Príloha č. 1

k Zmluve o dielo č. DZ332022

Požiadavky na bezpečnostné testovanie, test zraniteľnosti a sociálneho inžinierstva

Cieľom realizácie je preverenie existujúcich bezpečnostných opatrení implementovaných na ochranu infraštruktúry nemocnice. Výsledkom testovania je identifikácia a demonštrácia zraniteľností a nedostatkov s návrhom možných opatrení na ich nápravu v zmysle platnej legislatívy.

Návrhy a výsledok testovania by mal spĺňať legislatívne požiadavky s prihliadnutím ich aplikácie do infraštruktúry a zavedených bezpečnostných opatrení v nemocnici.

Penetračné testovanie a test sociálneho inžinierstva bude v súlade s platnou legislatívou v oblasti kybernetickej bezpečnosti, informačnej bezpečnosti a ochranou osobných údajov.

- Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Vyhláška č. 362/2018 Z.z. Vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Zákon č. 95/2019 Z.z. o informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov
- Vyhláška č. 179/2020 Z.z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Súčasťou testovania je test sociálneho inžinierstva resp. phisingový test odolnosti užívateľov nemocnice, ktorým sa overí znalosť zamestnancov voči emailovým útokom na základe predchádzajúceho interného vzdelávania.

Rozsah infraštruktúry nemocnice:

- 66 pracovných staníc vyžadujúcich správu,
- 34 tlačiarní,
- 4 fyzické servery,
- 2x HyperV server + SAS Storage (Microsoft Failover Cluster)
- 1x HV server (pre sekundárne DC, dohľad a FileShareWitness)
- 12x Virtual Machine (8x Windows2019, 4x Linux)
- Mikrotik GW + 34 WIFI (CapsMan)
- Zálohovanie Altaro
- 7x SWITCH (metalika, optika)
- VPN štátna pokladnica
- VPN pre homeoffice
- Ostatné bezpečnostné prvky

Minimálne požiadavky na rozsah prác

1. Vykonanie iniciálneho testu zraniteľnosti alebo penetračný test, vrátane preverenia bezpečnosti konfigurácie wifi sietí - Posúdenie implementovaných bezpečnostných opatrení, - vykonanie bezpečnostného testovania (testovanie zraniteľností, penetračné testovanie), - zahŕňa všetky serverové komponenty, - bezpečnostný audit konfigurácie servera a jeho komponentov (konfiguračné parametre poskytnuté pri realizácii testovania), - vylúčenie postupov, ktoré by mohli narušiť funkčnosť a prevádzku nemocničných procesov, - zhodnotenie bezpečnosti, popis vykonaných testov a ich výsledkov, - zhodnotenie zistení a odporúčania na nápravu, prezentácia výsledkov v priestoroch obstarávateľa.
2. Test sociálneho inžinierstva - Praktický test odolnosti užívateľov (cca 90 užívateľov), - emailové testovanie užívateľov simulovaným malvérom napr. v prílohe emailu, - zhodnotenie testovania a ich výsledku, - prezentácia výsledkov v priestoroch obstarávateľa