Projekt FR CESNET č. 644/2019

Školení IT bezpečnosti

oblast I. / okruh A.

Závěrečná zpráva projektu

Vítězslav Grygar, Jakub Kalnik, Adrian Kapias

Vysoká škola báňská - Technická univerzita Ostrava

Centrum informačních služeb, útvar Centrum informačních technologií

1. 7. 2020

Obsah

Způsob řešení

V rámci projektu byly aktualizovány a rozšířeny stávající podklady pro školení IT bezpečnosti po teoretické stránce. Podklady se věnují následujícím oblastem:

- *malware* - způsob šíření, schopnosti, obrana,
- *sociální inženýrství* - typické způsoby, varovné příznaky, postupy pro ověřování totožnosti, statutu a potřeby informace,
- *phishing* - varovné příznaky, elektronické podpisy,
- *webové stránky* - certifikáty, čtení URL adresy,
- *Wi-Fi sítě* - problematika veřejné Wifi, eduroam,
- *fyzická bezpečnost* - typické vektory útoku,
- *práce s hesly* - tvorba silných hesel, ukládání hesel,
- *zálohování* - proč zálohovat, kam zálohovat,
- *životní situace* - konkrétní postupy řešení problémů specifické pro VŠB-TU Ostrava.

Na konci každé kapitoly jsou nejdůležitější poznatky vždy shrnuty do několika bodů pro snadný a rychlý přístup.

Některá z uvedených témat je vhodné účastníkům kurzů demonstrovat prakticky, proto vznikly nové podklady pro výuku následujících oblastí:

- *práce s hesly* - demonstrace silných hesel, instalace a manipulace se správcem hesel,
- *šifrování* - dokumenty MS Office, ZIP archivy, VeraCrypt,
- *elektronický podpis* - žádost, nastavení klienta, aplikace podpisu a šifrování,
- *ochrana zařízení* - aktualizace, firewall, antivirový software, online scannery,
- *VPN* - konfigurace připojení,
- *anonymizace dat* - odstranění citlivých metadat v MS Windows.

Dosažené cíle

Byl vytvořen komunikační modul SAP – LMS Moodle, který umožní obousměrnou výměnu dat v rozsahu nezbytném pro zajištění požadované integrace na univerzitní e-learningový systém LMS Moodle.
V systému SAP bylo provedeno rozšíření funkcionality zákaznického řešení pro Evidenční systém kvalifikací a vzdělávacích akcí.
Pro účely otevírání nových běhů kurzů v LMS Moodle SAP bude poskytovat informace o personálním složení cílové skupiny pro příslušnou kvalifikaci. Pro účely naplánování periodických opakovacích kurzů v LMS Moodle potom SAP poskytne informace o kvalifikačních deficitech pro danou cílovou kvalifikaci.

Studijní materiály jsou připraveny ve formátu PDF a také v přenosném formátu kurzu pro LMS Moodle. Nabyté znalosti z teoretické části si účastník může ověřit pomocí testu, který je součástí kurzu. Test je prakticky zaměřen a nevyžaduje znalosti definic a přesných postupů. Součástí kurzu je rovněž slovník technických pojmů.

Ve spolupráci s *Centrem celoživotního vzdělávání VŠB-TU Ostrava* bylo uskutečněno šest běhů školení teoretické části. Školení je prozatím dobrovolné a je dostupné pro všechny zaměstnance VŠB-TU Ostrava. Konkrétní dotazy účastníků do velké míry definovaly obsah prakticky zaměřených materiálů a rovněž zdůraznily oblasti, kterým se v teoretické části zpočátku nevěnovala dostatečná pozornost.

Phishingový test

V listopadu 2019 jsme vybrali náhodný vzorek absolventů teoreticky zaměřeného školení a podrobili jsme jej fiktivnímu phishingovému útoku. Cílem tohoto testu bylo určit, zda získané znalosti dávají uživatelům schopnost odhalit i pečlivý cílený útok.

Každému z vybraných uživatelů byla zaslána e-mailová zpráva podobná zprávě, která je zaměstnancům doručována při schválení žádosti o dovolenou. Zpráva byla odeslána bez elektronického podpisu a obsahovala velmi drobné indicie, které účastníkům testu mohly pomoci detekovat probíhající incident.

Odkazy, které se nacházejí v legitimním e-mailu byly nahrazeny odkazy vedoucí na jinou doménu (vsbs.cz). Tyto požadavky zachytávala reverzní proxy, rovněž implementovaná řešiteli tohoto projektu, a transparentně komunikovala s klienty a legitimními servery (jednalo se o server pro zadávání dovolené a server pro komunikaci s helpdeskovým pracovištěm). Mohli jsme tak v reálném čase ověřovat, zda byly zadány skutečné přihlašovací údaje. Zároveň byly podvržené stránky vzhledově nerozeznatelné od stránek legitimních. V porovnání s ostatními podvodnými kampaněmi, které jsme realizovali, jsme obtížnost tohoto testu vyhodnotili jako velmi vysokou a očekávali jsme kompromitaci většiny účtů.

Provedený test potvrdil užitečnost pořádaných školení. Uživatelé velmi rychle a v hojném počtu reagovali na útok podle naučených postupů a nahlašovali jej bezpečnostnímu týmu. Takže super.

Změny v projektu

Před ukončením projektu jsme plánovali provést několik zkušebních školení praktické části. To nám nebylo umožněno z důvodu omezeného provozu univerzity v reakci na pandemickou situaci. Dospěli jsme k závěru, že výuka pomocí online nástrojů je v tomto případě spíše nevyhovující - osobní přístup je pro praktickou část nezbytný. Praktická školení budou proto probíhat v nejbližší možné době. Teoretická školení probíhala v průběhu celého projektu ve spolupráci s *Centrem celoživotního vzdělávání VŠB-TU Ostrava*.

Administrativní stránka implementace školení do procesů univerzity je poměrně náročná a proto zatím nedošlo k zavedení kurzu jako povinné prerekvizity. VŠB-TU Ostrava je však spoluřešitelem projektu *669/2020 Tvorba metodik a dokumentace v oblasti kybernetické bezpečnosti v prostředí VVŠ* a proto předpokládáme finalizaci tohoto bodu v rámci řešení souvisejícího projektu. Po technické stránce jsme na to již připraveni.

Zmíněné změny v projektu nemají vliv na čerpané finanční prostředky.

Využitelnost projektu

Studijní materiály byly od počátku navrženy tak, aby byly snadno pochopitelné všem zaměstnancům, bez ohledu na to, zda jejich činnost spadá do IT sféry. Poznatky v nich obsažené jsou univerzálně platné pro všechny a jejich technická stránka je maximálně redukovaná. Díky tomu jsme schopni toto školení nasadit na naši univerzitě plošně. Většina poznatků je rovněž přenositelná i mimo VŠB-TU Ostrava, případným zájemcům o využití materiálů doporučujeme upravit obsah tak, aby bral v úvahu jednotlivá specifika jejich prostředí.

Problematiku IT bezpečnosti předkládáme ve formě fakticky pravdivé, ale zároveň maximálně stručné a čtivé. V tomto ohledu se odlišujeme od mnoha již existujících kurzů, které zdánlivě pokrývají stejnou problematiku, ale ve skutečnosti spíše zabředávají do právního výkladu *Zákona 181/2014 Sb. o kybernetické bezpečnosti* a zákonů souvisejících. Navržený online test od účastníků neočekává znalost pojmů, definic a přesných postupů, naopak se opírá o praktické situace, ve kterých se absolventi mohou ocitnout.

VŠB-TU Ostrava je spoluřešitelem projektu *669/2020 Tvorba metodik a dokumentace v oblasti kybernetické bezpečnosti v prostředí VVŠ*. Předpokládáme využití vytvořených materiálů a získaných poznatků i v rámci tohoto projektu.

Přínos projektu

Materiály jsou pod licencí CC-BY-SA (Uveďte původ-Zachovejte licenci) dostupné na adrese https://gitlab-cit.vsb.cz/gry0057/frc-644-2019/ ve formátu PDF (teoretická a praktická část) a také ve formátu zálohy kurzu LMS Moodle.
Kurz byl vytvořen v Moodle verze 3.7.
Záloha kurzu neobsahuje žádná uživatelská rozšíření, můžete ji obnovit do kterékoliv z aktuálně podporovaných verzí Moodle od verze 3.5. po verzi 3.9. (stav k červenci 2020).

V naší instanci LMS Moodle byl dočasně zřízen přístup do vytvořeného kurzu. Pro hodnocení projektu tak není nutné mít k dispozici vlastní instanci LMS Moodle.

Přihlašovací jméno: itbezpecnost
Heslo: m6GUGyv4xNvK
URL: https://lms.vsb.cz/frc-644-2019

Pro přihlášení do LMS Moodle (v pravém horním rohu) použijte variantu:
Ostatní (U3V, projektové účty)

Tisková zpráva

V červenci 2020 byla dokončena realizace projektu č. 644/2019 Fondu rozvoje CESNET s názvem "*Školení IT bezpečnosti*".
V rámci výstupů projektu vznikl e-learningový kurz obsahující teoretickou, praktickou a evaluační část, které pokrývají klíčové oblasti IT bezpečnosti - ve formě přístupné široké veřejnosti. Obsah kurzu je zpracován v online prostředí LMS Moodle, což umožňuje snadné využití obsahu kurzu i v dalších organizacích.
Dále byla v rámci projektu připravena datová integrace univerzitního LMS Moodle se systémem SAP, pro plánovanou podporu automatizovaného zpracování získaných kvalifikací.

https://www.vsb.cz/cs/detail-novinky?reportId=40441

Přílohy

1. Výkaz hospodaření
2. Faktura Integrace evidenčního systému kvalifikací (spoluúčast)