**Příloha č. 1: Předmět plnění: Vzdělávání zaměstnanců MMR v oblasti kybernetické bezpečnosti**

Projekt Kyberbezpečnost MMR (Reg. č. projektu: CZ.03.4.74/0.0/0.0/15\_025/0011813), v jehož rámci je tato veřejná zakázka realizována.

Realizace této zakázky se předpokládá v období do 14 dnů ode dne nabytí účinnosti smlouvy do 31. 5. 2022 (předpokládaný termín). *Pozn. 3 etapy s ohledem na realizaci dílčích školení (1. etapa  - do 14 dnů ode dne nabytí účinnosti smlouvy do 31. 12. 2020; 2. etapa – od 1. 1. 2021 do 31. 12. 2021; 3. etapa – od 1. 1. 2022 do 31. 5. 2022). Etapy je možné přenastavit pouze na základě řádného zdůvodnění a schválení obou smluvních stran.*

První školení jsou zaměřena obecně na kybernetickou bezpečnost, tj. určena pro větší počet zaměstnanců Ministerstva pro místní rozvoj (dále jen „MMR“) - ke dni 26. 9. 2019 je počet zaměstnanců MMR 691 – může se měnit v průběhu projektu s ohledem na systemizaci.

Druhý typ školení je určen pro profesionály v IT oblasti a pro management ministerstva.

1. **Rozšiřující vzdělávací program kybernetické a informační bezpečnosti pro zaměstnance MMR**

Jedná se o rozšiřující vzdělávání v oblasti kybernetické bezpečnosti určené pro všechny zaměstnance MMR – cca 700 osob. Každý zaměstnanec absolvoval e-learningové vstupní vzdělávání (bude poskytnuto), a absolvuje také e-learnigový kurz „Dávej kyber“ poskytovaný Institutem pro veřejnou správu (<https://www.institutpraha.cz/kurzy/kyberneticka-bezpecnost/>). Rozšiřující vzdělávací program se zaměří na praktické znalosti v rámci KB a bude rozšiřovat a doplňovat již absolvované.

Program bude mít e-learningovou (cca 5 hodin) a praktickou přednáškovou část (cca 7 hodin) a bude rozdělen do dvou navazujících kursů (první e-learning cca 2 hod, první přednáška 3,5 hod, druhý e-learning 3 hod, druhá přednáška 3,5 hod). Cílem programu bude zejména zvýšení povědomí o kybernetických rizicích standardního užívání informačních technologií (nastavení hesel, bezpečnost e-mailu, hacking, rizika defaultních hesel, sledovatelnost/pseudonymita/anonymita, rizika spojená s infikovanými stránkami, malwarové útoky, social engineering přes mail a telefon). V rámci e-learningové části budou témata představena a teorie s nimi související vysvětlena, přednášky následně předvedou probrané v praxi (ukázka brute force attacku a slovníkových útoků na hesla, ukázka útoku na wi-fi včetně evil twin, MiM útoky, ukázka útoku přes web (beef apod.), exploit kity, tracking cookies, vysvětlení automatického trackingu v rámci OS, internet nezapomíná atd.)

Přesný obsah e-learningu a přednášek bude ve výše definovaném rozsahu vzájemně odsouhlasen s objednatelem.

|  |  |  |  |
| --- | --- | --- | --- |
| **Rozšiřující VP KB** | **Počet účastníků**  | **Obsah** | **Časová náročnost** |
| **E-learning I.** | cca700 (10 běhů pro cca 100 účastníků)  | Kyberzločin, antiviry, veřejnost internetu/anonymita, tracking, dark net, hesla, wi-fi hacking,  | 2 hod. |
| **Prezentace I.** | cca 700 (10 běhů pro cca 100 účastníků) | ukázka darknetového tržiště, nodistribute (virustotal), tracking cookies, spyware, brute force attack a slovníkový útok na hesla, ukázka útoku na wi-fi včetně evil twin, MiM útoky | 3,5 hod. |
| **E-learning II.** | cca 700 (10 běhů pro cca 100 účastníků) | Malware, social engineering přes mail a telefon, webové útoky  | 3 hod. |
| **Prezentace II.** | cca 700 (10 běhů pro cca 100 účastníků) | Exploit kity, Metasploit apod., Maltego, praktická ukázka maskování malware, webové útoky (BeEF apod.) | 3,5 hod. |

1. **Odborný vzdělávací program kybernetické a informační bezpečnosti**

50 absolventů rozšiřujícího kurzu (představení a vytipovaní zaměstnanci s odborným zaměřením na IT, KII systémy, bezpečnost apod.) se budou dále vzdělávat na roční periodické bázi.

Půjde o jeden odborný e-learning (cca 5 hod.) v každé etapě, následovaný workshopem (v místnosti s výpočetní technikou a zapojením účastníků) v rozsahu cca 5 hodin. V rámci workshopu budou účastníci skutečně prakticky používat hackerské nástroje a prakticky testovat jednotlivé typy útoků a exploitů. Předpokládáme využití virtuálních strojů s Kali Linux a Metasploitable atp. Každoročně se uskuteční minimálně šest termínů workshopu, každý pro maximálně 12 účastníků.

|  |  |  |  |
| --- | --- | --- | --- |
| **Odborný VP KB** | **Počet účastníků**  | **Obsah** | **Časová náročnost** |
| **E-learning a workshop 1** | cca 50 (šest běhů po max. 12 účastnících) | Trendy v  kyberbezpečnosti, Packet sniffing, útoky na wi-fi (WEP a WPA cracking), hesla, MiM, síťové útoky, zranitelnosti | 5 hod. + 5 hod. |
| **E-learning a workshop 2** | cca 50 (šest běhů po max. 12 účastnících) | Trendy v kyberbezpečnosti, Webové útoky, firewall, social engineering - Veil, Fat Rat, Empire atp.,  | 5 hod. + 5 hod. |
| **E-learning a workshop 3** | cca 50 (šest běhů po max. 12 účastnících) | Trendy v kyberbezpečnosti, Social engineering přes infikované stránky BeEF atp. základy tvorby trojanů | 5 hod. + 5 hod. |

Popsaný obsah je spíše návrhem směřování vzdělávání - přesný obsah e-learningu a workshopu bude vždy na příští rok ve výše definovaném rozsahu vzájemně odsouhlasen s objednatelem. Smyslem programu je zejména upozornit účastníky na snadnost s jakou je dnes možné v kyberprostoru zaútočit a na jednoduchost dostupných nástrojů.

1. **Vzdělávací program pro IT profesionály**

12 vybraných odborných zaměstnanců MMR (IT specialistů), 3 dny v každé etapě (2 dny první kurz + 1 den druhý kurz). Rozdělení na dvě skupiny, IT specialisté sítí (6 osob) a IT specialisté koncových zařízení (6 osob).

1. **IT specialisté sítí**

Odborné vzdělávání týkající se trendů v bezpečnosti sítí, architektury a nástrojů pro jejich správu. Klasické příznaky, že je síť kompromitována. Při napadení obvykle používané porty a protokoly. Varovné příznaky. Sandboxing, VPN, miskonfigurace sítě, síťové zranitelnosti, dobré praxe, nastavení firewallu a IPS (SIEM), honeypoty, tvorba snort pravidel, Nmap, Wireshark atp.

1. **IT specialisté koncových zařízení**

Odborné vzdělávání týkající se trendů pro koncová zařízení včetně mobilních. Antiviry, antimalware, sandboxing, virtualizace (včetně třeba Qubes), živé OS, šifrování, aplikace, aplikační zranitelnosti, známé slabiny, OS. Virustotal a jeho použití, základy analýzy škodlivého kódu. Základy pravidel pro antimalwarovou heuristiku (packery atd.), Tor.

Popsaný obsah je spíše návrhem směřování vzdělávání. Zhotovitel může zajistit tento program buď prostřednictvím dvou dvoudenních kursů (jedním pro každou skupinu), nebo poskytnutím seznamu jím poskytovaných kursů v dané oblasti (alespoň tři různé kursy ročně), ze kterých si IT profesionálové vyberou dva jednodenní, nebo jeden dvoudenní kurs ročně. V případě plněním formou dvoudenního kursu na míru, bude jeho obsah předem na každou etapu odsouhlasen objednatelem.

Zbylý jednodenní kurs (praxe) bude pro každou skupinu v rámci etapy sestaven z témat a otázek, které budou zaslány Zhotoviteli objednatelem (otázky z praxe, nebo zajímající IT profesionály). Lektor Zhotovitele na základě zaslaných otázek zpracuje presentaci a tu poté pro danou skupinu odpresentuje a rozebere v prostorách objednatele.

|  |  |  |  |
| --- | --- | --- | --- |
| **Odborné vzdělání IT**  | **Počet účastníků**  | **Obsah** | **Časová náročnost** |
| **IT specialisté sítí** | 6 | dle výběru ze seznamu, nebo KB sítí | 2 dny v každé ze tří etap |
| **IT specialisté koncových zařízení** | 6 | dle výběru ze seznamu, nebo KB koncových zařízení | 2 dny v každé ze tří etap |
| **IT specialisté sítí – praxe** | 6 | témata dodaná objednatelem | 1 den v každé ze tří etap |
| **IT specialisté koncových zařízení – praxe** | 6 | témata dodaná objednatelem | 1 den v každé ze tří etap |

1. **Vzdělávací program pro management MMR**

Vzdělávací program pro management se bude týkat dvou základních skupin. A to řídicího managementu KB – což je pět členů ŘVKB a manager kybernetické bezpečnosti, a pak samotného vrcholového managementu ministerstva – 8 náměstků a paní ministryně.

1. **Vrcholový management KB**

Všichni příslušníci managementu KB jsou školeni zároveň v rámci  programu II a někteří i III. V rámci programu IV. se budou v každé ze tří etap po dobu 6 hodin v etapě seznamovat s novými trendy v rámci KB od vývoje kybernetické války (počty zachycení, nové trendy), přes nové malwary a nejzásadnější útoky až po vývoj legislativy v rámci ČR týkající se přímo MMR.

1. **Vrcholový management MMR**

Vrcholový management MMR je nejrizikovější skupinou z hlediska social engineering útoků a zároveň skupinou chránící nejcennější data. 6 hodinový kurs v každé ze tří etap bude určen ke zvýšení uvědomění si rizika a také základních technik bezpečného používání nástrojů IT.

Vrcholovému managementu budou odprezentována témata jako anonymita na internetu, logování, tracking (od cookies až po hardwarovou identifikaci), spyware, APT, Tor a darknet, Tails, Qubes, anonymizační webové služby, VPN. Cílem je dosáhnout stavu, kdy si bude každý proškolený plně uvědmovat co to znamená pohybovat se v kyberprostoru a zároveň bude mít základní vědomosti o tom, jak si počínat co nejnenápadněji.

|  |  |  |  |
| --- | --- | --- | --- |
| **Vzdělání managementu** | **Počet účastníků**  | **Obsah** | **Časová náročnost** |
| **Vrcholový management KB** | 6 | Trendy v oblasti KB, svět a ČR, nejvýznamnější události a vývoj | 6 hodin v každé ze tří etap |
| **Vrcholový management MMR** | 9 | Sledovatelnost včetně možností APT a velkých hráčů, anonymita v kyberprostoru, VPN, darknet, bezpečné OS,  | 6 hodin v každé ze tří etap |

1. **Praktický trénink**

Praktický trénink v rámci systému MMR. Detekce různých druhů kybernetických útoků a jejich komplexního zvládnutí – přesný obsah tohoto typu vzdělávání bude vždy předem dohodnut se objednatelem. Prakticky vždy půjde o simulovaný kybernetický útok (ať už penetračním testováním, nebo social engineeringem, na zakázku vytvořený „malware“) a následně sledování odezvy a nápravná opatření. Z každého tréninku bude lektorem kursu vypracována zpráva o průběhu a výsledcích a zjištění a doporučení.

Typy útoků a testů budou vždy předem odsouhlaseny v závislosti na systému MMR. Zaměření bude zejména na social engineering útoky – od pokusů o nakažení kódem pomocí USB, přes phishingové kampaně až po spear phishing.

Ročně lze počítat se 3 útoky – praktického kurzu se účastní 15 vybraných zaměstnanců ze skupin Vrcholový management KB a specialisté IT. Rozsah praktického tréninku je cca 3 plné dny v každé ze tří etap pro zúčastněné zaměstnance.

**Obecné požadavky**

Ukončení školení v rámci projektu

Znalosti účastníků školení typu I. a II. budou ověřeny v rámci e-learningu na začátku a na konci, aby mohl být zdokladován jejich pokrok. Za účastníky školení typu III. a IV. vytvoří zhotovitel závěrečnou zprávu o jejich pokroku a zlepšení.

Zhotovitel vyhotoví osvědčení o absolvování příslušných školení pro jednotlivé účastníky. Konkrétní podoba osvědčení bude odsouhlasena objednatelem.

Prostory

Typ školení č. I bude realizováno v prostorách objednatele - AVI (Akademie veřejného investování) Pařížská 4, Praha 1. Typ školení II bude realizován v rámci prostor objednatele – ve specializované učebně. Třetí a čtvrtý typ školení bude probíhat v prostorách, které zajistí Zhotovitel, pátý na pracovišti objednatele.

Prostory zajištěné Zhotovitelem budou

1. Dostupné hromadnou dopravou od sídla Objednatele do 45 min, nebo v docházkové pětiminutové vzdálenosti od stanice metra.

2) Přiměřeně velké (minimálně 4m2 na jednu osobu účastnící se školení, minimální výška místnosti 2,7m), vzdušné a odhlučněné,

3) Naplňující veškeré požadavky BOZP a PO

4) Vybavené počítačovou technikou umožňující demonstrace probíraných kybernetických událostí a útoků (propojená bezpečná síť umožňující praktické ukázky útoků na místě)

5) Vybavené nástroji pro presentaci (projektor, plátno, tabule) a při každé presentaci také vytištěnými kopiemi presentované látky umožňující si přímo do nich dělat poznámky.

Veškerá školení, podkladové materiály i e-learning budou dodány v českém jazyce.

Konkrétní termíny realizace jednotlivých běhů školení budou dohodnuty mezi Zhotovitelem a objednatelem s dostatečným předstihem (minimálně 21 dnů před konáním školení), a to prokazatelným způsobem, např. e-mailem, zápisem z jednání apod.

**Technická kritéria na e-learning**

Technické požadavky na zpracování kurzu:

* Elektronický kurz a test musí plně odpovídat normě SCORM 1.2 či 2004 a musí být plně kompatibilní se stávajícím LMS objednatele (SharePoint LMS).
* Výukové materiály musí být kvůli správnému zobrazení vytvořeny ve velikosti cca 1000 x 660 pixelů.
* Kurz se musí správně zobrazovat v prohlížečích verze Microsoft IE 11, Microsoft Edge 40, Mozila Firefox 65 a novějších.
* Jeden SCORM balíček musí obsahovat vždy jednu lekci kurzu v podobě vícestránkového SCO (Single-SCO).
* Kurzy musí být dodávány ve formátu SCORM ve variantě s vlastním přehrávačem. Navigace v kurzu musí být zajištěna tlačítky v těle kurzu (zobrazení obsahu a struktury stránek dle definice v souboru imsmanifest.xml SCORM balíčku není podporováno).
* Lekce výkladové a lekce testová musí být odděleny (závěrečný test musí být samostatnou lekcí).
* Dělení kurzu na menší celky - kapitoly (lekce elektronického kurzu) a snímky (stránka či stránky elektronického kurzu).
* Kurz bude obsahovat průběžné kvízové otázky, dle nichž si bude moci uživatel ihned ověřit pochopení vykládané látky. V závěru každé lekce a celého kurzu bude  umístěn komplexní test z celé sekce.
* Součástí kurzu bude certifikát dostupný z LMS po úspěšném ukončení studia.
* Certifikát kurzu musí být navržen tak, aby jej bylo možné vytisknout na standardní tiskárně formátu A4.
* Certifikát nesmí být součástí kurzu (SCORM balíčku). Certifikát bude definován na úrovni LMS, a to formou HTML definice.
* Kurz má jednotnou koncepci obdobnou jako stávající kurzy (tlačítka Další a Předchozí pro listování mezi stránkami a tlačítka pro aktivaci specifických komponent - zobrazení rejstříku, slovníku, nápovědy, okna obsahu, zobrazení pozice v kurzu a další) a jeho grafický návrh bude předložen objednateli k akceptaci

**Specifika ukončení kurzu v LMS:**

* Výukový materiál či test bude korektně uzavřen tehdy, jsou-li splněny podmínky průchodu kurzem či testem (nutnost navštívení všech stránek, splnění testu apod.).
* Uzavření kurzu bude prováděno klepnutím na tlačítko, jehož stiskem uživatel stvrdí, že lekci prošel a porozuměl jí. Pokud budou zároveň splněny další podmínky (kupříkladu je dosaženo požadovaného skóre), bude lekce označena za dokončenou.
* Stiskem tlačítka „Zavřít“  musí dojít k zapsání následujících informací do LMS:
	+ Stav lekce (dle splnění podmínek v průběhu studia) – proměnná AICC\_Lesson\_Status
	+ Získané bodové skóre – proměnná AICC\_SCORE
	+ Uzavření a odevzdání úlohy v SharePoint LMS (uzavření okna spuštěné lekce a označení úlohy za dokončenou)
* Pokud uživatel úlohu příslušným tlačítkem neukončí, ale pouze zavře, je to považováno za přerušení studia, nikoliv za uzavření celé úlohy. V tomto případě není stav lekce aktualizován na „dokončeno“.

**Další požadavky:**

* Zhotovitel zajistí aktualizaci kurzu v případě vydání nových zákonů či vyhlášek v oblasti kybernetické bezpečnosti. Aktualizace výukových materiálů nesmí mít dopad na dosavadní výsledky studia, tj. v případě aktualizace musí být dodán SCORM balíček ve stejné struktuře. Zejména v případě testů musí být zachován způsob bodování a vyhodnocení.
* Zhotovitel poskytne součinnost při importu kurzu do stávajícího systému LMS objednatele a jeho odladění.
* Správu kurzu (import SCORM balíčku, přiřazení kurzu uživatelům, export výsledků studia apod.) v LMS bude provádět MMR.
* Licence bude minimálně pro celkem 1000 uživatelů, kteří budou přistupovat na dva shodné, ale oddělené LMS objednatele.