Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Telefon: + 386 (0) 1 230 97 30
Faks: + 386 (0) 1 230 97 78
www.ip-rs.si

Številka: 0612-73/2009
Datum: 22. 9. 2009

Informacijski pooblaščenec po državnem nadzorniku za varstvo osebnih podatkov Andreju Tomšiču izdaja na podlagi 2. in 8. člena Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 –ZUstS-A), 54. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1) in 32. člena Zakona o inšpekcijskem nadzoru (Ur. l. RS, št. 43/07, v nadaljevanju ZIN) v zadevi inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 pri zavezancu ****** (v nadaljevanju zavezanec), ki ga zastopa ****** po uradni dolžnosti naslednjo

ODLOČBO

Zavezancu ****** se odreja, da:

I. **v roku 60 dni** od vročitve te odločbe za zagotovitev poštenosti in zakonitosti obdelave osebnih podatkov, ki se obdelujejo pri uporabi opreme za varovanje omrežja zavezanca, **sprejme in začne izvajati varnostno politiko za varovanje internega omrežja zavezanca**; varnostna politika mora med drugim vsebovati:

- omejitve uporabe omrežja zavezanca;
- popis mehanizmov, ki se izvajajo za varovanje in stabilnost delovanja omrežja z navedbo protokolov in storitev, ki se pregledujejo;
- obrazložitev postopkov, ki se izvajajo za filtriranje ali pregledovanje prometa,
- režim nadgradenj opreme za varovanje internega omrežja zavezanca,
- postopke in ukrepe za nadzor fizičnega in logičnega dostopa do sistemskega prostora in opreme.

II. Z vsebino varnostne politike za varovanje internega omrežja zavezanca mora zavezanec v delu, ki se nanaša na 1., 2. in 3. alinejo točke I., **v roku 3 dni od izvršitve ukrepa iz točke I.**, obvestiti vse uporabnike internega omrežja zavezanca in pogodbene obdelovalce, ki vzdržujejo opremo za varovanje internega omrežja zavezanca.

III. **v roku 60 dni** od vročitve te odločbe z vzdrževalcem požarne pregrade…., ki deluje v internem omrežju zavezanca, sklene pogodbo, ki bo skladna z določbami 11. člena ZVOP-1, ali pa sam prevzame vzdrževanje požarne pregrade.

IV. O izvršitvi ukrepov iz I., II. in III. točke izreka te odločbe je zavezanec dolžan takoj pisno obvestiti državnega nadzornika za varstvo osebnih podatkov.

V. Posebni stroški v postopku niso zaznamovani.

O b r a z l o ž i t e v

1. Postopek inšpekcijskega nadzora

Informacijski pooblaščenec (v nadaljevanju Pooblaščenec) je dne 15. 5. 2009 prejel prijavo zaradi suma kršitve določb ZVOP-1. Prijavitelj je 7. 5. 2009 ugotovil, da mu pri povezovanju na poštne strežnike prek SSL šifriranega IMAP protokola skuša nekdo podtakniti lažen certifikat, ko želi do poštnih strežnikov dostopati znotraj omrežja zavezanca. Pri dostopanju od doma na te težave ni naletel. Prijavitelj se je obrnil na SI-CERT in bil z njihove strani obveščen, da do nepravilnosti v omrežju prihaja zaradi delovanja požarnega zidu, ki omogoča t.i. Deep Packet Inspection (DPI) omrežnega prometa. Glede na obvestilo SI-CERT-a naj bi omenjeni požarni zid z DPI zmožnostmi pregledoval tudi promet na SSL in TLS povezavah. Po obvestilu SI-CERT naj bi se omenjeni požarni zid fizično nahajal na……., vendar je pod nadzorom ……..oziroma njihovega pogodbenega izvajalca ……..Prijavitelj je o navedenem dogajanju dne 8. 5. 2009 po elektronski pošti obvestil vodjo Računalniškega centra Fakultete ****** ter istega dne tudi Računalniški center Univerze ******. Prijavitelj je dne 14. 5. 2009 prejel pojasnilo podjetja ….. Po pojasnilih podjetja …… pogodbenega obdelovalca zavezanca, gre za funkcionalnost fakultetne požarne pregrade ……ki je bila …….nadgrajena na najnovejšo verzijo programske opreme. Ta verzija ima privzeto vklopljeno tudi antivirusno in antispam pregledovanje za……. Pregledovanje kriptiranih protokolov …….naprava izvaja tako, da se uporabniku predstavlja s svojim certifikatom, in na ta način preveri vsebino kriptirane povezave za morebitne viruse, spyware in ostalo škodljivo programsko kodo. Pogodbeni obdelovalec zavezanca je še pojasnil, da ne gre za prestrezanje sporočil z namenom kršenja zasebnosti uporabnikov, temveč za zagotavljanje varnosti omrežja in njegovih uporabnikov ter da funkcionalnost pregledovanja poštnega in spletnega prometa ponujajo vse t.i. UTM (Unified Threat Management) naprava, med katere sodi tudi konkretna požarna pregrada. Pogodbeni obdelovalec je zavezancu predlagal, da se uporabnikom omrežja zavezanca predstavi, katere omejitve veljajo v omrežju zavezanca in kateri mehanizmi se izvajajo za zaščito in stabilno delovanje. V kolikor se uporabniki ne strinjajo s temi omejitvami, naj bi uporabljali npr. EDUROAM omrežje, kjer teh omejitev ni.

Državni nadzornik je v postopku inšpekcijskega nadzora izvedel inšpekcijski ogled dne 29. 5. 2009 na Računalniškem centru Univerze ******, ob katerem je bil sestavljen zapisnik št. 0612-73/2009/3. Ugotovljeno je bilo, da glede informacijske varnosti upoštevajo priporočila ARNESA, sicer pa je dokumentiranost varnostnih politik po 26 članicah Univerze ****** zelo različna. Za varnost lastnih omrežij skrbijo članice same. Podrobnejše informacije o omrežju ****** so razvidne iz Priporočila ****** iz julija 2007. Enotne varnostne politike na ravni univerze ni, ker naj bi bilo usklajevanje s ** članicami zelo težavno. Potrebno je upoštevati

dvojno pravno subjektiviteto članic ******, ki deloma nastopajo kot del pravne osebe ******, deloma pa kot ločeni pravni subjekti, sama meja pa ni vedno jasna. Kot izhaja iz omenjenega zapisnika naj bi pogosto prihajalo do trenj med težnjami po večji varnosti v smislu enovitega pristopa in želja članic po avtonomnosti. Ugotovljeno je bilo, da so v letu 2008 na Računalniškem centru Univerze ****** kupili 6 požarnih pregrad…….., ena od njih se uporablja pri zavezancu. Politike in nastavitve požarnih pregrad določajo na posamezni članici, vzdrževanje požarne pregrade pri zavezancu pa izvaja zunanji izvajalec……., ki se ravna po navodilih Računalniškega centra zavezanca (******). Požarna pregrada je bila nazadnje nadgrajena……, ko je bila nameščena nova verzija programske opreme. Naprava omogoča pregledovanje standardnih (varnih in običajnih) poštnih protokolov, kot je to razvidno iz pojasnila podjetja …….Administratorske pravice do naprave ima……, RC Fakultete ****** pa bralne pravice. Po pojasnilu navedenega podjetja gre za opremo, ki temelji na lastniški tehnologiji proizvajalca in ne gre za odprtokodne rešitve, s tem pa je lokalnim administratorjem onemogočen dostop do podatkov o vsebini, ki se pregleduje s pomočjo te naprave. Sama naprava nima diskovnih zmogljivosti in pošte ne shranjuje, temveč opozori na zaznane nedovoljene dogodke. Dnevniška datoteka se hrani na sami napravi. Pri kriptiranih povezavah naprava uporabniku ponudi svoj certifikat, kar je opazil tudi prijavitelj.

Po prejemu pritožbe je bila DPI funkcionalnost izključena. Zunanji izvajalec je RC Fakultete ****** svetoval pripravo varnostne politike, ki bi bila tudi osnova za pravila glede uporabe določenih funkcionalnosti. Ugotovljeno je bilo, da varnostne politike pri zavezancu niso posodobili ob prehodu s starih na nove požarne pregrade. Predstavnik ****** je opozoril, da sama funkcionalnost ni bila izvedena na uporabniku prikriti način, saj je moral uporabnik aktivno sprejeti ponujeni ceritifikat, sicer ni mogel nadaljevati z delom.

Dne 2. 6. 2009 je bil izveden ogled pri zavezancu. Ugotovljeno je bilo, da zavezanec kot članica ****** sledi priporočilom le te, tako da lastnih varnostnih informacijskih politik, kot so politika dopustne rabe službenih računalnikov, politike delovanja IT službe, politika uporabe elektronskih dokumentov, politike uporabe in nameščevanja programske ter strojne opreme, politika uporabe aplikacij, politika uporabe storitev interneta (svetovni splet, e-pošta, ftp…), politika uporabe varnostnih mehanizmov ipd. pri zavezancu nimajo. V pripravi naj bi bil pravilnik ravnanju z e-pošto, s katerim naj bi uredili to vprašanja glede rabe e-pošte na ravni zavezanca. Zavezanec je s strani ****** dobil Priporočilo ****** iz leta 2007, ter navodila za sistemsko sobo, helpdesk in podporo uporabnikom.

Pred tremi leti so pri zavezancu kupili svojo požarno pregrado, …..pa so jo zamenjali zaradi slabe prepustnosti in slabše funkcionalnosti. Izbor in nakup opreme je opravil Računalniški center Univerze ******, sama požarna pregrada pa je fizično locirana ……Takšne požarne pregrade naj bi imelo še nekaj fakultet. Osnovno konfiguracijo pregrade je opravilo podjetje …….RC zavezanca ni dal nobenih navodil podjetju …..za nadgradnjo oziroma navodil, katere funkcionalnosti naj vklopi in razen zahtevkov za odpiranje določenih portov in implementacije pravil internega požarnega zidu, ki ločuje administrativni del od ostalega

omrežja zavezanca, niso dajali drugih zahtev na podjetje …….Državni nadzornik in informatik sta si ogledala spletni dostop do nastavitev požarne pregrade. Zavezanec ima spletni dostop, ki je omejen na določen IP naslov, uporabniško ime in geslo, nimajo pa nobene dokumentacije o požarni pregradi, prav tako nimajo sklenjene pogodbe s podjetjem ……saj je ta sklenjena s strani Računalniškega centra univerze ******.

Dne 2. 7. 2009 je bil izveden še ogled na sedežu podjetju…...

Predstavniki podjetja so na ogledu pojasnili, da je praksa pri različnih članicah ****** različna in sicer imajo z nekaterimi sklenjene vzdrževalne pogodbe, v katerih od članic univerze zahtevajo pripravo varnostnih politik, pri nekaterih članicah pa teh določb ni vključenih v pogodbe.

Na ogledu je bilo ugotovljeno, da naprava, ki je nameščena pri zavezancu trenutno ne izvaja nobenega beleženja v dnevniške datoteke. Logiranje se vklopi ob zaznanem incidentu na zahtevo uporabnika torej pooblaščenih oseb zavezanca. Naprava omogoča, da se v dnevniški datoteki na sami napravi hrani podatke o prestreženih napadih, zaznanih virusih in ostale sistemske zapise, npr. ob napakah (prevelika temperatura), ne hrani pa se v tej datoteki nobenih osebnih podatkov. Naprava ne omogoča logiranja zavrnjenih paketov na samo napravo, kar pomeni, da se na napravi ne hranijo podatki o tem, kateri paketi so šli skozi napravo in kateri ne. Rok hrambe dnevniških datotek na sami napravi je omejen z zmogljivostjo naprave, okvirno gre za dolžino nekaj strani. Dostop do te naprave ima največ 5 oseb redno zaposlenih s t.i. servisnim uporabniškim imenom in geslom, ki pa ni vezano na posameznega uporabnika, ampak je zaradi narave dela (reševanje napak, ko je lahko drugi zaposleni odsoten) skupno. Sam dostop administratorjev do naprave se ne beleži. Incidenti so definirani s strani proizvajalca požarne pregrade, gre za podpise virusov in druge škodljive programske kode (spyware, malware). Pri antivirusnem delu se incident lahko zabeleži v dnevniško datoteko na napravi, podobno velja za IPS in druge zmogljivosti naprave. Zavezanca do tega trenutka niso obveščali o posameznih incidentih. S pomočjo požarne pregrade se da ugotoviti, kdo je kdaj dostopal do katere spletne strani, če je vklopljeno beleženje v dnevniške datoteke, in sicer se lahko v dnevniško datoteko zabeležijo ti podatki, da je razvidno, kateri IP je kdaj dostopal do katere spletne strani. Omenjeno funkcionalnost omogočajo vse požarne pregrade in številni drugi mrežni elementi. Državni nadzornik si je ogledal delovanje po posameznih funkcionalnostih (System, Router, Firewall, UTM itd.). Ob ogledu so bile izdelane zaslonske slike, ki potrjujejo predhodno podane navedbe glede nastavitev naprave in dnevniških datotek.

2. Obrazložitev sprejetih ukrepov

Uvodoma je bilo potrebno ugotoviti, kdo je v konkretnem primeru zavezanec kot upravljavec osebnih podatkov. Nedvomno je v konkretnem primeru zavezanec po določbah ZVOP-1 Fakulteta ******. Po definiciji iz 6. tč. 6. člena ZVOP-1 je upravljavec osebnih podatkov

fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave. V konkretnem primeru je Računalniški center Univerze ****** izvedel samo postopek nabave požarne pregrade, sama pregrada pa je bila predana v upravljanje Fakulteti ******. Članice Univerze ****** so za vzdrževanje požarne pregrade sklenile pogodbe s pogodbenim obdelovalcem podjetjem …..po navedbah zavezanca, pa zavezanec takšne pogodbe s podjetjem ……nima sklenjene.

Kot je bilo ugotovljeno v postopku inšpekcijskega nadzora je do nadgradnje požarne pregrade, ki je pomenila vključitev t.i. funkcionalnosti DPI prišlo po inerciji, ključen element pri tem pa je odsotnost ustreznih varnostnih politik pri zavezancu, zlasti politike nadgradenj programske opreme in varovanja internega omrežja. Ob odsotnosti tovrstne politike je bila požarna pregrada nadgrajena za zadnjimi nadgradnjami, ki so vključevale funkcionalnost DPI, ki preverja vsebino komunikacije in deluje tako na nekriptiranih kot tudi na kriptiranih povezavah, o čemer pa uporabniki niso bili posebej obveščeni. Pregledovanje kriptiranih protokolov naprava izvaja tako, da se uporabniku predstavlja s svojim certifikatom in na ta način preveri vsebino kriptirane povezave za morebitne viruse, vohunsko in ostalo škodljivo programsko kodo.

Da pri delovanju omenjene požarne pregrade prihaja do obdelave osebnih podatkov je neizpodbitno, saj naprava obdeluje prometne podatke, med katere sodijo podatki o obiskanih spletnih straneh in poslanih elektronskih poročilih, kar dejansko izhaja iz narave stvari oz. namena delovanja požarne pregrade. Sama DPI funkcionalnost pa preverja tudi ustreznost vsebine glede na vnaprej postavljene kriterije. S tega vidika je uporaba tovrstne tehnologije lahko sporna, saj prihaja do trenj oziroma tehtanja med različnimi pravicami. Po eni strani pravice uporabnika omrežja zavezanca do razumne meje zasebnosti tudi na delovnem mestu, ki utemeljeno pričakuje zasebnost svoje korespondence in varstva osebnih podatkov, po drugi strani pa prav tako legitimne pravice zavezanca do varovanja svojega premoženja, konkretno varnosti lastnega omrežja, s tem posledično pa potencialno tudi zasebnosti drugih uporabnikov omrežja.

ZVOP-1 ne vsebuje določb, ki bi natančneje regulirale uporabe opreme, ki omogoča varovanje omrežja, zato je potrebno odgovore poiskati v temeljnih načelih varstva osebnih podatkov. 2. člen ZVOP-1 določa načelo zakonitosti in poštenosti in sicer naj bi se osebni podatki obdelovali zakonito in pošteno. 3. člen ZVOP-1 dalje opredeljuje načelo sorazmernosti in sicer morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Za odločitev državnega nadzornika v konretnem primeru je prav tako pomembno načelo namenskosti uporabe osebnih podatkov. 16. člen ZVOP-1 namreč določa, da se osebni podatki lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.

Glede na navedena načela je potrebno pri obdelavi osebnih podatkov zagotoviti pošteno in zakonito obdelavo, sorazmernost ter namenskost obdelave osebnih podatkov. Da bi lahko obdelava osebnih podatkov bila poštena in zakonita mora biti posameznik o obdelavi osebnih podatkov obveščen. Ob odsotnosti varnostne politike, ki bi opredeljevala postopke ob nadgradnjah programske opreme je v konkretnem primeru prišlo do vključitve dodatne funkcionalnosti požarne pregrade in do obdelave osebnih podatkov, o kateri posamezniki niso bili obveščeni, prav tako pa je verjetno marsikateri uporabnik enostavno sprejel ponujeni certifikat požarne pregrade in s tem omogočil požarni pregradi nadzor vsebine kriptirane komunikacije, ne da bi se resnično zavedal namena in okoliščin nadzora. Iz navedenih vzrokov je bilo potrebno zavezancu naložiti sprejem ustrezne varnostne politike, s katero mora zavezanec utemeljiti razloge za vklop funkcionalnosti varnostne opreme, postopke nadgradnje varnostne opreme ter način obveščanja posameznikov o namenu in načinu delovanja te opreme.

Ali bi državni nadzornik od zavezanca lahko zahteval, da funkcionalnost DPI izvajala le nad tistimi uporabniki omrežja zavezanca, ki bi se s tem strinjali in torej podali privolitev? Državni nadzornik za varstvo osebnih podatkov ni našel pravne podlage, ki bi zavezancu prepovedovala uporabo funkcionalnosti DPI, zaradi zagotavljanja načela zakonitosti in poštenosti obdelave osebnih podatkov, pa je bilo zavezancu zato potrebno naložiti v izreku odločbe navedene ukrepe - uporabnik mora namreč imeti možnost informirane odločitve. Ali je uporaba varnostnih mehanizmov, kot je uvedba DPI funkcionalnosti, potrebna za vzdrževanje varnosti omrežja ali ne, je vprašanje, o katerem stroka verjetno nima enotnega odgovora in tako ostaja diskrecijska pravica zavezanca, ki ima legitimno pravico, da takšen ukrep uvede, podobno kot velja za druge omrežne elemente, ki teoretično tudi omogočajo nadzor vsebine in/ali prometnih podatkov (npr. mrežni prehodi, posredovalni strežniki, poštni strežniki). S tehtanjem pravice posameznika do varovanja svoje zasebnosti pa mora po drugi strani uporabnik imeti možnost informirane odločitve, da presodi, ali bo uporabljal komunikacijske kanale, ki so podvrženi varovanju z DPI tehnologijo ali ne, predpogoj pa seveda je, da je o tem ustrezno vnaprej obveščen in da lahko informirano odločitev sploh sprejme.

Načelo namenskosti obdelave osebnih podatkov je v konkretnem primeru, ko gre za uporabo DPI tehnologije z namenom varovanja omrežja pred škodljivo programsko kodo, izrednega pomena. Tehnologije oziroma oprema, ki je namenjena varovanju omrežja, deluje pa na način, ki ga lahko štejemo za obdelavo osebnih podatkov, sme biti uporabljena izključno za ta namen, uporaba v ostale namene pa je možna le na podlagi ustrezne pravne podlage. Podobno ne nazadnje velja pri elektronski pošti – sistemski administratorji oziroma drugi zaposleni v službi za informatiko bi tehnično gledano lahko posegali v vsebino komunikacije ali obdelovali prometne in s tem osebne podatke za druge namene, npr. po navodilu nadrejenega, ki želi nadzirati uporabo interneta ali elektronske pošte. Vsekakor pa bi bilo takšno početje brez ustrezne pravne podlage nezakonito in bi lahko predstavljalo bodisi kršitev ZVOP-1 bodisi storitev kaznivega dejanja. Konkretna naprava je primarno namenjena varovanju omrežja, kot vsaka druga tehnologija pa se teoretično lahko uporabi

tudi za nezakonite namene. Glede na to, da naprava pri svojem delovanju pregleduje vsebino komunikacije, je nujno potrebno poskrbeti za transparentnost, varnost in predvidljivost njenega delovanja s sprejemom ustrezne politike in obveščanja uporabnikov. Prav tako pomembno je, da se zaposleni, ki imajo dostop do naprave, tako pri zavezancu kot pri pogodbenem obdelovalcu natančno zavedajo, da predstavlja uporaba naprave za druge namene, ki niso povezani z varovanjem omrežja, nezakonito ravnanje.

S tem je odločba utemeljena in z njo je bilo treba na podlagi 54. člena ZVOP-1 odrediti odpravo ugotovljenih nepravilnosti in pomanjkljivosti, kot je določeno v izreku te odločbe.

Odločba je izdana po uradni dolžnosti in je na podlagi 22. člena Zakona o upravnih taksah takse prosta.

Pouk o pravnem sredstvu:

Zoper to odločbo ni pritožbe, dopustno pa je sprožiti upravni spor s tožbo na Upravnem sodišču Republike Slovenije v Ljubljani, Fajfarjeva 33, v roku 30 dni po prejemu te odločbe. Tožba se vloži pri pristojnem sodišču neposredno pisno ali se mu pošlje po pošti. Tožba z morebitnimi prilogami se vloži najmanj v treh izvodih. Tožbi je treba priložiti tudi to odločbo v izvirniku ali prepisu.

mag. Andrej TOMŠIČ
državni nadzornik
za varstvo osebnih podatkov

Vročiti:
- zavezancu, z vročilnico;
- arhiv, tu.