Příloha č. 2 – Vymezení kurzů

Školení bude probíhat formou teoretického výkladu s praktickými ukázkami a samostatných cvičení na virtuálních počítačích.

Školení budou přednášet školitelé, kteří disponují příslušným certifikátem pro produkty společnosti Microsoft pro oblasti Administrace Windows serverů a Správa MSSQL serverů.

Hlavní metodou výuky budou přednášky s příklady aplikací v praxi. Každý vzdělávací kurz musí mít prostor pro diskuzi.

Školení bude probíhat v počítačové učebně školitele nebo v mobilním školící učebně školitele v sídle objednatele, přičemž objednatel zajistí místnost, školitel příslušnou ICT techniku.

Školení v sídle školitele bude maximálně do 120 km od sídla zadavatele na území ČR, maximální doba jedné jízdy veřejnou dopravou 2h a maximálně 2 přestupy.

Součástí školení budou tištěné nebo elektronické studijní materiály.

Školení bude na sebe navazovat dle zadaného pořadí u vydefinovaných kurzů a to v oblastech: Administrace Windows serverů, Správa MSSQL serverů a Network Security – Hacking v praxi, přičemž se kurzy nesmějí termínově překrývat.

V ceně školení jsou zahrnuty školící prostory. Školící místnosti musí být určeny ke vzdělávacím aktivitám v IT oblasti, případně by jim měly být uzpůsobeny. To znamená, že by měly být vhodně osvětleny, vybaveny stoly, židlemi a příslušnou ICT technikou.

Účastníkům školení bude umožněno do jednoho roku opětovně zopakovat všechny požadované kurzy (součástí cenové nabídky).

Každý účastník obdrží po skončení vzdělávací aktivity osvědčení o účasti. Dodavatel dodá tato osvědčení také v elektronické podobě.

Na konci vzdělávací aktivity proběhne s účastníky test ověřující pochopení daného tématu (potvrzení o prověření znalostí), dále dodavatel zajistí hodnotící dotazníky.

Veškeré tištěné a elektronické materiály musí splňovat požadované prvky publicity poskytovatele dotace.

1. **Administrace Windows serverů**:
   1. **Windows Server 2016 – správa účtů a prostředků**

- minimálně čtyřdenní školení pro 2 zaměstnance

- školení bude zaměřeno na vytváření a správu uživatelských účtů a skupin v Active Directory, správu prostředků souborového systému NTFS a jeho zabezpečení, sdílení adresářů a správu prostředí pomocí Group Policy.

- kurz bude obsahovat ukázky a postupy dobré praxe při instalaci a správě Windows serveru.

* 1. **Windows Server 2016 – správa bezpečnosti**

- minimálně čtyřdenní školení pro 2 zaměstnance

- školení bude zaměřeno na implementace bezpečnosti sítí postavených na Windows a Active Directory

- kurz bude obsahovat ukázky a postupy dobré praxe pro správu Windows serveru v kontextu bezpečnosti.

* 1. **Windows Server 2016 – Active Directory řešení neobvyklých a kritických situací**

-minimálně čtyřdenní školení pro 2 zaměstnance

- školení bude zaměřeno na správu Active Directory s důrazem na řešení běžných, neobvyklých i kritických situací

* 1. **Windows Server 2016/2012 – audit bezpečnosti podle ČSN/ISO/IEC 27001 a ČSN/ISO/IEC 27002**

-minimálně čtyřdenní školení pro 2 zaměstnance

- školení bude zaměřeno na obsah norem ISO/IEC 27001 a ISO/IEC 27002 v jejich druhé revizi z roku 2013

- bezpečnostní doporučení budou probírána v kontextu a na příkladech bezpečnostních technologií sítí postavených na Windows Server, operačních systémech pracovních stanic Windows

1. **Správa MSSQL serverů**:
   1. **Microsoft SQL Server 2016 - administrace databázového systému**

-minimálně čtyřdenní školení pro 2 zaměstnance

- školení bude zaměřeno na správu MSSQL serveru, zabezpečení přístupu k datům a vysvětlení bezpečnostního modelu SQL Serveru, zálohování databází a jejich obnova, automatizace správy a monitorování provozu SQL Serveru

* 1. **Microsoft SQL Server 2016 – ladění výkonu a optimalizace**

- minimálně třídenní školení pro 2 zaměstnance

- školení bude určeno pro prohloubení znalostí správce MSSQL serveru, kteří jsou zodpovědní za monitoring a optimalizaci výkonu SQL Serveru

1. **Network Security – Hacking v praxi**

-minimálně čtyřdenní školení pro 2 zaměstnance

- školení bude určeno pro administrátory, kteří jsou zodpovědní za bezpečnost počítačových sítí

- školení administrátory seznámí se základními nástroji a principy, které se používají pro kybernetické útoky a penetrační testování a zároveň bude obsahovat příklady dobré praxe jak se útokům bránit a předcházet

**Minimální obsah školení:**

**Ad 1.a) Windows Server 2016 – správa účtů a prostředků**

Školení bude obsahovat:

1. Postupy instalace a základní konfigurace, řešení potíží, konfigurace a správa
2. Detailní představení integrovaných nástrojů pro správu Windows serverů: server Manager, PowerShell, vzdálená správa + RSAT
3. Instalace doménového řadiče a konfigurace
4. Představení Trust domén a Federaci domén
5. Detailní představení objektů v AD a jejich správu jako jsou: uživatelské účty, skupiny, jejich funkce a typy, organizační jednotky
6. Možnosti použití GPO a jejich aplikování, správa GPO objektů, řešení potíží a aplikováním GPO
7. Využití GPO v praxi, aplikování skriptů, mapování síťových disků a tiskáren, instalace software
8. Přehled funkcí DNS serveru, instalace a konfigurace DNS serveru, integrace DNS a AD
9. DHCP server: statická a dynamická konfigurace IP adres, Instalace a konfigurace DHCP serveru DHCP failover a vysoká dostupnost
10. Souborový server a NTFS: řízení přístupu k datům, sdílení adresářů, oprávnění pro sdílen
11. Monitorování, auditování a nástroje pro monitorování výkonu

Školení bude obsahovat praktická cvičení.

**Ad 1.b) Windows Server 2016 – správa bezpečnosti**

Školení bude obsahovat:

1. Vysvětlení principů bezpečnosti Windows serverů
2. Představení uživatelských a servisních účtů, logon session, access token, SID a SID history
3. Představení principů ověřování uživatelů, autentizace pomocí NTLM, Kerberos, SSL certifikátů a čipových karet
4. Představení auditování a sledování přístupu a ověřování
5. Představení multiuživatelské prostředí, identity procesů, identity služeb a IIS AppPoolIdentity, SYSTEM, Network Service a Local Service
6. Představení trust, forest trust, trust účty, selective trust a komplexní prostředí, migrace uživatelů
7. Představení NTFS a Share oprávnění, user rights, Access Based Enumeration (ABE)
8. Představení lokálních skupin, delegace oprávnění pro správu serverů a stanic, delegace v Active Directory
9. Detailní představení Group Policy a Security Policy, software restrictions, password policies
10. Představení Windows Firewall a jeho centrální správa přes Group Policy
11. Představení Dynamic Access Control
12. Představení Active Directory Certificate Services (AD CS), PKI a správa certifikátů a privátních klíčů
13. Představení přístup do sítě a šifrování IPSec a 802.1x
14. Představení TLS/SSL certifikáty a jejich aplikace pro IIS, RDP apod.
15. Detailní představení šifrování BitLocker a EFS a jejich rozdíly, aplikace a zálohování klíčů

Školení bude obsahovat praktická cvičení.

Ad 1.c **Windows Server 2016 – Active Directory řešení neobvyklých a kritických situací**

Školení bude obsahovat příklady dobré praxe, podporované, nepodporované a/nebo nedoporučené scénáře nasazení a kombinace s dalšími rolemi a řešení neobvyklých a kritických situací při správě:

1. Active Directory jako síťová služba
2. LDAP, Kerberos, NTLM, SMB, DCOM a GC rozhraní
3. Východiska designu multimaster replikace
4. Maximální omezení databáze a objektů
5. Forest, domain, trust, trust link, security boundary, global catalog
6. Domain naming master a Schema master
7. Definice typů atributů, vlastní atributy, indexování, časové atributy
8. Atributy bezpečnostních objektů, jako jsou uživatelé, skupiny, počítače, trusty a managed service accounts
9. PDC emulator, RID master a infrastructure master
10. Vyhledávání objektů v LDAP
11. Zabezpečení objektů, řízení a předávání přístupu, delegace, skripty, AdminSDHolder, skryté uživatelské účty
12. Zásady hesel, granulární zásady hesel, identity integration a Forefront Identity Manager
13. Anonymní přístup, simple-bind, testování přístupu a řešení potíží
14. Mazání objektů, tomstone, recycle bin, obnova a reanimation objetů a atributů
15. Klientské interakce, vyhledávání řadičů domény (DC), závislost na parametrech linky
16. RODC, jejich bezpečnost a replikace, klientské vztahy a read/only DNS, RODC v DMZ
17. AD sites, IP rozsahy, optimalizace a řešení problémů při přesunech a výpadcích DC a klientů
18. Nástroje NLTEST, NETDOM, KLIST, NSLOOKUP, DCDIAG, PORTQRY, DFSDIAG
19. Integrace DNS, klienti a DNS, dynamické registrace a jejich bezpečnost, údržba obsahu DNS
20. Optimalizace DNS infrastruktury, její vliv na rychlost startu a konvergenci klientů
21. Principy a detaily replikace, přenosové protokoly, zabezpečení a autentizace
22. Replikace atributů, její problémy a kolize, multimaster a single master replikace, replikace do global catalog (GC)
23. USN rollback, tomstone lifetime (TSL), řešení chybových stavů
24. Plánování rozložení FSMO rolí, distribuce a počty DC, sites, počty a trusty mezi doménami
25. Struktura AD databáze, databázové tabulky, uložení objektů a referencí
26. Zálohování, obnova, práce s databází, shadow copy, autoritativní restore
27. Obnova virtuálních snapshotů/checkpointů a klonování řadičů domény, offline domain join

Školení bude obsahovat praktická cvičení.

**Add 1.d) Windows Server 2016 – audit bezpečnosti podle ČSN/ISO/IEC 27001 a ČSN/ISO/IEC 27002**

Školení bude obsahovat podrobné seznámení s problematikou kybernetické bezpečnosti v kontextu auditu bezpečnosti a příklady dobré praxe pro oblasti:

* Norma ISO/IEC 27001, druhá revize z roku 2013
* Základní články a principy ISO/IEC 27001 (2013)
* ISO/IEC 27001 v kontextu počítačové sítě postavené na Windows a Active Directory
* Norma ISO/IEC 27002, druhá revize z roku 2013
* ISO/IEC 27002 Information Security Policies v kontextu sítí postavených na Windows
* ISO/IEC 27002 Human Resource Security v kontextu sítí postavených na Windows
* ISO/IEC 27002 Asset Management v kontextu sítí postavených na Windows
* ISO/IEC 27002 Access Control v kontextu sítí postavených na Windows
* ISO/IEC 27002 Cryptography v kontextu sítí postavených na Windows
* ISO/IEC 27002 Physical and Environmental Security v kontextu sítí postavených na Windows
* ISO/IEC 27002 Operations Security v kontextu sítí postavených na Windows
* ISO/IEC 27002 Communications Security v kontextu sítí postavených na Windows
* ISO/IEC 27002 System Acquisition, Development and Maintenance v kontextu sítí postavených na Windows
* ISO/IEC 27002 Supplier Relationships v kontextu sítí postavených na Windows
* ISO/IEC 27002 Information Security Incident Management v kontextu sítí postavených na Windows
* ISO/IEC 27002 Information Security Aspects of Business Continuity Management v kontextu sítí postavených na Windows
* Porovnání starší verze 1 normy ISO/IEC 27002 z roku 2005 s aktuální druhou revizí z roku 2013

Školení bude obsahovat praktická cvičení.

**Ad 2.a) Microsoft SQL Server 2016 - administrace databázového systému**

Školení bude obsahovat podrobné seznámení s oblastmi:

* Autentizace a autorizace uživatelů
* Serverové a databázové role
* Autorizace uživatelů při přístupu ke zdrojům
* Ochrana dat šifrováním a možnosti auditu
* SQL Server Recovery Models
* Zálohování databází
* Obnova databází
* Automatizace správy SQL Serveru
* Správa zabezpečení spužby SQL Server Agent
* Monitorování SQL Serveru za použití objektů Alert a notifikací
* Úvod do správy databázového systému použitím PowerShell
* Trasování SQL Serveru
* Monitorování SQL Serveru
* Řešení problémů
* Import a Export dat

Školení bude obsahovat praktická cvičení.

**Ad 2.b) Microsoft SQL Server 2016 – ladění výkonu a optimalizace**

Školení bude obsahovat podrobné seznámení s oblastmi:

* Architektura SQL Serveru, plánování a běh procesů, porovnání rozdílů v běhu procesů ve Windows a v SQL Serveru
* Seznámení s klíčovými parametry ovlivňujícími výkon úložiště dat z pohledu SQL Serveru, přehled různých úložišť dat vhodných pro SQL Server, Konfigurace diskového úložiště s ohledem na výkon SQL Serveru
* Datové struktury
* Paměť SQL Serveru, principy přidělování operační paměti ve Windows, principy hospodaření SQL serveru s operační pamětí, In-memory OLTP
* Souběžný přístup, zámky a transakce
* Indexy a statistiky – význam, optimalizace
* Exekuce dotazů a analýza exekučních plánů
* Cache exekučních plánů a jejich rekompilace
* Extended Events
* Monitorování, trasování a tvorba performance baseline

**Ad 3) Network Security – Hacking v praxi**

Školení bude obsahovat podrobné seznámení s oblastmi:

* Úvod do problematiky kybernetické bezpečnosti
* Odchytávání dat
* Spouštění procesů pod službami a plánovanými úlohami
* Analýza prostředí náchylných k sociálnímu inženýrství
* Skenování síťových služeb pomocí skenování otevřených portů a bannerů
* Analýza používaných operačních systémů
* Princip a aplikování ARP poisioningu pomocí nástrojů pro Microsoft Windows i Linux
* Hesla a jejich prolamování
* Principy ukládání hesel v operačních systémech
* Přenos hesel při síťovém ověřování
* Downgrade ověřovacích metod
* Útoky na hesla hrubou silou pomocí CPU, grafických karet a distribuovaného útoku
* Rainbow Tables - principy vyhledávání, způsob generování pro konkrétní prostředí a druhy útoků, analýza time/memory tradeoff efektu
* Druhy rámců používaných v bezdrátových sítích
* Analýza bezdrátových sítí v dosahu
* Zneužití neautorizovaných rámců
* WiFi Injection a monitor mód WiFi karet
* Útoky na WEP sítě
* Útoky na WPA1 PSK a WPA2 PSK sítě
* Prolamování EAPOL rámců pomocí grafických karet
* Vetřelecká AP
* WPS
* Pokročilejší útoky
* Zasílání falešných certifikátů, importování kořenových certifikačních autorit a vytváření legitimních falešných certifikátů obcházení HTTPS zabezpečení
* Využití Metasploit Frameworku pro exploitaci síťových služeb
* Skrývání prostředků pomocí rootkitů