



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE IN JAVNO UPRAVO

DIREKTORAT ZA INFORMATIKO IN E-STORITVE

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 86 51

F: 01 478 86 49

E: gp.mju@gov.si

www.mju.gov.si

REPUBLIKA SLOVENIJA
Urad Vlade RS za komuniciranje

Gregorčičeva 25
1000 Ljubljana

Gp.ukom@gov.si

Številka: 010-504/2012/3

Datum: 12. 2. 2013

Zadeva: Odgovor na predlagam.vladi.si predlog 3738: Nadzor državnih uradnikov

Zveza: Vaš dopis št. 092-392/2012/1 z dne 7.11.2012

Spoštovani!

Predlog št. 3738 *Nadzor državnih uradnikov* je v predlagani obliki neprimeren. V primeru izvajanja nadzora nad zaposlenimi, kot je predlagano, verjetno ne bi bilo sprejeto niti s strani Informacijske pooblaščenke RS.

MPJU je v zvezi s to problematiko že podajal odgovore, da je tehnično mogoče izvesti omejitve dostopa do interneta, vendar menimo, da MPJU ni tisti, ki bi javnim uslužbencem omejeval pravico do zasebnosti na delovnem mestu in pravico do informiranja. Menimo, da je to predvsem politična odločitev, ki jo mora sprejeti politika in jasno določiti primerne vsebine, do katerih javni uslužbenci lahko dostopajo med delovnim časom. Popolna omejitev dostopa do storitev in vsebin na internetu vsekakor ne bi bila primerna rešitev, saj bi s tem onemogočili tudi dostop do vsebin, ki pa so povezane z delovnimi nalogami. Bolj primerno bi bilo, da bi nekako skladno z etičnim kodeksom javnih uslužbencev uredili tudi to področje in določili vsebine, ki niso primerne za uporabo javnim uslužbencem med delovnim časom. Takšne skupine bi lahko bile npr. pornografija, spletne igre, igre na srečo, spletna pošta (razen uradna pošta organa, ki je tudi lahko spletna), P2P komunikacija, izmenjava datotek, socialna omrežja (razen za PR službo, marketing), forumi in podobno.

MPJU tehnično že sedaj na robnih požarnih pregradah zaradi varnostnih razlogov omejuje nekatere storitve na internetu, za katere (skupaj z drugimi strokovnjaki na tem področju) menimo, da so škodljive za omrežje HKOM in naprave ter informacijske sisteme v omrežju, ki ga upravljamo. Tako skladno s priporočili proizvajalca opreme požarne pregrade CheckPoint že blokiramo vse storitve na internetu, ki so označene s stopnjo tveganja 4 in 5. Skladno z dopisom MPJU št. 386-2/2011/16 z dne 12. 3. 2012, ki je bil poslan organom, pa bomo v kratkem omejili tudi nekatere skupine – kategorije vsebin kot so P2P komunikacija, izmenjava datotek (file sharing) in podobne, ki so označena s stopnjo 3. Tu se postavlja vprašanje primernosti dostopa do nekaterih vsebin, omenjenih v prejšnjem odstavku, za kar pa MPJU ni pristojen.

Uveljavitev nadzora nad zaposlenimi kot predlagano s predlogom št. 3738, pa bi predstavljal tudi organizacijsko tehnični problem, saj MPJU v luči varčevanja in zmanjševanja finančnih in kadrovskih virov nima možnosti, da bi te naloge izvajal. Naloge MPJU so, da zagotavlja

razpoložljive in varne storitve. Uporabniki pa so tisti, ki bi imeli radi na voljo vse storitve, tudi tiste, za katere vemo, da niso povezane z delovnimi nalogami. Takojšnja omejitev nekaterih priljubljenih storitev, bi nam kratkoročno prinesla veliko dodatnega dela predvsem z iskanjem neobstoječih napak v delovanju in prepričevanju uporabnikov v sprejete varnostne odločitve.

MPJU v okviru nadzora nad delovanjem omrežja izvaja naloge zagotavljanja dostopa do storitev na internetu. Tako je možno opraviti tudi statistiko dostopov do spleta, kjer med najpogostejšimi storitvami najdemo iskalnik google, spletno pošto in znane slovenske portale z novicami; npr. portal 24ur.com dosega okoli 4 % vsega mesečnega internetnega prometa.

MPJU tudi opaža porast primerov zlorabe službenega omrežja za sporne objave na spletnih forumih, zato bi bilo vredno razmisliti o ustrezni izobrazbi in obnašanju zaposlenih pri uporabi forumov in socialnih omrežij. V primeru prijave MPJU Policiji vedno posreduje vse potrebne podatke za odkritje storilca kaznivih dejanj.

Menimo, da bi ob primerni podpori politike, ustrezni kadrovske in finančne okrepitvi MPJU, DIES lahko izvedel vse ukrepe, ki bi tovrstne probleme, ki motijo predlagatelje, lahko rešili tako, da do motečih pojav in zlorab dostopov do interneta ne bi prihajalo.

Ukrepi, ki so potrebni, so:

- da MPJU skladno z zakonskimi pooblastili lahko ureja informacijsko varnostno politiko brez postavljanja izjem, ki so posledica »politične moči« posameznih organov,
- da se pripravi primerno izobraževanje za vse javne uslužbence v smislu obnašanja na spletu,
- da Vlada RS zagotavlja ustrezna sredstva za izvajanje teh ukrepov.

Lepo pozdravljeni,

Pripravil:
mag. Damijan Marinšek
sekretar

Mojca Kucler Dolinar
državna sekretarka

Poslano:

- naslovniku – elektronsko