VŠ:	Ostravská univerzita		
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	500	500	0
Čerpáno	500	500	0

Základní informace		
	Hlavní řešitel	**Kontaktní osoba**
Jméno:	Ing. Pavel Pomezný	Ing. Břetislav Lišťák, MBA
VŠ:	Ostravská univerzita	Ostravská univerzita
Adresa/Web:	Bráfova 5, 701 03 Ostrava; www.osu.cz	Bráfova 5, 701 03 Ostrava; www.osu.cz
Telefon:	+420 553 461 133	+420 553 461 109
E-mail:	pavel.pomezny@osu.cz	bretislav.listak@osu.cz

ZPRÁVA O PRŮBĚHU ŘEŠENÍ PROJEKTU	
Cíl projektu	**Uveďte stanovený cíl a uveďte, do jaké míry byl splněn, případně důvod, proč splněn nebyl.**
1	Cílem projektu bylo vytvořit metodiky, postupy a scénáře pro zvýšení úrovně kybernetické bezpečnosti na veřejných vysokých školách v ČR, které budou reflektovat individuální potřeby a možnosti jednotlivých škol. V prostředí Ostravské univerzity byla vytvořena množina dokumentů v podobě šablon, které si mohou jednotlivé školy přizpůsobit svým specifickým potřebám. Vzájemnou diskuzí, spoluprací a aktivní účastí na seminářích byla realizována předběžná analýza možných dopadů nové regulace NIS2 do prostředí vysockých škol. Vytvořena sada nových phishingových kampaní, identifikovány možné ukazatele pro kontrolu dodržování bezpečnostních politik, realizována základní klasifikace informací, včetně návrhu organizačního opatření Směrnice klasifikace informací. Položeny základy tvorby krizových plánů vybraných systémů univerzity. Klíčovým dílem tohoto cíle (projektu) bylo zahájení přípravy na plnění nových povinností NIS2 pro naši univerzitu jako správce významných informačních systémů podle ZoKB, která byla naplňována s každým realizovaným seminářem.

Plnění výstupů projektu	**Uveďte výstupy projektu a do jaké míry byly splněny, případně důvod, proč splněny nebyly.**
1	**Postupy pro ověřování dodržování vybraných bezpečnostních politik (V1)**. Identifikovány vybrané relevantní ukazatele, které lze v infrastruktuře univerzity měřit a tím si ověřit, zda lze ověřovat dodržování politik. Na univerzitě lze nalézt dva možné zdroje ukazatelů : (a) síťová infrastruktura (b) infrastruktura Microsoft. V obou oblastech prostřednictvím monitoringu provozních a lokalizačních údajů lze nalézt ukazatele pro segmentaci sítě, komunikaci na perimetru, blokování nevyžádané komunikace, neúspěšné přihlášení uživatelů, vytváření pravidel přeposílání elektronické pošty a další. Vytvořen pracovní, neveřejný analytický dokument, který je interním materiálem univerzity obsahující doporučení pro zlepšení postupů pro ověřování a dodržování bezpečnostních politik. **Výstup splněn.**
2	**Sada scénářů cvičných phishingových kampaní pro trénink univerzitních uživatelů (V2)**. Výstup realizován ve dvou krocích. V prvním kroku implementován vlastní systém pro rozesílání cvičných phishingových zpráv a jejich následné vyhodnocení, včetně realizace cvičné kampaně na vybraných fakultách a pracovištích. Ve druhém kroku implementován nový systém, dodavatelsky od společnosti CESNET, včetně přípravy nových kampaní na testování uživatelů. Vytvořen analytický dokument, který je interním materiálem univerzity a obsahuje popis samotné realizované kampaně, včetně přípravných postupů. **Výstup splněn.**
3	**Analýza dopadů nové směrnice NIS 2 do prostředí univerzity (V3).** Výstup realizován ve dvou krocích. V prvním kroku analyzován návrh regulace NIS2, návrh znění nového zákona, včetně všech souvisejících návrhů. Identifikovány možné dopady nové regulace do prostředí univerzity. Spolupráce na připomínkovém řízení návrhu zákona kybernetické bezpečnosti a vyhlášky stanovující vyšší povinnosti. V druhém kroku realizován detailní audit připravenosti univerzity na novou legislativu, včetně navržení seznamu nezbytných opatření a náročnosti jejich implementace. **Výstup splněn.**
4	**Analýza současného stavu a potřeb v oblasti klasifikace zabezpečovaných informací univerzity (V4)**. Identifikovány pracoviště univerzity zpracovávající množství informací a dat. Realizovány analytické pohovory a identifikována množina informací a dat na univerzitě zpracovávaných. Na základě pohovorů stanovena indikativní hodnota diskutovaných informací. Rozdělení informací do kategorií. Navržena matice informací, jejich kategorie, možnosti ukládání a zpracování. **Výstup splněn.**

5	**Návrh Politiky klasifikace informací (opatření rektora) (V5)**. Navržen základ nového opatření Politiky klasifikace informací a tento předán právnímu oddělení k dalšímu zpracování. **Výstup splněn.**
6	**Soubor bezpečnostních požadavků na dodavatele (V6)**. Identifikováni dodavatelé, potenciální kandidáti na významné dodavatele. Označeny rizikové scénáře a definována množina opatření pro zmírnění rizik, plus přidána doporučení pro zlepšení. Vypracován návrh základních smluvních oblastí, které je nezbytné zohlednit při uzavírání smluvního vztahu. Vypracován konkrétní příklad smluvního ustanovení = návrhu vzorové smlouvy. Problematika předána právnímu oddělení k dalšímu zpracování. **Výstup splněn.**
7	**Popis stávajících postupů v zajištění krizového řízení v prostředí univerzity optikou VIS (V7)**. Ve spolupráci s tajemníky fakult a auditorem popsán aktuální stav krizového řízení na univerzitě. Vypracován interní analytický dokument, který obsahuje výsledky šetření, včetně výstupů dotazníkového šetření realizovaného Pracovní skupinou projektu CRP za naši univerzitu. **Výstup splněn.**
8	**Definice a rozvoj krizových plánů pro zajištění kontinuity činností a obnovu po katastrofě u VIS (V8)**. Vytvořeny návrhy pro zpracování plánů obnovy systému POSTA, STAG, MAGION a tyto přeneseny na pracoviště CIT univerzity pro další rozpracování. Realizace plánů obnovy je součástí systému pro správu identit systému IDM. **Výstup splněn.**
9	**Doporučení a postupy pro efektivní a zabezpečený sběr provozních záznamů z prvků ICT (V9)**. Provozní a lokalizační údaje jsou v prostředí univerzity zpracovávány formou (a) lokálního sběru s vyhodnocováním logů na dotčených prvcích infrastruktury, (b) sběru a vyhodnocování mimo dotčené aktivum pomocí dohledového a monitorovacích systému zpracovávající a vyhodnocující systémové logy a (c) sběr a vyhodnocování prostřednictvím technologie nezávislé na monitorovaných prvcích infrastruktury = technologie využívající síťové sondy. **Výstup splněn.**
10	**Rozvoj odborných kompetencí zodpovědných bezpečnostních rolí (V10)**. Realizována množina odborných školení specialistů ICT a zavedena centrální evidence těchto školení v rámci pracoviště CIT univerzity. **Výstup splněn.**
11	**Účast na společných seminářích a zapojení se do konzultací k jednotlivým výstupům a návrhům řešení dalších partnerů projektu (V11).** Účast na bezmála 14 pořádaných seminářích, včetně aktivního vystupování v rámci diskuzí. **Výstup splněn.**
12	**Vzájemné srovnání dílčích výstupů k dosažení použití v prostředí univerzity (V12)**. Pravidelné vyhodnocování každé sdílené znalosti, zejména při pravidelných seminářích. Využitelné výstupy v prostředí OU - (a) návrhy bezpečnostních politik (b) krizových plánů (c) nejasností ve formulacích nové regulace NIS2 (d) společná platforma MKB a další. **Výstup splněn.**
13	**Závěrečné vyhodnocení projektu a zpracování závěrečné zprávy (V13)**. Zpracováním závěrečné zprávy **výstup splněn.**

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.	-----	-----

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**	500	500	0	0%
	Osobní náklady:				
2.1	Mzdy (včetně pohyblivých složek)	351	351	0	0%

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	0	0	0%
2.3	Odvody pojistného na veřejné zdravotní pojištění a pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a příděly do sociálního fondu	119	119	0	0%
	Ostatní:				
2.4	Materiální náklady (včetně drobného majetku)	0	0	0	0%
2.5	Služby a náklady nevýrobní	30	30	0	0%
2.6	Cestovní náhrady	0	0	0	0%
2.7	Stipendia	0	0	0	0%
3.	**Celkem běžné a kapitálové finanční prostředky**	500	500	0	0%

Bližší zdůvodnění čerpání v jednotlivých položkách (přidejte řádky podle potřeby)

Číslo položky (viz předchozí tabulka)	Název výdaje a jeho zdůvodnění	Částka (v tis. Kč)
2.1	Odměny a mzdy – díl mzdových nákladů pro nově zřízenou povinnou pozici manažera kybernetické bezpečnosti; odměna pro specialisty CIT za nasazení systému pro testování phishingových kampaní	351
2.2	Odvody pojistného na veřejné zdravotní pojištění a pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a příděly do sociálního fondu.	119
2.3	Služby a náklady nevýrobní - díl nákladů pro realizaci auditu kybernetické bezpečnosti, přesněji souladu stavu KB univerzity vůči požadavkům regulace NIS2; náklady pro certifikaci CSIRT (Bezpečnostní tým pro řešení počítačových bezpečnostních incidentů Ostravské univerzity) a získání akreditace TF-CSIRT nebyly realizovány ze zdroje projektu, ale z jiného zdroje univerzity.	30

* VŠ vyplní pouze žlutě podbarvená pole tabulky.

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