VŠ:	Vysoká škola technická a ekonomická v Českých Budějovicích		
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:	Doc. Ing. Robert Frischer, Ph.D.	Bc. Liliana Kopicová
VŠ:	Vysoká škola technická a ekonomická v Českých Budějovicích	Vysoká škola technická a ekonomická v Českých Budějovicích
Adresa/Web:	Okružní 517/10, 370 01 České Budějovice	Okružní 517/10, 370 01 České Budějovice
Telefon:	+420 778 081 410	+420 778 760 846
E-mail:	frischer@mail.vstecb.cz	kopicova@mail.vstecb.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. Zvolené výstupy VŠTE popsané níže reflektují zvýšení úrovně kyberbezpečnosti v prostředí VŠTE. Cíl byl naplněn.
Plnění výstupů projektu	**Uveďte výstupy projektu a do jaké míry byly splněny, případně důvod, proč splněny nebyly.**
1	**Nasazení nástroje pro budování situačního povědomí o dění v počítačové síti** - V rámci předcházení a rychlého řešení incidentů nasadilo IT oddělení VŠTE monitorovací nástroj PRTG, který v reálném čase monitoruje a hlídá klíčové prvky síťové infrastruktury a zařízení, která jsou nedílnou součástí bezproblémového chodu VŠTE. Software na základě SNMP protokolu dokáže monitorovat jakékoliv zařízení v síti, včetně koncových zařízení, služeb a protokolů. Software dokáže v případě indikace problému zaslat upozornění emailem, textovou zprávou nebo notifikací na mobilní telefon za pomocí mobilní aplikace. Výstup byl zcela splněn.
2	**Realizace cvičné phishingové kampaně vůči univerzitním uživatelům** - Na VŠTE byla v rámci projektu provedena Phishingová kampaň. Zapojeni byli jak zaměstnanci, tak studenti. Jednalo se o cílenou a koordinovanou akci, resp. Spear Phishing. Šlo o cílený phishingový útok, kdy si virtuální útočník dopředu získal veškeré dostupné informace o cílové skupině a vytvořil phishingovou zprávu přesně na míru. Obsah zprávy byl předem velmi pečlivě konzultován a vybrán. Cílem akce bylo zmapovat zejména komunikační kanály, které jsou v uživatelích zakotveny a jak uvažují v případě stresové situace, která by mohla mít zásadní vliv na jejich životní a pracovní úroveň. Dále také bylo zjištěno, kolik % uživatelů poskytlo své přihlašovací údaje a podíl studentů vs zaměstnanci. Výsledky Phishingové kampaně bereme jako zásadní a velmi užitečné. Na základě výstupů budeme připravovat změny ve směrnicích školy a budou vytvářeny školící semináře pro uživatele, které vysvětlí vážnost takových útoků a samozřejmě také metody, jak se bránit a jak hrozby rozpoznávat. Výstup byl zcela splněn.
3	**Začlenění klasifikace informací do univerzitního prostředí** - Problematika je na VŠTE řešena vznikem nové směrnice k využívání datových úložišť a klasifikaci ukládaných informací. Směrnice bude definovat konkrétní úložiště dat, která jsou pro zaměstnance VŠTE k dispozici a bude určovat použití uložišť pro konkrétní kategorii citlivosti informací. Současně směrnice bude vymezovat pravidla pro bezpečné použití těchto úložišť. Výstup byl zcela splněn.

4	**Integrace krizových plánů pro zajištění kontinuity činností univerzity** - V rámci tohoto výstupu se Komise pro kybernetickou bezpečnost VŠTE zabývala tvorbou a aktualizací krizového plánu pro případ kybernetického útoku na školu v různém rozsahu napadení. V návaznosti na tuto problematiku se Komise bude zabývat také povinnostmi vyplývajícími ze Směrnice Evropského parlamentu a Rady EU „NIS2“. Bezpečností pokyny při zjištění kybernetického útoku: 1. Informování vedoucího pracovníka Úseku informatiky: Prorektor pro informatiku - Informování předsedy a manažera Komise pro kybernetickou bezpečnost VŠTE – postup při kybernetickém útoku se primárně řídí pokyny předsedy. - Informování IT týmu VŠTE o napadení a jeho obecném rozsahu 2. Zjištění rozsahu a závažnosti způsobených škod. Zjištění, zdali byl útokem dotčen některý z významných informačních systémů (VIS) VŠTE. V případě identifikace rizika dojde k fyzickému odpojení klíčových serverů ze sítě, aby se minimalizovala možnost šíření útoku a dále budou dočasně odpojeny datové okruhy klíčových pracovišť. 3. Vyhodnocení rozsahu škod a zajištění sítě proti dalším útokům. Identifikace způsobu, jakým byla síť napadena, zajištění a uchování důkazů pro budoucí vyšetřování daného incidentu. 4. Postupné obnovení provozu nenapadených systémů. 5. Kontaktování vlastníků napadených systémů. 6. Kontaktování externích zainteresovaných partnerů. 7. Kontaktování orgánů činných v trestním řízení, pokud to rozsah a způsob napadení vyžaduje. 8. Obnovení IT struktury, revize opatření, analýza incidentu, identifikace slabých míst, kterých útočník využil, implementace opatření, která povedou k vyšší bezpečnosti. Výstup zcela splněn.
5	**Audit/Penetrační test zákonem regulovaného VIS** - V rámci tohoto výstupu byl na VŠTE proveden penetrační test zákonem regulovaného VIS. Jako cílový VIS byl vybrán systém iFIS, který je na VŠTE nasazen on-premise. Penetrační test obsahoval jak vnitřní, tak vnější sken. Interní test byl proveden nástrojem nasazeným přímo uvnitř sítě a v rámci tohoto testu byly testovány servery, na kterých je aplikace provozována. Externí sken byl realizován z internetu a skenoval veřejnou IP adresu, přes kterou dodavatelé systému v případě potřeby (aktualizace, servisní zásahy atd.) přistupují k aplikaci. Výstup byl zcela splněn.
6	**Rozvoj odbornosti a certifikace Manažera KB dle zákonných požadavků** - Manažerem kyberbezpečnosti bylo absolvováno třídenní školení MANAŽER IT BEZPEČNOSTI – ISMS DLE ISO/IEC 27001. Hlavním cílem tohoto kurzu bylo získání jasné představy o řízení informační bezpečnosti v reálném prostředí. Ústředním bodem bylo zevrubné, v praxi aplikovatelné pochopení mezinárodní normy ISO/IEC 27001 vč. aktualizované přílohy A zrcadlící novou normu ISO/IEC 27002:2022. Speciální pozornost byla věnována řízení rizik, jakožto stěžejnímu procesu v ISMS. Výstup byl zcela splněn.
7	**Vytvoření oddělené, kontrolované datové infrastruktury pro klíčová oddělení školy** - V rámci bezpečnosti uvnitř datové infrastruktury VŠTE je každé oddělení definováno svou vlastní virtuální sítí (dále VLAN), kterou je odděleno od ostatních. Tyto VLANY slouží jako preventivní ochrana proti neoprávněnému přístupu, jelikož provoz mezi jednotlivými sítěmi je značně omezen, každá z VLAN má svá specifická pravidla a zásady. Provoz mezi jednotlivými sítěmi je povolen pouze nezbytným službám a důležitým systémům (včetně VIS). Veškerý provoz navíc prochází přes firewall, na kterém je monitorován a vyhodnocován a logován. Vyhodnocení probíhá v reálném čase a v případě narušení bezpečnosti dochází k upozornění IT pracovníků, kteří díky tomu mohou problém operativně řešit. Stejným způsobem jsou řešené i bezdrátové sítě, které jsou vzájemně oddělené a mají omezený přístup k datové infrastruktuře na základě toho, o jakou síť se jedná. Konkrétně například studentská wifi síť je omezena pouze na nezbytné služby a systémy, které studenti využívají pro své studium – zbytek sítě a infrastruktury je pro tuto studentskou síť nedostupný. Obdobným způsobem jsou ošetřena všechna klíčová oddělení školy s cílem zajistit co nejvyšší bezpečnost jak z pohledu uživatelů, tak z pohledu dat. Výstup byl zcela splněn.
8	**Vytvoření nezávislé datové infrastruktury pro situace s vysokou prioritou, nebo havárie** - Na základě zkvalitňování výuky a poskytovaných služeb na Vysoké škole technické a ekonomické se realizují nezávislé sekundární datové linky na odloučená pracoviště v rámci Českých Budějovic – Centrum odborné přípravy VŠTE v Českých Budějovicích, Coworking centrum VŠTE a Ústav podnikové strategie sídlící v ulici Nemanická. Výstup byl zcela 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.	Změna ve struktuře čerpání položky Osobní náklady	Změna ve struktuře čerpání osobních nákladů je způsobena rozhodnutím o využití zapojení pracovníků do projektu pouze přes DPP. Došlo tedy k přesunu finančních prostředků z položky 2.1 do položky 2.2.

2.	Změna ve struktuře čerpání položky Ostatní náklady	Navýšení rozpočtu v položce 2.5 na úkor ponížení rozpočtu v položkách 2.4 a 2.6. Důvodem změny byl důraz na provedení phishingové kampaně, na základě ceny služby jsme tedy omezili rozpočet na materiál a nevyužité prostředky na cestovné jsme taktéž přesunuli do rozpočtu na služby.

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)	224	5	-219	-44%
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)	76	265	189	38%
2.3	Odvody pojistného na veřejné zdravotní pojištění a pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a příděly do sociálního fondu	0	30	30	6%
	Ostatní:				
2.4	Materiální náklady (včetně drobného majetku)	85	46	-39	-8%
2.5	Služby a náklady nevýrobní	100	145	45	9%
2.6	Cestovní náhrady	15	9	-6	-1%
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	Mzdy (včetně pohyblivých složek) - náklad související s vyplacením odměny v projektu	5
2.2	Ostatní osobní náklady - náklady na DPP členů realizačního týmu projektu	265
2.3	Zákonné odvody - náklady SP, ZP a FKSP související s vyplacenými mzdy, DPP	30
2.4	Materiální náklady (včetně drobného majetku) - náklady spojené s nákupem techniky pro realizační tým řešící kyberbezpečnost na VŠTE	46
2.5	Služby a náklady nevýrobní - náklady spojené s realizací cvičné phishingové kampaně	145
2.6	Cestovní náhrady	9

* VŠ vyplní pouze žlutě podbarvená pole tabulky.

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