanje varnostnih izzivov nujno nadaljevanje digitalne transformacije v organizaciji s stalnim izobraževanjem in informiranjem zaposlenih, rednim prenosom znanja, usposabljanjem naslednikov ter predvsem s skrbnim in rednim posodabljanjem informacijske infrastrukture. Pri vzdrževanju varnostnih procesov AJPES aktivno sodeluje z zunanjimi strokovnjaki na področju zagotavljanja kibernetske varnosti in sledi novim praksam na tem področju.

Z dvigovanjem varnostnih standardov včasih trčimo na drugi strani v željo po čim hitrejšem in čim lažjem dostopu do določenih javnih podatkov. Imate kakšne izkušnje z odzivom vaših uporabnikov, ker bi jih določeni dodatni varnostni koraki motili pri dostopanju do teh evidenc?

Ugotavljamo, da se najdejo uporabniki, ki jim je nadležno dostopanje do javnih podatkov za kakršnim koli t.i. „zidom". Marsikdo bi najraje videl, da je vse javno objavljeno dostopno brez registracije oz. prijave. Menimo, da je najmanj problematičen (ter najmanj nadležen) dostop s predhodno registracijo oz. prijavo uporabnika. Dostopa s KDP (kvalificiranim digitalnim potrdilom, certifikatom) ali z uporabo državne centralne storitve SI-PASS pa za uporabnike predstavljata več nevšečnosti. Dostop s SI-PASS je kar kompliciran za povprečnega uporabnika, vendar je prednost, da tak dostop lahko uporabnik kreira sam. Dostop s KDP pa povzroča nevšečnosti predvsem takrat, ko mora certifikat uporabnik pridobiti na ustrezen način (SIGEN-CA traja vsaj 10 dni, Halcom in drugi pa so tudi plačljivi). Občasno, npr. ob zadnjih zakonskih spremembah z obveznostjo e-naslovov pa smo naleteli tudi na negativni odziv zgolj z vidika realiziranja zakonskih zahtev, ki včasih uporabnikom niso logične in svoje nezadovoljstvo žal usmerijo na tehnične rešitve pri AJPES.

Vaša organizacija ima vzpostavljen in vpeljan standard kakovosti ISO 9001. Ste mogoče razmišljali tudi o kakšnem koraku uvajanja standarda ISO 27001 na področju informacijske varnosti?

AJPES uporablja dobre prakse standardov iz družine ISO/IEC 27001, prav tako pa ima AJPES že vzpostavljen sistem obravnave neprekinjenega poslovanja. Razmišljamo pa tudi o uvedbi ISO 27001, saj smo omejeni s kadrovskimi viri, predvsem na področju zagotavljanja primerno izurjenega osebja.

Slovensko združenje za korporativno varnost je primer dobre prakse sodelovanja državnih, javnih in gospodarskih institucij. Lahko v prihodnosti pričakujemo, da se boste tesneje povezali z delovanjem omenjenega združenja in tako skozi to pomembno mrežo zagotavljali izmenjavo dobrih praks, izkušenj in novih spoznanj na področju varnosti?

AJPES se zavzema za izmenjavo poslovnih praks in opolnomočenje vseh vrst uporabnikov, saj le-to prinaša enostavnejšo in varnejšo uporabo portala in podatkov. Nedvomno lahko rečemo, da smo sodelovanju naklonjeni, glede na naše zmožnosti pa bo potem odvisno v kolikšni meri ga bomo lahko tudi izvedli. ■