VIAVIS střežíme podstatné

[redacted]
vedoucí samostatného oddělení bezpečnosti ICT

Česká průmyslová zdravotní pojišťovna
Úsek strategie
Čermákova 1951, 272 01 Kladno

V Ostravě 9. 7. 2020

Věc: Nabídka provedení interního penetračního testu

společnost VIAVIS a.s. si váží vašeho zájmu o vypracování této nabídky. Při jednání bylo dohodnuto, že předložíme nabídku na **provedení interního penetračního testu ICT**.

Testování bude provedeno dle metodik OSSTMM (Open-Source Security Testing Methodology Manuál), OWASP (OWASP (Open Web Application Security Project) a Web Application Security Consortium Thread Classification.

- Testy budou nedestruktivní, navíc nesmí omezit běžící služby na serverech, pokud bude proveden test DDoS, pak krátkodobě.
- Po ukončení testování budou odstraněny veškeré stopy po penetračním testování a všechny systémy a kompromitované komponenty budou uvedeny do stavu před testováním.
- Penetrační testování bude kooperativní – tedy ve spolupráci s jednotlivými kontaktními osobami.

Navržené metody a postupy nezvýší bezpečnostní rizika oproti současnému stavu. Dále nezpůsobí nestabilitu prostředí, která by způsobila významné potíže zaměstnancům s užíváním informačních systémů. Tento požadavek bude zohledněn tak, že:

- prověření bezpečnosti proběhne v dohodnutou dobu tak, aby byly minimalizovány případné dopady např. mimo obvyklou pracovní dobu,
- v rámci přípravy bude vytvořen plán k prověření bezpečnosti penetračních testů. Realizátor prověření bezpečnosti vždy dopředu oznámí pověřené osobě zadavatele

čas a charakter testování tak, aby v případě nestability systému mohl zadavatel včas zorganizovat řešení,

- veškeré agresivní testy budou předem konzultovány se zadavatelem.

Interní penetrační testy budou prováděny z prostředí interní LAN sítě lokálně v prostředí ČPZP, tj. bude simulováno počínání potencionálního útočníka pokoušejícího se o průnik z vnitřní sítě. Jejich cílem je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu interní sítě, kde se dá předpokládat nižší úroveň zabezpečení.

Interní penetrační testy budou částečně kopírovat externí testy pro interní datovou síť a dále budou zaměřeny na:

- odposlech komunikace se systémem,
- odchycení a přesměrování této komunikace,
- zneužití odchycených informací a komunikace směrem k aplikačním službám (serverům),
- útoky na uživatele systému prostřednictvím tohoto systému,
- přístup k účtům.
- Testů k získání informací a identifikací systémů a aplikací
- Všeobecných testů zranitelnosti
- Testů týkajících se infrastruktury systému
- Testů spolehlivosti a bezpečnosti konfigurace
- Testů existence backdoors
- Testů autentizace a schémat pro kontrolu přístupu
- Testů routerů a switchů
- Kontroly operačních systémů
- Testů aplikačních chyb a vad v systémech a aplikacích
- Testů nedostatečného zabezpečení

- Testování slabých míst zahrnující body selhání s cílem způsobit odmítnutí služeb aplikací
- Test kvality autentizačních mechanismů u všech identifikovaných služeb podporujících vzdálené přihlášení.
- Nalezení bezpečnostních děr v aplikacích typu klient-server

Výstupy auditu

Výstupem auditu bude písemný dokument – Zpráva o provedeném auditu bezpečnosti ICT, která bude předána v elektronické formě objednateli a bude zahrnovat zejména:

- popis metodiky penetračního testování a použitých nástrojů,
- podrobný popis průběhu penetračního testování,
- podrobný popis dosažených výsledků, výstupů testů,
- návrh protiopatření k eliminaci identifikovaných zranitelností.

Lokality interních testů

Základní interní penetrační test – Ostrava

WiFi penetrační test – Ostrava nebo Praha nebo Kladno

Termín plnění: do 1 měsíce po obdržení písemné objednávky, případně dle dohody.

Cenová nabídka: **Cena bez DPH 120.000 CZK**

DPH 21 % činí 25.200 CZK

Cena s DPH 145.200 CZK

Nabídka je platná do 31. 08. 2020

Děkujeme Vám za Váš zájem a těšíme se na spolupráci. V případě jakýchkoli dotazů mě, prosím, kontaktujte.

S pozdravem a přáním hezkého dne

[redacted]

VIAVIS střežíme podstatné

Obránců Míru 237/35, 703 00 Ostrava

[redacted]