2025

Návrh plnění veřejné zakázky

PROJEKT 101145866 — IXTrust Platform

NAVRHOVATEL: ČVUT V PRAZE, FAKULTA ELEKTROTECHNICKÁ

DATUM: [KVĚTEN, 2025]

Obsah

1. Předmět zakázky

Předmětem této nabídky je realizace a zajištění odborné podpory v oblasti komunikace a šíření povědomí o projektu zaměřeném na kybernetickou bezpečnost, realizovaného v rámci spolufinancování z prostředků EU (Digital Europe Programme – DEP). Plnění bude probíhat ve spolupráci se zadavatelem, přičemž jeho cílem je naplnění následujících oblastí:

A) Vypracování komunikačního plánu projektu
B) Organizace a zajištění vzdělávacích a popularizačních aktivit
C) Podpora stáží a pilotních zapojení studentů

Identifikační údaje uchazeče

České vysoké učení technické v Praze
Fakulta elektrotechnická
Jugoslávských partyzánů 1580/3
160 00 Praha 6 - Dejvice
Česká republika

Adresa datové schránky ČVUT v Praze: p83j9ee
DIČ: CZ68407700
IČ: 68407700

Odpovědná osoba za vypracování této nabídky a realizaci aktivit:

Ing. Jaroslav Burčík, Ph.D., LL.M.
Centrum pro kybernetickou bezpečnost
České vysoké učení technické v Praze, Fakulta elektrotechnická
Katedra telekomunikační techniky
Technická 2, 160 00 Praha
Mobil: +420 773 510 551
Mail: burcik@fel.cvut.cz
Web: https://netacad.fel.cvut.cz

Prokázání kvalifikačních předpokladů

Právní postavení a akreditace

České vysoké učení technické v Praze (ČVUT) je veřejná vysoká škola univerzitního typu zřízená zákonem. Univerzita byla založena již v roce 1707 a patří k největším a nejstarším technickým vysokým školám v Evropě. ČVUT má v současné době osm fakult a studuje na něm přes 19 tisíc studentů.

ČVUT disponuje širokou škálou akreditovaných studijních programů přímo zaměřených na oblast kybernetické bezpečnosti, kryptografie a síťových technologií.

Fakulta elektrotechnická (FEL), která bude realizovat poptávané služby, vyučuje tuto specializaci v rámci studijního programu Softwarové inženýrství a Technologie (SIT), Otevřená informatika (OI) a dále je možno získat zkušenosti z této oblasti v rámci výuky specializovaných předmětů v programu Elektronicka a komunikace (EK).

Infrastruktura a capacity

ČVUT FEL disponuje specializovanými laboratořemi pro kybernetickou bezpečnost, kde studenti pracují s realistickými scénáři a testovacími prostředími. Fakulta zároveň úzce spolupracuje v této oblasti s veřejným sektorem a podniky. Nabízí konzultační a tréninkové kapacity pro poskytování praktických cvičení v oblasti penetračního testování, analýzy malwaru, forensní analýzy a dalších specializovaných oblastí kybernetické bezpečnosti.
Univerzita má dlouhodobé zkušenosti s organizací vědecko-výzkumných aktivit, včetně programu "Výzkumné léto na FIT" pro nadané studenty a pravidelného pořádání odborných soutěží a konferencí v oblasti informatiky a kybernetické bezpečnosti

Zkušenosti s podobnými projekty

Níže uvádíme projekty a zkušenosti, které historicky zaštitoval či stále realizuje realizační tým zakázky.

Akademie kybernetické bezpečnosti (AKB)
FEL ČVUT provozuje vlastní vzdělávací koncept Akademie kybernetické bezpečnosti určený pro studenty vysokých a středních škol ČR. Program je postaven na kurzech CCNA – Cisco Networking Academy Program, a CompTIA, doplněných vlastními přednáškami a kyberbezpečností laboratoří Netlab. Absolventi získávají mezinárodně uznatelné průmyslové certifikace a podílejí se na rozvoji a provozu bezpečnostní laboratoře NetLAb

Centrum pro kybernetickou bezpečnost
FEL ČVUT provozuje specializované Centrum pro kybernetickou bezpečnost, které slouží jako regionální kontaktní místo pro profesní rozvoj, výzkum a sdílení znalostí mezi akademickým světem a podniky. Centrum realizuje vzdělávací kurzy v prezenční i e-learningové formě a provozuje osvětové aktivity a praktické vzdělávání studentů, zaměřené na kybernetickou bezpečnost.

Spolupráce se státním sektorem a komerční sférou

Realizační tým se v posledních 5 letech podílel na vice než 30 projektech komerční spolupráce s průmyslovými partnery či státním a neziskovým sektorem v oblasti různých aspektů kyberbezpečnosti. A to ať již technického charakteru (skenování zranitelností, architekturní práce) či netechnických oblastí kyberbezpečnosti jako je práce na analýzách legislativního souladu, tvorbě bezpečnostních politik, navrhování odpovídajících vzdělávacích plánů atp.

Na katedře bylo vyvinuto specializované zařízení E-Shaper a F-Tester pro emulaci a záměrné narušování telekomunikačních sítí. Tyto nástroje jsou využívány Českým telekomunikačním úřadem pro ověřování kvality mobilních sítí a společností CETIN pro testování datové komunikace z pohyblivých prostředků.

Odborné conference a semináře

Realizační tým má zkušenosti s organizací rozsáhlých odborných akcí zaměřených na kybernetickou bezpečnost. V září 2024 inicioval a úspěšně realizoval inovativní formát spolupráce mezi akademickou sférou a komerční praxí. Ve spolupráci se Studentskou sekcí IEEE při ČVUT uspořádal konferenci Cybersecurity Horizons 2024, která se stala významnou platformou pro propojení předních odborníků z univerzitního prostředí s reprezentanty soukromého sektoru.

Konference byla koncipována jako multioborová akce zaměřená na prezentaci aktuálních výzkumných projektů, vytváření strategických partnerství mezi akademickým výzkumem a průmyslovými aplikacemi a sdílení praktických zkušeností z implementace bezpečnostních technologií. Akce získala širokou podporu významných firem a velmi kladné hodnocení.

2. Návrh realizace

Návrh realizace komunikačního plánu

Identifikace cílových skupin

Studenti IT a kybernetické bezpečnosti
Primární cílovou skupinou jsou studenti bakalářských a magisterských programů ČVUT zaměřených na informatiku, kybernetickou bezpečnost, kryptografii a síťové technologie. Jedná se o motivované jedince se zájmem o praktické uplatnění teoretických znalostí v oblasti obrany proti pokročilým trvalým hrozbám (APT). Tato skupina představuje budoucí odborníky v oblasti kybernetické bezpečnosti a potenciální kandidáty pro stážní programy u zákazníků IXPERTA.

Akademická obec
Zahrnuje pedagogy, výzkumné pracovníky a doktorandy z oblasti kybernetické bezpečnosti na ČVUT i dalších vysokých školách. Cílem je posílit spolupráci mezi akademickou sférou a komerční praxí při sdílení nejnovějších poznatků o kybernetických hrozbách a obranných strategiích. Akademická obec funguje jako multiplikátor znalostí směrem k širší odborné komunitě.

Odborná veřejnost ze soukromého sektoru
Představuje IT specialisty, bezpečnostní analytiky a manažery zodpovědné za kybernetickou bezpečnost zejména v malých a středních podnicích kritické povahy (zdravotnický sektor, kritická infrastruktura). Tato skupina potřebuje praktické znalosti o implementaci komplexních bezpečnostních řešení proti APT hrozbám s omezenými rozpočty a kapacitami.

Klíčová sdělení o hodnotě EU spolufinancování

Projekt IXTrust Platform je realizován s podporou programu Digitální Evropa (Digital Europe Programme - DEP), což zdůrazňuje strategický význam kybernetické bezpečnosti pro celou Evropskou unii. Komunikace bude akcentovat následující klíčové hodnoty:

- Evropská solidarita v kybernetické bezpečnosti: EU investuje do ochrany všech členských států proti pokročilým kybernetickým hrozbám, které nezná hranice
- Dostupnost pokročilých technologií: EU spolufinancování umožňuje malým a středním podnikům přístup k enterprise-level bezpečnostním řešením, která by si jinak nemohly dovolit
- Budování odolné digitální Evropy: Projekt přispívá k naplnění strategie kybernetické bezpečnosti EU a posílení evropské digitální autonomie
- Investice do budoucnosti: Vzdělávání nové generace odborníků na kybernetickou bezpečnost představuje strategickou investici do dlouhodobé bezpečnosti evropského digitálního prostoru

Kanály komunikace

V rámci realizace projektu navrhujeme využít tyto komunikační kanály:

Odborné semináře a workshopy:

- Organizace tematických workshopů přímo v prostorách ČVUT s kapacitou pro minimálně 200 účastníků celkem
- Odborné semináře ve spolupráci s komerčními partnery a zákazníky IXPERTA
- Webináře a online semináře pro širší dosah odborné komunity

Online platformy a digitální komunikace:

- Využití webových stránek ČVUT, ČVUT FEL a specializovaných portálů výzkumných skupin ČVUT zaměřených pro kybernetickou bezpečnost
- Sociální sítě (LinkedIn, Discord) ČVUT pro sdílení aktuálních informací o projektu
- Newsletter ČVUT FEL a Časopisy z vydavatelství Česká Technika pro zviditelnění projektu mezi širší skupinou studentů zaměstnanců a absolventů ČVUT

Tradiční média a PR aktivity:

- Tiskové zprávy v klíčových milnících projektu
- Rozhovory s vedoucími projektu v odborných médiích
- Případové studie úspěšných implementací u zákazníků IXPERTA

Akademické konference a vědecké akce:

- Prezentace spolupráce na konferencích CESNET,
- Organizace specializovaných sekcí o kyberbezpečnostních hrozbách v rámci osvětových seminářů a konferencí pořádaných na ČVUT

Návrh harmonogramu aktivit

Fáze 1: Zahájení a budování povědomí (květen - prosinec 2025)

- Červen 2025: Oficiální spuštění komunikačního plánu a první tiskové zprávy
- Červen - září 2025: Příprava 5 integrovaných přednášek po 60 minutách do standardních předmětů, příprava miniprojektů pro stážisty
- Říjen - prosinec 2025:
    - 1) Organizace minimálně 3 workshopů s celkovým pokrytím 200+ účastníků
    - 2) Vyhlášení a výběr 10 zájemců do stipendijního programu IXPERTA ČVUT (pracovní název navrhujeme „IXTRUST Master“)
- Průběžně: Měsíční publikování článků na odborných portálech o hodnotě EU investic

Fáze 2: Implementace a praktické zapojení (listopad - červen 2026)

- Listopad 2025:
    1) Zahájení stážového programu fáze 1 – odborné vzdělávání CompTIA 1. semestr pro vybrané studenty u zákazníků IXPERTA
    2) Výuka kurzu CompTIA Security+ pro stipendisty
    3) Zadání tematických miniprojektů přihlášeným stážistům
- Únor - květen 2026:
    1) Konec února 2026 odborné vzdělávání CompTIA 2. semestr pro vybrané stážisty (výuka kurzu CompTIA CySa+)
    2) Průběžné hodnocení postupu prací miniprojektů
    3) Květen 2026 – start kurzu Python for Datascience pro stipendisty
    4) Neformální setkávání specialistu IXPERTA se studenty s cílem probudit hlubší zájem o problematiku
- Červen 2026:
    - 1) Vyhodnocení první fáze stáží a prezentace výsledků
    - 2) Zahájení stážového programu fáze 2 - Příprava a rozřazení studentů pro stáže u partnerů IXPERTA

Fáze 3: Realizace stáží a vyhodnocení a udržitelnost (červenec - prosinec 2026)

- Červenec – říjen 2026: Realizace stáží u partnerů IXPERTA (možné zapojení do odborného dohledu specialisty ČVUT)
- Listopad 2026: Finalizace všech osvětových aktivit a dokumentace výsledků
- Prosinec 2026: Publikování souhrnné zprávy o výsledcích projektu

3. Seznam dostupné infrastruktury

Specializované laboratoře pro kybernetickou bezpečnost

NetLAB - Virtuální laboratoře pro kybernetickou bezpečnost

- Revoluční systém vzdáleného přístupu k praktické výuce a výzkumu v oblasti informačních technologií
- Umožňuje studentům i výzkumníkům snadný přístup k simulaci, návrhu a testování moderních scénářů kybernetické bezpečnosti
- Pokrývá široké spektrum od síťových technologií až po operační systémy
- Dostupné 24/7 pro praktickou výuku penetračního testování, analýzy malwaru a detekce útoků

Centrum pro kybernetickou bezpečnost ČVUT FEL

- Specializované pracoviště koordinované katedrou telekomunikační techniky
- Regionální kontaktní místo pro profesní rozvoj a výzkum v oblasti kybernetické bezpečnosti
- Infrastruktura pro realizace vzdělávacích kurzů v prezenční i e-learningové formě
- Akademie kyberbezpečnosti ČVUT FEL zaměřená na kybernetickou bezpečnost s certifikovanými kurzy

Přednáškové a vzdělávací prostory

Hlavní budova FEL - Technická 2, Praha 6

- Moderně vybavené přednáškové místnosti s kapacitou od 30 do 200 míst
- Audiovizuální technika včetně projektorsů, interaktivních tabulí a konferenčního systému
- Wi-Fi pokrytí a napájení pro notebooky účastníků
- Bezbariérový přístup do všech hlavních učeben

Podpůrná infrastruktura

Studentské prostory a zázemí

- Studovny s Wi-Fi a napájením pro dlouhodobé projekty
- Kuchyňky a odpočinkové prostory pro účastníky dlouhodobých kurzů
- Bezpečnostní systém s 24hodinovým dohledem

Parkování a dostupnost

- Parkovací místa pro účastníky externích akcí
- Výborná dostupnost veřejnou dopravou (metro Dejvická)
- Bezbariérový přístup do všech hlavních částí budovy

4. Cenová nabídka

Celková nabídková cena činí **382 000 Kč bez DPH.** ČVUT je pro účely zakázky plátcem DPH.

Celková cena zahrnuje realizaci těchto položek:

1) Realizaci komunikačního plánu
2) Přípravu a realizace workshopů pro 200 účastníků
3) Přípravu a vedení studentů v rámci stipendijního programu
4) Finanční podporu a odměnu studentům za úspěšnou realizaci miniprojketů stipendijního programu
5) Náklady na materiál, licence a výuku spojené se zajištěním odborných kurzů CompTIA a Python
6) Koordinační a komunikační aktivity se zadavatelem

Fakturace a platební podmínky

Fakturaci navrhuje provést takto: K 31.12.2025 bude vystavena zálohová faktura ve výši 1/3 nabídnuté ceny (tedy 127 tis. Kč bez DPH) a následně na základě předávacího a akceptačního protokolu, po dokončení všech aktivit bude v prosinci 2026 vystavena finální faktura do výše nabídnuté ceny.

Ing. Jaroslav Burčík, PhD.

Digitálně podepsal Ing. Jaroslav Burčík, PhD.
Datum: 2025.06.06 09:12:17 +02'00'