Příloha č. 5a dokumentace zadávacího řízení na uzavření rámcové dohody

-

Specifikace předmětu plnění

Část 1 - IT bezpečnost a hacking

Předmětem plnění veřejných zakázek zadávaných na základě rámcové dohody v rámci části 1 zadávacího řízení bude **realizace odborných kurzů týkajících se „IT bezpečnosti a hackingu“.**

I. Požadované kurzy:

1. Kurzy týkající se efektivního testování webových aplikací, provádění manuálních i automatických testů bezpečnosti, seznámení s projektem OWASP, s jeho metodikami a volně dostupnými nástroji.

- 2x Testování bezpečnosti webových aplikací (5 dnů)

2. Kurzy zaměřující se na vybudování znalostí implementace bezpečnosti sítí postavených na Windows a Active Directory. (Windows Server 2012, Windows XP, 2003, Vista, 7, 2008, 2008 R2, 8, 2012 i 2012 R2 a síťové technologie, Active Directory, nebo aplikační služby. Požadujeme dosažení znalosti bezpečnostních parametrů technologií jako je Active Directory (AD DS), NTFS, file sharing (SMB) a SMB signing, BitLocker, EFS, Dynamic Access Control (DAC), code signing, základy TLS a HTTPS, LDAPS a RDPS, SQL server, nebo IIS.

- 16x Windows Server 2016/2012 – správa bezpečnosti (5 dnů)

3. Kurzy v oblasti webhackingu a zranitelností webových aplikací, metod, pomocí kterých se provádí útoky na webové aplikace a přidružené systémy obrany proti technikám útoků zneužívajících identity koncových uživatelů, útoků vedoucích ke krádeži uložených dat, nebo k defacementu webových stránek, či kompletnímu ovládnutí webového serveru.

- 6x WebHacking v praxi – Zranitelnost webových aplikací (5 dnů)

4. Kurzy v oboru vyšetřování počítačových útoků a zajišťování evidence, shromažďování důkazů pro stíhání útočníků a metody identifikace stop po útočnících v případě napadení firmy kybernetickým útokem, ať už se jedná o hromadný útok či ojedinělé napadení konkrétní oběti.

- 4x Computer Hacking Forensic Investigator (5 dnů)

5. Kurz zabývající se základními nástroji a principy, které se používají pro útoky a penetrační testování, metodami, pomocí kterých se provádí útoky na počítačové sítě a serverové systémy z vnitřní části sítě a při útocích Man-in-the-Middle proti klientům mimo vnitřní síť.

- 8x Network Security – Hacking v praxi (5 dnů)

6. Kurz zaměřený na techniky hackingu, jako jsou pokročilá enumerace a skenování sítí či systémů v celopodnikovém rozsahu, tvorba malwaru a trojských koňů, pokročilé síťové útoky eliminující omezení VLAN a jiné techniky, testování webových serverů a aplikací, SQL Injection či hackování mobilních platforem.

- 8x Certified Ethical Hacker v9 (5 dnů)

7. Kurzy věnující se pokročilejším technologiím pro ochranu počítačových sítí na různých úrovních, implementování systému pro detekci průniku IDS/IPS (Intrusion Detection System/Intrusion Prevention System), implementování honeypotu k odhalení a analýzovaní útoků v jejich velmi rané fázi.

- 6x Certified Network Defender (5 dnů)

8. Kurzy určené správcům serverů, k zabezpečení serverů a komunikace po síti (Internet), implementování aktivních prvků pro zabezpečení systému jako jsou kontrolory integrity, systémy HIDS a NIDS a používání technologií jako jsou GRSecurity, AppArmor a SELinux.

- 6x UNIX/Linux – bezpečnost, zabezpečení serveru (2 dny)

9. Kurzy pro bezpečnostní IT specialisty, které je seznámí s principy a implementací šifrovacích metod, o principech šifrování a hashů, analýzou jednotlivých šifrovacích a podepisovacích rutin.

- 2x EC-Council Encryption Specialist (3 dny)

10. Kurz zabývající se analytickou stránkou etického hackingu, sestavením finální analýzy a reportingu ze všech nástrojů a technik, rozpoznávání hlavních rizik, navrhování komponentů zabezpečení, zavádění metodik, jejich testování pro co nejúčinnější ochranu před hackery.

- 2x EC-Council Certified Security Analyst (5 dnů)

11. Kurz zaměřený na seznámení se s obsahem norem ISO/IEC 27001 a ISO/IEC 27002 v jejich druhé revizi z roku 2013.

- 6x Windows Server 2016/2012 – audit bezpečnosti podle ČSN/ISO/IEC 27001 a ČSN/ISO/IEC 27002 verze 2013 (4 dny)

12. Kurz zaměřený na běžné uživatele informačních technologií, bezpečné spravování svých dat, domácích počítačů, notebooků a bezdrátových sítí. Kurzy zabývající se bezpečností na Internetu, při běžném využívání sociálních sítí, e-mailových služeb, či online nakupování. Školení ve věci netechnických způsobů hackingu, krádeže identity a triky kapsářů s reálnými ukázkami a případovými studiemi, ve kterých se lidé stali obětí zločinu v reálném či virtuálním světě.

- 4x Certified Secure Computer User (2 dny)

13. Kurzy zaměřené na hackování na platformě Android, na obranu proti technikám útoků zneužívajících zranitelnosti mobilních aplikací, jež mohou vést k úniku důvěrných dat, k obejití autentizace, nebo k plnému ovládnutí mobilního zařízení.

- 14x Bezpečnost a hacking Android aplikací (5 dnů)

14. Přípravný kurz ke zkoušce Certified Information Systems Security Professional (CISSP, ISC2).

- 2x Certified Information Systems Security Professional (5 dnů)

15. Kurz určený správcům síťových serverů zaměřený na zabezpečení dat na serveru, na základy šifrování v oblasti počítačové bezpečnosti, na používání systémů PGP (GnuPG), SSL/TLS, DM-

Crypt.

- 4x UNIX/Linux – bezpečnost dat, bezpečná komunikace, šifrování (1 den)

16. Kurz pro přípravu pro celosvětově uznávanou certifikační zkoušku CompTIA Security+ SY0-301, která je standardem pro IT certifikaci v oblasti bezpečnosti. Školení v oblasti správy bezpečnosti počítačových sítí a operačních systémů na platformě OS Windows. Kurz zaměřený na přehled IT bezpečnostních řešení a implementaci různých bezpečnostních opatření.

- 2x CompTIA Security + (5 dnů)

17. Kurz pro začínající bezpečnostní administrátory, zaměřený na základní přehled o komponentách bezpečnosti, typech útoků, nejčastěji zneužívaných slabinách a hrozby ve vnitřní a vnější části sítě tak, aby zaměstnanci byli schopni vytvořit bezpečnostní pravidla a nasazovat opatření, která chrání informace organizace.

- 6x EC-Council Network Security Administrator (5 dnů)

II. Další požadavky zadavatele:

1. Zadavatel požaduje, aby dodavatel zajistil proškolení zaměstnanců zadavatele i v dalších kurzech týkajících se „IT bezpečnosti a hackingu“ nad rámec výše uvedených kurzů, které v případě potřeby bude zadavatel specifikovat v návaznosti na konkrétní situaci a nové trendy v oblasti IT bezpečnosti a hackingu.
2. Jednotlivé kurzy budou probíhat v českém případně v anglickém jazyce.
3. Zaměstnanec zadavatele účastnící se jednotlivého kurzu obdrží vždy podkladové a studijní materiály ke každému kurzu daného tématu v českém nebo anglickém jazyce, v listinné nebo elektronické podobě.
4. V případě, že jsou jednotlivé kurzy ukončeny udělením certifikátu (pokud k uvedenému kurzu certifikát existuje), obdrží jej všichni účastníci, kteří daný kurz absolvují. Pokud ke kurzu certifikát neexistuje, obdrží účastník osvědčení o absolvování daného kurzu.