SLUŽBA ZA NABAVO OPREME, MATERIALA IN STORITEV

Oddelek nabave nezdravstvenega materiala in storitev

Ljubljanska ulica 5, 2000 Maribor, Slovenija

Tel.: 02 321 25 59 Faks: 02 321 25 22



**Številka povabila: 21-2022**

**Datum: 26.08.2022**

**POVPRAŠEVANJE**

Spoštovani!

Vabimo vas k oddaji ponudbe za: **Varnostni pregled**

Predmet naročila je podrobneje specificiran v obrazcu.

Rok za sprejem ponudb: 30.08.2022 do 12:00 ure.

Merilo za izbor je najnižja končna vrednost ponudbe v EUR brez DDV.

Pri oblikovanju cene upoštevajte:

* Plačilo: 60 dni od prejema pravilno izstavljenega računa;
* Popuste in rabate;
* Davek na dodatno vrednost (izkazati je potrebno stopnjo in znesek DDV);
* Morebitne druge stroške (npr. prevozne, špediterske, carinske, drobni in vezni material, delo).

Ponudbo lahko pošljete po pošti ali oddate osebno na naslov:

Univerzitetni klinični center Maribor

Služba za nabavo nezdravstvenega materiala in storitev

Ljubljanska ulica 5

2000 Maribor

z oznako na ovojnici: »Ponudba za**: Varnostni pregled**

**(21-2022)**«, s ponudnikovim naslovom na hrbtni strani ovojnice,

ali na e-poštna naslova:

[vesna.fras@ukc-mb.si](mailto:vesna.fras@ukc-mb.si)

[nabava@ukc-mb.si](mailto:nabava@ukc-mb.si)

SLUŽBA ZA NABAVO OPREME, MATERIALA IN STORITEV

Oddelek nabave nezdravstvenega materiala in storitev

Ljubljanska ulica 5, 2000 Maribor, Slovenija

Tel.: 02 321 25 59 Faks: 02 321 25 22



Številka ponudbe: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ponudnik

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Specifikacija

UKC Maribor želi s pomočjo zunanjega neodvisnega izvajalca izvesti varnostni pregled (penetracijski test) zunanje in notranje infrastrukture ter izbranih aplikacij.

Namen je odkriti in preveriti stanje informacijski varnosti interne aplikacije, katero uporablja preko 2000 zaposlenih in preko katere se obvladuje centralna baza podatkov.

Namen je zagotavljati sprejemljivi nivo informacijske varnosti, da bi se pravočasno zaznale varnostne pomanjkljivosti in ranljivosti omrežja, sistemov in storitev, ki utegnejo ogrožati zaupnost, celovitost in razpoložljivost podatkov ter poslovanja ustanove.

Varnostno preverjanje mora biti izvedeno po mednarodno uveljavljenih metodologijah OSSTMM (Open Source Security Testing Methodology Manual), PTES, NIST in CIS Security benhmarks za infrastrukturo ter OWASP za aplikacijsko varnost.

Pri mehanizmih preverjanja in postopkih testiranja mora ponudnik slediti vodilom NIST SP800-115 in standardom ISO/IEC 27001:2013, ISO/IEC 27002:2013, PCI DSS 3.2.1 in ISO/IEC TR 27008:2011.

Rezultati varnostnega pregleda morajo biti strnjeni v poročilu, ki vsebuje podrobnosti vseh izvedenih testov, odkrite morebitne varnostne grožnje in priporočila.

Vsebovati mora najmanj:

-Vodstveni povzetek (»Executive Summary«) podaja povzetek stanja varnosti informacijskega sistema in priporočila za izboljšane stanja.

-Podrobno tehnično poročilo za tehnično osebje vsebuje vse metode in opise testiranj, identificirane varnostne grožnje in priporočila z navodili za odpravo oz. zmanjšanje le-teh.

Rezultate varnostnega pregleda mora ponudnik predstaviti na posebnem sestanku, kjer bo skupaj z naročnikom podrobno pregledal morebitne ugotovljene varnostne pomanjkljivosti in predlagal konkretne rešitve in izboljšave.

Skladno z metodologijo se izvedejo naslednje aktivnosti, ki zagotavljajo celovitost pregleda: (Določitev sistemske varnosti javnega segmenta omrežja.)

• zbiranje javno dostopnih informacij o topologiji omrežja, zunanjem IP naslovnem prostoru, vrstah strežnikov

• pregled usmerjevalnih zapisov, ki vodijo do IP naslovnega prostora

• mrežni pregled zunanjega IP naslovnega prostora in odkrivanje storitev, ki so dostopne z interneta (cca. 13 naslovov IP)

• pregled storitev dostopnih z Interneta z orodji za odkrivanje ranljivosti

• pregled varnosti sistema elektronske pošte (SMTP)

• pregled varnosti DNS strežnikov

• pregled sistema za oddaljeni dostop – VPN

• preverjanje odkritih morebitnih ranljivosti

Glede na specifične storitve stranke se določene teste ustrezno prilagodi.

Varnostni pregled interne aplikacije:

Aplikacija deluje na način Client-server. Na strežniku je »master aplikacija, na delovnih postajah pa samostojno delujoč »client« (Clarion 5.5).

Centralni strežnik je Medis, podatkovni strežnik je MS SQL dodatno je še 7 pomožnih strežnikov. Vsi so MS Windows 2012R2.

Zahtevane aktivnosti:

pregled brez prijave

-Spoznavanje aplikacije (pregled varnostne arhitekture)

-Skeniranje aplikativnih ranljivosti

-Odkrivanje pomanjkljivosti v konfiguraciji

-Avtentikacija uporabnikov

-Preverjanje odkritih aplikativnih ranljivosti

pregled s prijavo

-Varnost in upravljanje seje

-Avtorizacija uporabnikov

-Preverjanje poslovne logike in obvestil o napaki

-Preverjanje veljavnosti podatkov in odpornosti proti vrivanjem po OWASP metodologiji

Ponudnik mora izkazovati ustrezne certifikate za izvedbo testa, in sicer najmanj:

-Certified Information Systems Auditor – CISA

-EC-Council Certified Ethical Hacker – CEH

-PCI DSS QSA

-BSI Training Academy – Information Security Management Systems Auditor/Lead Auditor Training Course (BS ISO/IEC 27001:2013)

-GSEC – GIAC Sercurity Essentials SANS SEC401

-Offensive Security Certified Professional – OSCP

Ponudnik: