ID – ime projekta

Opis projekta

Naročnik

Vrednost projekta

OANV (Ocenjeni aplikacijski nivo varnosti)

CANV: 5[i]

"SKRIVNOST" - Visoko varnostno kritična aplikacija

OANV – ključne aktivnosti	
1. Pogodbene zaveze	0
2. Varnostne zahteve	0
3. Varnostna arhitektura	0
4. Varnostno preverjanje	0

OANV - aktivnosti	
5. Ljudje	0
6. Varno kodiranje	0
7. Preverjanje varnostnih funkcij	0
8. Ključne ranljivosti	0
9. Metrike	0
10. Varnostni standardi in prakse	0

1. Pogodbene zaveze

Točk: 0[ii]

Zahteva po sodelovanju varnostnega strokovnjaka	**Kriterij**: V pogodbi je določeno, da na projektu pri izvajalcu ves čas sodeluje izkušen varnostni strokovnjak, saj ljudje, ki razvijajo, praviloma nimajo razvite napadalske miselnosti.	0
Določitev varnostnih mejnikov in metrik	**Kriterij**: V naročniški pogodbi so jasno zapisani varnostni mejniki in varnostne metrike. Če so varnostni mejniki združeni s projektnimi mejniki, morajo biti posebej označeni. Na ta način se določi bodoči nivo varnosti aplikacij in načine merjenja uspeha. Primeri mejnikov: varnostni test sprejemljivosti, "security push". Primeri metrik: števec ranljivosti, sDD, sDAR, krivulja odkrivanja ranljivosti ipd.	0
Odgovornost za ranljivosti	**Kriterij:** V naročniški pogodbi je jasno zapisano, da je odpravljanje vseh ranljivosti vsaj v obdobju 1 leta vključeno v pogodbeno ceno. V pogodbi je tudi določeno, da ima odpravljanje ranljivosti najvišjo prioriteto. Na ta način so vse pogodbene stranke pred podpisom bolj stimulirane k oceni stroškov napak.	0

2. Varnostne zahteve

Točk: 0

Varnostne funkcionalnosti določene	**Kriterij:** Zahtevane varnostne funkcionalnosti so dobro definirane, zadostne in lahko uporabljive. Primeri varnostnih funkcionalnosti so vgrajevanje pametnih kartic, uporaba digitalnih potrdil, biometrija, šifriranje, upravljanje dostopov do podatkov, izdelava varnostnih kopij, anonimizacija ipd.	0
Določene revizijske funkcije	**Kriterij:** V funkcionalnih zahtevah so izrecno zapisane obvezne funkcije beleženja dnevniških zapiskov, sledenje dogodkov, zapis dostopov in spreminjanja podatkov. Še posebej natančno je določena obdelava visoko privilegiranega dostopa ter izjeme.	0
Določeno ciljno varnostno stanje	**Kriterij:** Za vsako podatkovno sredstvo je določen najnižji zahtevan nivo varnosti na podlagi ocene zaupnosti, celovitosti in dostopnosti podatkov ("CIA - Confidentiality, Integrity, Accesibility").	0

3. Varnostna arhitektura

Točk: 0

Varnostni profil	**Kriterij:** Zahtevan je popis ključnih podatkovnih naborov (podatkovnih zbirk, datotek, registrov, sistemskih nastavitev ipd.), aplikacijskih vstopnih in izstopnih točk, komunikacijskih vmesnikov, uporabnikov z dostopi, uporabljenih varnostnih mehanizmov, željenih vgrajenih mehanizmov, integriranih drugih aplikacij ali modulov. Jasno so zapisane varnostne predpostavke.	0
Arhitekturni model groženj	**Kriterij:** Arhitekturni model groženj ("threat model") je popisan, na več nivojih je jasno določen potek podatkov in meje zaupanja, potencialni napadi in grožnje so temeljito dokumentirani in analizirani, pripravljena so drevesa napadov in mitigacije groženj.	0
Določitev in redukcija področja napada ("attack surface")	**Kriterij:** Zahteva se priprava določitve področja napada ("attack surface") - sistematična analiza vseh potencialnih točk napada ter pregled vseh aplikacijskih in integracijskih vmesnikov. Pričakuje se omejitev področja napada na čim manj vmesniških mest ter izdelava seznama kategoriziranih potencialnih groženj in napadov (recimo po modelu "STRIDE - Spoofing, Tampering, Repudiation, Information disclosure, DOS, Elevation of privileges").	0

4. Varnostno preverjanje — Točk: 0

Avtomatsko varnostno preverjanje	**Kriterij:** Določeno je, da se izvaja avtomatsko testiranje po metodi "black box" ali da se uporabljajo orodja za avtomatsko iskanje ranljivosti (statična ali dinamična, penetracijski preizkusi). Po vsakem avtomatskem preverjanju je nujno obvezno ročno analiziranje rezultatov.	0
Ročno varnostno preverjanje	**Kriterij:** Avtomatska orodja najdejo predvsem znane in preproste oblike ranljivosti, ne pa tudi logičnih napak, bolj zapletenih izvedb znanih ranljivosti ter novih vrst ranljivosti. Zato je priporočljivo izvajati ročno varnostno "black box" preverjanje in ročno varnostno preverjanje kode.	0
Neodvisne poglobljene simulacije napadov	**Kriterij:** Izvajajo se simulacije napadov usposobljenih napadalcev z namenom doseganja določenih varnostnih ciljev. Izvajajo se neodvisni preizkusi znanih vrst napadov, sistematično preverjanje znanih ranljivosti, preizkusi napadov po drevesu napadov, aplikacijsko značilni napadi, okoljsko specifični napadi ipd. Način izvajanja preizkusov je predvsem negativno varnostno testiranje.	0

5. Ljudje — Točk: 0

Projektni člani varnostno usposobljeni	**Kriterij:** Vsi člani razvojne ekipe so uspešno opravili splošna usposabljanja za varno delo z računalnikom in izobraževanje redno obnavljajo.	0
Varnostno usposobljene skupine	**Kriterij:** Posamezne skupine sodelujočih dokazujejo potrebna specialistična znanja s področja informacijske varnosti. Razvijalci in arhitekti se izobražujejo na področju varnega kodiranja, arhitekti poznajo model groženj, preizkuševalci se izobražujejo na področju iskanja znanih ranljivosti ipd.	0
Sodelovanje neodvisnega zunanjega strokovnjaka za aplikacijsko varnost	**Kriterij:** Pri vseh fazah projekta sodeluje strokovnjak za aplikacijsko varnost, ki ni član razvojne ekipe. Njegova vloga je skrb za stalno opozarjanje na varnostne grožnje v aplikaciji.	0

6. Varno kodiranje — Točk: 0

Uporaba razvijalskih avtomatskih orodij	**Kriterij:** V času razvoja je zahtevana uporaba razvijalskih orodij za nadzor posameznih modulov ali enot, s katerimi se odkriva tok napačnih podatkov. Gre za avtomatsko higienično preizkušanje v času razvoja z uporabo znanih razvijalskih orodij - stresnega testiranja ("fuzzing testing"), preizkušanja posemaznih modulov ("unit testing"), uporaba orodij za nadzor pomnilnika ipd.	0
Varno kodiranje	**Kriterij:** Razvijalci obvladujejo osnove varnega kodiranja (izobraževanje, izkušnje) in se znajo v večini primerov izogniti TOP lestvicam ranljivosti (OWASP, WASC, SANS ipd.).	0
Načela varnega kodiranja	**Kriterij:** Razvojne ekipe se dosledno držijo uporabe stabilnih, varnostno preizkušenih knjižnic ter pišejo kodo po lastnih načelih varnega kodiranja ("secure coding guidelines").	0

7. Preverjanje varnostnih funkcij — Točk: 0

Načrtovano testiranje varnostnih funkcionalnosti	**Kriterij:** Načrt preizkušanja funkcionalnosti vsebuje obvezno preverjenje delovanja varnostnih funkcij, pa tudi preverjanje delovanja revizijskih funkcionalnosti.	0
Regresijsko testiranje varnostnih funkcionalnosti	**Kriterij:** Po vsaki večji spremembi izdelka se zahteva uspešna izvedba regresijskega testiranja varnostnih in revizijskih funkcij, ročna ali avtomatizirana.	0
Izkušeni etični hekerji	**Kriterij:** Varnostne funkcionalnosti in ranljivosti iščejo izkušeni varnostni strokovnjaki z napadalsko mentaliteto, ki so se v preteklosti že potrdili v iskanju ranljivosti. Preizkušanje varnosti ni naloga za začetnike ali razvijalce, ki ne razumejo napadalske mentalitete.	0

8. Ključne ranljivosti — Točk: 0

Iskanje TOP ranljivosti	**Kriterij:** Sistematično iskanje in odpravljanje TOP ranljivosti (recimo OWASP, WASC, SANS/CWE TOP ipd.) ter znane ranljivosti in upoštevanje groženj v aplikacijah in modulih, ki jih integriramo. Zahtevano je dosledno verificiranje popravkov.	0
Iskanje kompleksnih ranljivosti	**Kriterij:** Iskanje in odpravljanje ranljivosti ter verificiranje popravkov logičnih, kompleksnih in sofisticiranih ranljivosti. Spremljanje novih vrst napadov in napak.	0
Vrednotenje ranljivosti	**Kriterij:** Zahtevano je ločevanje ranljivosti od drugih funkcionalnih napak in vrednotenje napak s stališča varnostnih posledic, klasificiranje ranljivosti po varnostnih parametrih ter vodenje evidence ranljivosti po splošnih (CVSS, CWE ipd.) ali lastnih klasifikacijah.	0

9. Metrike — Točk: 0

Preverjanje usklajenosti varnostnih zahtev glede na zakonodajo	**Kriterij:** V sprejemnih testiranjih je zahteva po preverjanju usklajenosti z zakonodajo, ki zagotavlja varnost in zasebnost (ZEPEP, ZVOP). V sprejemnih testiranjih je zahteva po preverjanju usklajenosti s splošnimi varnostnimi standardi (kot recimo PCI DSS).	0
Uporaba procesnih metrik	**Kriterij:** Za posamezne aktivnosti, povezane z varnostnimi zahtevami, je zahtevano evidentiranje porabljenega časa in sredstev. Uporabljajo se prilagojene metrike, kot so "sDAR" (security Defect Arrival Rate), "sDD" (security Defect Density), krivulja odkrivanja ranljivosti ipd.	0
Uporaba lastnih varnostnih aplikacijskih metrik	**Kriterij:** Varnostne metrike in njihove željene ciljne vrednosti so določene hkrati z osnovnimi varnostnimi zahtevami.	0

10. Varnostni standardi in prakse — Točk: 0

Splošni varnostni standardi	**Kriterij:** Zahteva se upoštevanje splošnih informacijsko-varnostnih standardov (ISO 2700x, COBIT, PCI DSS, SANS CAG ipd.). Čeprav splošni varnostni standardi ne dajejo jasnih napotkov za gradnjo varnih aplikacij, pomagajo dvigovati varnostno zavest sodelujočih.	0
Zrelostni aplikacijsko-varnostni modeli	**Kriterij:** Zahteva se upoštevanje zrelostnih aplikacijskih varnostnih standardov, kot so OWASP Open SAMM, BSIMM ipd.	0
Aplikacijski varnostni standardi in prakse	**Kriterij:** Zahteva se upoštevanje specializiranih aplikacijsko-varnostnih standardov, modelov in dobrih praks, kot so OWASP ASVS, ISO 15408, Microsoft SDL ipd, pa tudi lastnih ali branžnih pravilnikov s področja varne gradnje programske opreme (zdravstveni aplikacijski varnostno-informacijski standardi ipd.).	0

[i] Povzetek ocene CANV
[ii] Seštevek obteženih točk po posameznih aktivnostih področja