PROJEKTS

Koksnes plūsmas IT komunikācijas platformas drošības (ielaušanās) testu darba uzdevums

VKP IT darba grupa 18.03.2019

- *Tīmekļa lietotne (webapplication) – drošības testēšana jāveic atbilstoši OWASP (OpenWebApplicationSecurityProject) testēšanas vadlīnijām*
- *Tīmekļapakalpes(webservices) - drošības testēšana jāveic atbilstoši OWASP (OpenWebApplicationSecurityProject) testēšanas vadlīnijām*
- *Mobilā lietotne – drošības testēšana jāveic atbilstoši mobilo lietotņu izstrādes vadlīnijām (OWASP Top 10 Mobile controls)*
- *Konfigurācijas pārbaudes – atbilstoši ražotāja rekomendācijām, drošības standartiem un labajai praksei. Ja ir kompetents izstrādātājs un administrators, tad var neveikt*
- *Datu apstrādes novērtējums- atbilstoši Vispārīgās datu aizsardzības regulas Nr.2016/679 (GDPR) un Latvijas Republikas normatīvo aktu prasībām*

Pretendenta apraksts Projekta vadības grupas izpratnē ir ticis komunicēts kā:

- *Pretendents– pieredze informācijas sistēmu drošības pārbaužu (ielaušanās testu) veikšanā vismaz 5 projektos, kur veiktas vismaz 20 pārbaudes (pa pārbaudes jomām).*
- *Personāls– sertificēts vienā vai vairākās šādās kompetencēs (atkarībā no izvēlētām jomām) :*
    - *Ētiskais hakeris - CEH (Certified ethical hacker) vai OSCP (Offensive Security Certified Professional) sertifikāts.*
    - *Informācijas drošības speciālists - CISSP (Certified Information System Security Professional) sertifikāts.*
    - *Informācijas sistēmu auditors - CISA (Certified Information Systems Auditor) sertifikāts.*

Līdz 18.martam izteiktie priekšlikumi, apsvērumi un precizējumi:

AUDITA ORGANIZĒŠANA

- **Pretendentam nosūtāmā informācija par Sistēmu**:
    - iepriekš IT darba grupai nosūtītā informācija
    - grafisks attēls (prezentācijas 2.slaids)
    - valoda PHP
    - vajadzību definīcijas dokumentā ir arī drošības un veiktspējas prasības (Sistēmas izstrādes darba uzdevumā)
    - apjoms – vidēji diennaktī ap biznesa 16 000 transakcijas dienā.
    - fiziska serveru/telpas pārbaude nav nepieciešama, jo ir plānots ārpakalpojums
- **Plānotie audita izpildes maksimālie termiņi:**
    - līdz 4 nedēļām
    - ja audits atrod kritiskās ievainojamības, tad, vienojoties par nepieciešamo laiku izstrādei un testiem - pārtestēt.
- **Personāls:**
    - Papildus - sertificēts personas datu aizsardzības speciālists, jo Sistēmā plānota personu datu apstrāde
    - Tā kā šis varētu sadārdzināt audita izmaksas, tad, iespējams, finansu piedāvājumu lūgt gan ar, gan bez GDPR audita.

CITI PRIEKŠLIKUMI

- Riski:
    - paroļu nosūtīšana e-pasta saitēs
    - lietotāju datu bāzes (ne) aktualizēšana
    - datu iekšēja drošība
- Priekšlikums: no kaut kāda informācijas piekļuves līmeņa piekļuve/autorizācija varētu būt ar bankas vai personas ID karti

Mārtiņš Gaigals
papiNet pilotprojekts Latvijā

Tālrunis 29166096
E-pasts martins.gaigals@vmf.lv
www.lkuuv.lv

papiNet