VŠ:	České vysoké účení technické v Praze		
Rozvojový projekt na rok 2023			
Formulář pro závěrečnou zprávu - dílčí část projektu			
Prioritní oblast:	2. Prioritní témata pro společné projekty vysokých škol bez předem vyčleněné alokace		
Tematické zaměření:	2.f) zvyšování bezpečnosti digitálního prostředí, kybernetická bezpečnost		
Název projektu:	**Budování situačního povědomí v kyberprostoru VVŠ a efektivní reakce na krizové situace**		
Období řešení projektu:	**Od: 1. 1. 2023**	**Do: 31. 12. 2023**	
Dotace v tis. Kč:	**Celkem:**	**V tom běžné finanční prostředky:**	**V tom kapitálové finanční prostředky:**
Požadavek	2500	2500	0
Čerpáno	2465	2465	0

Základní informace

	Hlavní řešitel	**Kontaktní osoba**
Jméno:	Ing. Jiří Richter	Ing. Tomáš Veselý
VŠ:	České vysoké učení technické v Praze	České vysoké učení technické v Praze
Adresa/Web:	Jugoslávských partyzánů 1580/3, Praha 6, www.cvut.cz	Jugoslávských partyzánů 1580/3, Praha 6, www.cvut.cz
Telefon:	+420 603 456 766	+420 735 610 011
E-mail:	jiri.richter@cvut.cz	tomas.vesely@cvut.cz

ZPRÁVA O PRŮBĚHU ŘEŠENÍ PROJEKTU

Cíl projektu	**Uveďte stanovený cíl a uveďte, do jaké míry byl splněn, případně důvod, proč splněn nebyl.**
č.1: Posílení přímé spolupráce	I tento rok jsme udržovali spolupráci s ostatními školami a účastnili jsme se společných seminářů a workshopů. Dva workshopy jsme připravili z oblastí našich výstupů pro ostatní. V případě požadavků na individuální pomoc jsme spolupracovali také i s jednotlivci. Cíl považujeme za splněný
č.2: Zajištění situačního povědomí	V tomto roce jsme zajistili pro ČVUT licenci na flow monitor Noction, který jsme nasadili do pilotního provozu na několika součástech ČVUT a postupně jsme ho začali využívat pro detekci některých bezpečnostních událostí v síti i pro monitoring provozních událostí. Pro základní monitoring jsme využívali uživatelské rozhraní, které je přímo součástí SW Noction, které jsme postupně přizpůsobili zavedením několika skriptů pro snadnější vyhodnocení událostí v několika oblastech. Flow collector Noction má výhodu snadného napojení na celou řadu síťových prvků a proto jsme mohli jeho zapojení do sítě ČVUT realizovat poměrně rychle. Vedle sondy Noction jsme začali připravovat i zapojení sondy pro behaviorální analýzu síťového provozu Greycortex Mendel, která však pro efektivní sběr a vyhodnocování událostí vyžaduje velmi specifické zapojení. Sondu Mendel chceme zapojit a začít využívat v roce 2024. Postupně chceme pro vyhodnocování událostí v síti zavést systém SIEM. Cíl považujeme za splněný
č.3: Začlenění klasifikace informací do univerzitního prostředí	Tým odboru bezpečnosti na ČVUT využil některé výstupy z CRP2022 a CRP2023 k přepracování interní legislativy, zejména pak ke změně struktury Systému řízení bezpečnosti informací. Součástí připravené aktualizace legislativy je i nová verze klasifikace informací, která by měla být vydána začátkem roku 2024. Cíl považujeme za splněný
č.4: Detekce těžby kryptoměn	Pro detekci těžby kryptoměn jsme využili již zmíněnou sondu Noction, která nám umožňuje sledovat vybrané vzorky komunikace. Pro sledování těžby jsme vytvořili několik skriptů, které se zaměřují na sledování komunikace nejznámějších těžařských programů a tento typ komunikace jsme sledovali na několika součástech ČVUT. Některé typy této komunikace byly detekovány a bylo zajištěno její blokování na příslušných součástech. Cíl považujeme za splněný

Plnění výstupů projektu	**Uveďte výstupy projektu a do jaké míry byly splněny, případně důvod, proč splněny nebyly.**
č.13: Rešerše existujících řešení pro řízení aktiv a doporučení pro jejich nasazení v prostředí VVŠ	V rámci projektu jsme zajistili přehled vytipovaných informačních systémů pro evidenci a řízení aktiv. Snažili jsme se o popis hlavních vlastností těchto systémů tak, aby to ostatním školám umožnilo snažší výběr systému. Cíl považujeme z větší části za splněný
č.14: Návrh postupu nasazení automatizovaného nástroje pro vyhledávání a	V této části projektu jsme hledali informační systémy, které by umožňovaly automatické vyhledávání změn v evidenci podpůrných aktiv. Zajistili jsme přehled řady systémů, které by tyto požadavky měly splňovat. Z nedostatku volných kapacit se nám nepodařilo zajistit praktické ověření této funkce na vytipovaném systému. Jako bonus jsme však zajistili přehled systémů z kategorie komerční, free a český software. Cíl považujeme za částečně splněný

č.15: Řízení privilegovaných účtů systémem PIM/PAM	V projektu jsme prakticky ověřili zavedení systému PIM v prostředí Azure active directory, což mělo za cíl ověření náročnosti implementace, konfigurace a praktické nasazení. Do této ověřovací fáze bylo zapojeno 5 administrátorů, kteří byli nuceni různé systémy spravovat pomocí dočasného a podmíněného přidělení oprávnění. Systém sice neumožňoval plnohodnotné prostředí PAM, ale styl práce z pohledu administrátora byl obdobný jako v pokročilejším systému PIM/PAM. Společně s partnerskou firmou jsme potom zajistili přehled výčtu funkcí, které může poskytnout plnohodnotný systém PIM/PAM a přehled a hodnocení minimálně dvou komerčních systémů s odlišnou cenovou politikou, které vyspělé systémy PIM/PAM zastupují. V této kategorii informačních systémů se, bohužel, Open Source ani Free systémy nevyskytují.
č.16: Rešerše současných řešení pro nasazení vícefaktorové autentizace	Vícefaktorou autenizaci používáme u privilegovaných účtů již delší dobu. Tentokrát jsme navíc zapojili povinně celou jednu větší skupinu správců méně vyznamného informačního systému. Uživatelům bylo umožněno ověření heslem a jako druhý faktor měli k dispozici SMS či MS Authenticator. Praxe z tohoto ověřování nám ukázala oblasti, na které bychom se zaměřit v dalším hledání optimálního řešení. S partnerskou firmou jsme nakonec navrhli nejlepší řešení řízení přístupu, včetně integrace vícefaktorové autentizace. Návrh vycházel jak z potřeb ČVUT, tak i z větší části výsledků dotazníkového šetření, které jsme v rámci projektu také připravili. Řešení by tedy mělo vyhovovat více univerzitám. Cíl považujeme za splněný

Změny v řešení	**Pokud došlo v průběhu řešení ke změnám, uveďte je a vysvětlete příčinu**	
Číslo změny	**Jednotlivé změny (přidejte řádky dle potřeby)**	**Zdůvodnění**
1.	Přesun finančních prostředků ze mzdových do služeb	Z důvodu nedostatečných interních kapacit jsme některé činnosti oproti původnímu plánu outsourcovali
2.		
3.		
4.		

Přehled o pokračujícím projektu	**Pokud se jedná o pokračující projekt, uveďte, od kdy se realizuje a kolik finančních prostředků již bylo vyčerpáno. V případě, že je plánováno pokračování projektu v dalších letech, uveďte výhled do budoucna.**		
	Rok realizace	**Čerpání finančních prostředků (souhrnný údaj)**	**Poznámka (případně výhled do budoucna)**

Specifikace čerpání finanční dotace na řešení projektu *					
		Přidělená dotace na řešení projektu - ukazatel I (v tis. Kč)	**Čerpání dotace (v tis. Kč)**	**Rozdíl (v tis. Kč)**	**Rozdíl (v %)**
1.	**Kapitálové finanční prostředky celkem**	0	0	0	0 %
1.2	Dlouhodobý nehmotný majetek (SW, licence)	0	0	0	0 %
1.3	Samostatné věci movité (stroje, zařízení)	0	0	0	0 %
1.4	Ostatní technické zhodnocení	0	0	0	0 %
2.	**Běžné finanční prostředky celkem**	2 500	2 465	-35	-1 %
	Osobní náklady:				
2.1	Mzdy (včetně pohyblivých složek)	1210	767	-443	-18 %
2.2	Ostatní osobní náklady (odměny z dohod o pracovní činnosti, dohod o provedení práce, popř. i některé odměny hrazené na základě nepojmenovaných smluv uzavřených podle zákona § 1746 odst. 2 č. 89/2012 Sb., občanský zákoník)	0	78	78	3 %
2.3	Odvody pojistného na veřejné zdravotní pojištění a pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a příděly do sociálního fondu	435	293	-142	-6 %
	Ostatní:				
2.4	Materiální náklady (včetně drobného majetku)	0	0	0	0 %
2.5	Služby a náklady nevýrobní	840	1325	485	19 %
2.6	Cestovní náhrady	15	2	-13	-1 %
2.7	Stipendia	0	0	0	0 %
3.	**Celkem běžné a kapitálové finanční prostředky**	2500	2 465	-35	-1 %

Bližší zdůvodnění čerpání v jednotlivých položkách (přidejte řádky podle potřeby)		
Číslo položky (viz předchozí	**Název výdaje a jeho zdůvodnění**	**Částka (v tis. Kč)**
2.1	Mzdové prostředky ve formě úvazků, včetně odměn pro řešitelský tým na realizace definovaných cílů a výstupů a hlavních činností, a to jak v rámci pracovní skupiny, tak v rámci implementačních aktivit v rámci ČVUT. Čerpání bylo nižší, než původně plánované, protože z důvodu nedostatečných interních kapacit jsme některé činnosti byli nuceni outsourcovat.	767
2.2	Odměny z dohod o provedení práce pro realizační tým projektu za účelem zajištění jednotlivých plánovaných výstupů projektu.	78
2.3	Zákonné odvody zdravotního a sociálního pojištění, příspěvek do sociální fondu. Z důvodu nižšího čerpání mzdových prostředků došlo k nedočerpání této položky.	293
2.5	Finanční prostředky byly využity pro potřebu konzultační činnosti (služby), díky které bylo možné dokončit práci na konkrétních výstupech. Z důvodu nedostatečných interních kapacit jsme některé činnosti oproti původnímu plánu museli outsourcovat. Přesun mezi položkami 2.1+2.3 a 2.5 byl v povolené výši do 20%.	1325
2.6	Cestovní náhrady pro členy realizačního týmu na společné jednání v Pardubicích.	2

* VŠ vyplní pouze žlutě podbarvená pole tabulky.

Poznámka: V případě, že potřebujete sdělit další doplňující informace, uveďte je v příloze.