KOMISIJA ZA PREPREČEVANJE KORUPCIJE

REPUBLIKA SLOVENIJA

Pojasnilo glede varnosti spletnih obrazcev Komisije za preprečevanje korupcije

Po noveli Zakona o integriteti in preprečevanju korupcije iz leta 2011 morajo zavezanci podatke o premoženjskem stanju, omejitvah poslovanja in sezname zavezancev komisiji posredovati prek elektronskega obrazca, dostopnega na spletnih straneh komisije.

Ker se na komisiji zavedamo problema varnosti osebnih in drugih podatkov, ki se prenašajo prek komunikacijskih omrežij, zlasti interneta, varnost podatkov, posredovanih prek spleta zagotavljamo na več nivojih.

Dostop do spletnih obrazcev prek šifrirane povezave

Spletni obrazci, prek katerih zavezanci komisiji posredujejo podatke, so dostopni samo prek šifrirane spletne povezave. To pomeni, da so spletni obrazci dostopni prek šifrirane HTTPS povezave (ang. *HyperText Transfer ProtocolSecure*). HTTPS povezava med spletnim strežnikom in spletnim brskalnikom uporabnika s pomočjo varnostnih protokolov SSL oziroma TLS omogoča šifriran prenos podatkov med strežnikom in odjemalcem (spletnim brskalnikom) ter s tem zagotavlja visoko stopnjo varnosti pri prenosu podatkov.

Spletni strežnik komisije je nastavljen tako, da uporabnike vedno preusmeri na HTTPS šifrirano povezavo, tudi če se uporabnik zmoti in do strežnika poskuša dostopati prek navadne, nešifrirane povezave. Varnostna analiza HTTPS povezave spletnega strežnika komisije s strani podjetja Qualys SSL Labs sicer kaže, da je šifrirana spletna povezava spletnega strežnika komisije korupcije visoko kakovostna, saj je skupna ocena konfiguracije SSL povezave ocenjena z oceno A.

Varnost pri vnašanju in preverjanju podatkov ter hramba podatkov na spletnem strežniku v šifrirani obliki

Spletne obrazce zavezanci izpolnjujejo v treh korakih. V prvem koraku zavezanec v spletni obrazec, ki se prikaže v njegovem spletnem brskalniku,vnese svoje podatke.

V drugem koraku se podatki prek šifrirane povezave prenesejo na spletni strežnik komisije, kjer se preveri njihova **veljavnost**. To pomeni, da spletna aplikacija preveri, ali so podatki posredovani v pravilni obliki (na primer: da sta ime in priimek osebe zapisana v skladu z razpoložljivim naborom črk in znakov za zapis osebnega imena v Republiki Sloveniji, da sta EMŠO ali davčna številka zapisana v skladu z zakonsko veljavnim načinom in da se v posredovanem EMŠO ali davčni številki ujema izračun kontrolne številke in drugo)

Pri tem preverjanju se podatki ne shranijo na strežnik, aplikacija na strežniku pa je zasnovana tako, da se podatki v nobenem primeru ne shranjujejo v začasne datoteke, pač pa se hranijo izključno v delovnem pomnilniku (RAM). V primeru, da spletna aplikacija ugotovi neveljavnost podatkov, zavezancu sporoči napako, ko pa so podatki ustrezno preverjeni, uporabnik v drugem koraku lahko podatke pred dokončno potrditvijo še pregleda oziroma se vrne na ponoven vnos oziroma popravljanje.

V tretjem koraku se (preverjeni) podatki prek varne povezave prenesejo na spletni strežnik komisije. Tam spletna aplikacija ustvari PDF dokument, ki poleg posredovanih podatkov vsebuje še identifikacijsko črtno kodo.

Ta PDF dokument se prikaže v spletnem brskalniku uporabnika, uporabnik pa ga natisne, podpiše (fizično ali elektronsko) in pošlje na naslov komisije.

Hkrati se podatki iz spletnega obrazca v elektronski obliki shranijo tudi na strežniku. **Podatki se shranijo v šifrirano datoteko**. Pri tem je uporabljeno tako imenovano asimetrično šifriranje, kar pomeni, da podatkov na spletnem strežniku komisije ni mogoče dešifrirati. Dešifriranje je mogoče le na ločenem internem strežniku komisije, saj na spletnem strežniku ni šifrirnih ključev za dešifriranje podatkov.

Dodatna varnost spletnega strežnika

Spletni strežnik komisije poleg tega uporablja še dodatne zaščitne mehanizme. Tako uporabljamo ustrezno nastavljeno požarno pregrado (ang. *firewall*), s katero onemogočamo nepooblaščene dostope do strežnika, administrativni dostop do strežnika pa ima le omejen krog oseb. Skrbimo tudi za ustrezne varnostne posodobitve programske opreme na strežniku ter varnostno arhiviranje podatkov.

Prenos podatkov v interno omrežje komisije in varnost internega strežnika

Šifrirane datoteke s podatki iz spletnih obrazcev se prek posebne, še dodatno šifrirane povezave samodejno prenesejo na interni strežnik komisije. Ta strežnik se nahaja v zaščitenem HKOM omrežju.

Kljub temu, da je HKOM omrežje državne uprave ustrezno zavarovano, je naš interni strežnik še dodatno zavarovan na več ravneh. Tako uporabljamo dodatno požarno pregrado, trdi disk strežnika je v celoti šifriran, dostop do administracije strežnika ima le omejen krog oseb. Poskrbljeno je tudi za fizično varnost strežnika in varnostno arhiviranje podatkov.

Ko se šifrirane datoteke s podatki prenesejo na interni strežnik, se dešifrirajo in shranijo v bazo podatkov, vendar šele po tem, ko na komisiji prejmemo s strani zavezanca podpisan obrazec s črtno kodo. Podatki iz te baze so nato vidni v interni aplikaciji Corruptio, ki teče na tem internem strežniku.

Varovanje podatkov v internih podatkovnih bazah in aplikacijah komisije

Dostop do aplikacije Corruptio je omogočen le omejenemu krogu oseb, omogočen pa je le iz internega računalniškega omrežja komisije oziroma za nekaj oseb z enkratnim geslom zaščitenih VPN povezav. Kljub temu, da se tako uporabniki aplikacije, kot tudi strežnik nahajajo v internem omrežju komisije, je dostop do aplikacije mogoč samo prek šifrirane povezave.

Vsi dostopi do aplikacije Corruptio – torej tudi vpogledi v osebne podatke – se neizbrisno beležijo in sicer na ločenem strežniku. Sistem je zasnovan tako, da v primeru, da bi nekdo odklopil ta ločeni strežnik za neizbrisno beleženje revizijskih sledi (torej dostopov do osebnih podatkov), osnovna aplikacija za dostop do osebnih podatkov Corruptio preneha delovati.

Ustrezno je zavarovan tudi strežnik, ki hrani revizijske sledi (dodatna požarna pregrada, v celoti šifriran trdi disk, varnostno arhiviranje, zelo omejeni administrativni dostopi,…).

Seznanjenost zaposlenih na komisiji z obveznostjo varovanja osebnih podatkov

Vsi uporabniki aplikacije Corruptio in podatkovnih baz, ki jih aplikacija uporablja, so dobro seznanjeni z *Zakonom o varstvu osebnih podatkov* in svojimi obveznostmi glede varovanja osebnih podatkov. Uporabniki (zaposleni na komisiji) so se udeležili izobraževanja tako o varstvu osebnih podatkov, kot tudi o varnosti informacijskih sistemov, podpisali pa so tudi ustrezne izjave glede varstva osebnih podatkov. Izobraževanja

iz področja varstva osebnih podatkov in informacijske varnosti so za zaposlene na komisiji obvezna in se periodično ponavljajo, saj želimo, da zaposleni svoja znanja iz teh področij redno obnavljajo in nadgrajujejo.

Na enak način so bili z *Zakonom o varstvu osebnih podatkov* in osnovami informacijske varnosti seznanjeni tudi zunanji sodelavci (programerji), ki sicer nimajo samostojnih dostopov do omenjene infrastrukture (strežnikov in podatkovnih baz). V primeru kakršnegakoli dela na strežnikih ali bazi podatkov zunanjim sodelavcem komisije dostop omogoči ena izmed za to pooblaščenih oseb na komisiji,in sicer vedno le iz prostorov komisije. Ta oseba tudi nadzira delo in aktivnosti zunanjih sodelavcev.

Na komisiji se zavedamo dejstva, da popolne varnosti ni mogoče zagotoviti, lahko pa zagotovimo, da smo se glede varovanja osebnih in drugih podatkov, ki jih zavezanci posredujejo komisiji, potrudili po svojih najboljših močeh, v skladu z zakonom in ustreznimi varnostnimi standardi, ki veljajo na tem področju.