Zavod za informatičku djelatnost Hrvatske d.o.o. Zagreb

Izvješće o analizi sukladnosti programskog rješenja elektroničke dostave ponuda javne nabave s aspekta informacijske sigurnosti

- SAŽETAK -

Zagreb, ožujak 2013.

1. SAŽETAK

ZIH – Zavod za informatičku djelatnost Hrvatske proveo je detaljnu analizu i pregled programskog rješenja elektroničke dostave ponuda javne nabave s aspekta informacijske sigurnosti, te analizu razvojne i korisničke dokumentacije. Pregled je proveden temeljem kriterija koji proizlaze iz primjenjivih zakonskih i podzakonskih akata Republike Hrvatske, primjenjivih europskih direktiva, međunarodnih normi u domeni informacijske sigurnosti i testiranja programske opreme te preporuka dobre prakse u razvoju web aplikacija. Svi ovi kriteriji detaljno su elaborirani u *Izvješću o analizi sukladnosti programskog rješenja elektroničke dostave ponuda javne nabave s aspekta informacijske sigurnosti* koje je predano Narodnim novinama.

Sa stajališta informacijske sigurnosti ključni zahtjevi odnose se na sigurnost veze korisnika sa sustavom, sigurnost identiteta korisnika, enkripciju i dekripciju pojedinih dokumenata, 4-eyes princip, digitalni potpis, vremenski žig i raspoloživost samog sustava. Zadovoljenje tih zahtjeva provjereno je kroz pregled izvornog koda te analizu razvojne i korisničke dokumentacije.

Pregled izvornog koda napravljen je imajući u vidu najkritičnije sigurnosne rizike web aplikacija prema OWASP-u (Open Web Applications Security Project) te sigurnosna pitanja karakteristična za proces javne nabave (verifikacija ponuditelja i naručitelja, integritet i povjerljivost sadržaja ponude). Tim pregledom i analizom rezultata testiranja utvrđeno je da su implementirane potrebne kontrole za izbjegavanje prepoznatih rizika. Integritet i povjerljivost ponude ostvaruje se kriptografskim tehnikama primjenom javnog i privatnog ključa. Javni ključevi pohranjeni su u bazi sustava javne nabave, dok se privatni ključ šalje e-mail-om naručitelju. Svaki dokument koji dolazi se u memorijskom prostoru HASH-ira i nakon toga dvostruko kriptira sa simetričnim ključem koji se potom pohranjuje kriptiran s javnim ključevima naručitelja te potom sprema u DM sustav. Na taj način potvrđuje se mjesto pohrane dokumentacije kao hermetički zaštićeni „safe-box", kojem nitko neovlašten ne može pristupiti, što i jeste u skadu sa zahtjevima projekta. Sigurnost otvaranja ponuda očuvana je provjerom vremena otvaranja ponuda te postojanjem prijave privatnih ključeva dvaju predstavnika naručitelja na web stranici sustava.

Analizom razvojne dokumentacije utvrđeno je da su adekvatno definirani svi sigurnosni zahtjevi i da su u potpunosti slijeđeni zahtjevi hrvatskog zakonodavstva, ali i europskih direktiva u području elektroničke nabave i digitalnog potpisa. Također, ugrađeni su i zahtjevi normi informacijske sigurnosti po pitanju kriptografskih kontrola i sigurne razmjene informacija elektroničkim putem. Testna dokumentacija i testni slučajevi pokazuju da su u cijelosti istestirani i sigurnosni aspekti programskog rješenja.

Iz analize korisničke dokumentacije proizlazi da su upute dobro strukturirane i pregledne, u cijelosti slijedeći proces nabave. Usklađene su sa svim pravnim, statutarnim i regulatornim zahtjevima. Jasne su i jednostavne za primjenu od strane korisnika. Također, *Korisničke upute za e-Tendering, uloga naručitelja*, daju i obveze ovlaštenih predstavnika po pitanju pohrane privatnog ključa i njegove dostave nakon isteka roka za dostavu ponuda.

Kako iz navedenog proizlazi da je iznimno bitno osigurati povjerljivost, integritet i raspoloživost privatnih ključeva, preporuka je raditi na podizanju razine informacijske sigurnosti kod potencijalnih naručitelja, kroz definiranje politika upravljanja elektroničkom poštom, zaporkama i izradom sigurnosnih kopija podataka.

Na kraju, može se zaključiti da ovo rješenje za elektroničku dostavu ponuda javne nabave u cijelosti zadovoljava identificirane sigurnosne zahtjeve i preporuča se za primjenu u praksi. Ugrađeni sigurnosni mehanizmi garantiraju prihvatljivu razinu sigurnosti u kompletnom procesu nabave. Sve informacije iz ponuda koje se dostavljaju u procesu nabave u cijelosti su sigurne i ni na koji način ne mogu biti korištene od strane Narodnih novina, kao pružatelja usluge e-Tendering.

2. DODATAK – Sigurnosne preporuke za naručitelje

Preporuke za korištenje elektroničke pošte

Elektronička pošta mora se štititi od neovlaštenog pristupa ili bilo kakvih promjena. Svi korisnici koji imaju mogućnost korištenja elektroničke pošte odgovorni su za povjerljivost, integritet i raspoloživost informacija koje se njome prenose. Sve poruke sadrže naznaku povjerljivosti (npr. u podnožju poruke). Poruke koje se šalju putem javne mreže ne smiju uključivati klasificirane informacije, kao npr. povjerljive ili tajne, ukoliko nisu kriptirane. Kod otvaranje e-maila s privitcima automatski se provodi testiranje privitaka na viruse. Korisnici moraju osigurati da su informacije koje su proslijedili putem e-maila ispravno adresirane i poslane odgovarajućim osobama. Na sve dolazne mailove naručitelja primjenjuje se spam filter koji se automatski sinkronizira sa više globalnih antispam listi.

Sve pohranjene, proslijeđene ili zaprimljene informacije te informacije sadržane u službenim pretincima elektroničke pošte korisnika, smatraju se vlasništvom naručitelja.

Napomena: U slučaju da naručitelj želi izbjeći slanje privatnog ključa putem elektroničke pošte, preporuka je da sam kreira vlastiti par ključeva i dostavi ih sustavu.

Preporuke za korištenje zaporki

Zaporke se ne smiju zapisivati, slati e-mailom, dijeliti s drugim korisnicima te pohranjivati na računalnim sustavima u nezaštićenom obliku. Također, preporuka je ne koristiti istu zaporku na različitim sustavima. Korisnik treba mijenjati zaporku u redovitim vremenskim razmacima (minimalno svakih 6 mjeseci). Preporuka je ne koristiti opciju *'zapamti moju zaporku'* koju nude mnoge aplikacije. Ako postoji bilo kakva indicija da je sustav ugrožen ili postojeća zaporka kompromitirana, korisnik je dužan o tome informirati administratora i čim prije promijeniti postojeću zaporku. Pri kreiranju zaporke preporuka je pridržavati se sljedećih smjernica:

- dužina zaporke barem 6 znakova
- uključuje velika i mala slova (a–z, A–Z); znamenke (0-9) i specijalne znakove: ! @ # $ % ^ & * ( ) _ + = \ ` { } [ ] : " ; ' < > ? , . /
- ne predstavlja smislenu riječ ni u jednom jeziku, dijalektu ili žargonu
- nije bazirana na osobnim informacijama, kao što su imena i bitni datumi vezani za članove obitelji.

Preporuke za izradu sigurnosnih kopija podataka

Za sve važne poslovne informacije, uključujući elektroničku poštu, moraju se redovito raditi sigurnosne kopije. Također, potrebno je osigurati da se iz njih mogu obnoviti podaci u slučaju kvara ili pada informacijskog sustava. Za svaki sustav potrebno je definirati procedure za izradu sigurnosnih kopija, koje uključuju opseg sigurnosnih kopija, učestalost izrade, vrijeme čuvanja te učestalost provjere ispravnosti sigurnosnih kopija.

U slučaju nepostojanja automatske replikacije podataka na alternativnu lokaciju, preporuka je kreirati sigurnosne kopije podataka na svim serverima na kraju svakog radnog dana. Sigurnosne kopije se trebaju čuvati na sigurnim mjestima, npr. u vatrootpornom sefu. Sigurnosne kopije trebaju imati odgovarajuću razinu fizičke zaštite u skladu s povjerljivošću informacija i odgovarajućim standardima

koji se primjenjuju na lokaciji naručitelja. U slučaju da se radi o klasificiranim informacijama, sigurnosne kopije podataka trebaju se zaštititi kriptografski.

Ispravnost sigurnosnih kopija se redovito provjerava, u propisanim vremenskim intervalima, a u cilju otkrivanja eventualnih neispravnosti. Procedure vraćanja podataka sa sigurnosnih kopija moraju biti dokumentirane i pohranjene na definiranim lokacijama naručitelja. Spomenute procedure potrebno je redovito provjeravati i po potrebi revidirati.

Prilikom zbrinjavanja medija sa starim kopijama podataka, nužno ih je prethodno prebrisati, kako ne bi došlo do curenja povjerljivih informacija van organizacije naručitelja.

Direktorica ZIH-a

Dr.sc. Silvana Tomić Rotim