Budování situačního povědomí v kyberprostoru VVŠ a efektivní reakce na krizové situace

Mgr. František Hostek, manažer kybernetické bezpečnosti

20. 2. 2024

Univerzita Karlova

Cíle a projekty CRP – PS2

- UK odpovídalo za vedení pracovní skupiny PS-2 a splnění vlastních cílů

- CRP lze rozdělit na 3 samostatné projekty:

1. Klasifikace informací (cíl č. 10) a výstupy V8-V11
2. Řízení rizik dodavatelského řetězce (cíl č. 11) a výstup V12
3. Implementace výstupů ostatních pracovních skupin

CRP PS-2 – projektový tým

Univerzita Karlova

- Vedoucí projektového týmu
  - Mgr. František Hostek
- Realizátoři projektu za stranu UK
  - Ing. Vladimír Horák
  - Mgr. Jan Gruber
  - Mgr. Michal Voců
  - PhDr. Jan Víšek
- Zástupci jednotlivých fakult

Další zapojené role

- Projektový dohled
- Externí dodavatelé pro splnění cílů č. 10 a č. 11

CRP PS-2 – harmonogram

Výstupy projektu (VP)

V souladu s naplněním Rozvojového projektu na rok 2023 a dosažením klíčových cílů č. 10 a 11 je nezbytné zajisit dosažení níže uvedených výstupů.

CÍL	VP	NÁZEV	D	01/23	02/23	03/23	04/23	05/23	06/23	07/23	08/23	09/23	10/23	11/23	12/23
10	*V8*	Analýza současného stavu potřeb v oblasti klasifikace zabezpečovaných informací	●				▬	▬	▬	▬	▬				
10	*V9*	Návrh a definice postupů v rámci životního cyklu zabezpečovaných informací v digitální podobě	●					▬	▬	▬	▬				
10	*V10*	Studie proveditelnosti klasifikace informací doplněná o organizační i technická opatření	●								▬	▬	▬	▬	
10	*V11*	Návrh a ověření směrnice klasifikace informací	●									▬	▬	▬	
11	*V12*	Soubor bezpečnostních požadavků na dodavatele	●								▬	▬	▬	▬	▬

(D) Dodavatelé

● Ano ● Ne

Stav projektu

V přípravě | V realizaci | Dokončeno

CRP PS-2 – rozpočet

- Kapitálové finanční prostředky celkem – 0 Kč

- **Běžné finanční prostředky** celkem - 3.000.000 Kč

- Finanční prostředky pro **dosažení výstupů** č. 8–12 – 2.500.000 Kč
- Finanční prostředky pro **implementaci výstupů** – 500.000 Kč

Cíl č. 10 Klasifikace informací - obecné

- Holistické uchopení problematiky klasifiace informací tak, aby byla zajištěna důvěrnost zpracovávaných informací v prostředí VVŠ

- **Délka projektu**: 01-12/2023 (výstupy do 30.11.2023)

- **Projektový tým**: Projektové řízení a koordinace v rámci CRP: Mgr. Hostek
  Projektový dohled: externí
  Hlavní řešitel: Mgr. Hostek
  Řešitelský tým UK: Ing. Horák, Mgr. Gruber, Ing. Heidenreich
  Spolupracující řešitelský tým externí: dodavatel

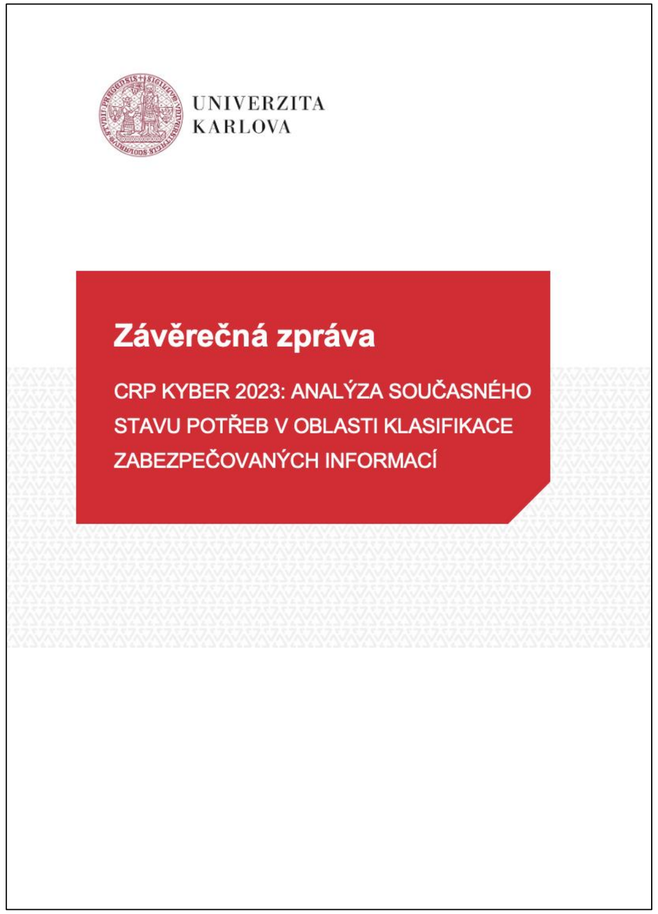
Cíl č. 10 Klasifikace informací - výstupy

- Výstupy projektu jsou:
  - V8 - Analýza současného stavu potřeb v oblasti klasifikace zabezpečovaných informací – **dokončeno**
  - V9 - Návrh a definice postupů v rámci životního cyklu zabezpečovaných informací v digitální podobě – **dokončeno**
  - V10 - Studie proveditelnosti klasifikace informací doplněná o organizační i technická opatření – **dokončeno**
  - V11 - Návrh a ověření směrnice klasifikace informací – **dokončeno**

V8 – výstup a zhodnocení

- Výstup V8 vznikl prostřednictvím detailní analýzy vnitřního prostředí UK a také prostřednictvím OSINT analýzy
- Na zpracování komplexního výstupu V8 se podílelo 15 fakult UK
- Zaměřeno na **18 kategorií zpracovávaných informací**:
  - 1) prezentace z přednášek, 2) výzkumná data/zprávy, 3) marketingové materiály, 4) informace o poskytovaných službách, 5) interní e-mailové korespondence, 6) zápisy z jednání, 7) vnitřní směrnice a předpisy, 8) vnitřní plány práce, 9) informace o projektech a grantech, 10) ekonomické údaje, mzdy a rozpočty, 11) smlouvy, 12) osobní údaje studentů, zaměstnanců, 13) čísla identifikačních průkazů, rodná čísla, 14) čísla kreditních karet, 15) software, zdrojové kódy aplikací, 16) bezpečnostní a provozní dokumentace ICT, 17) zdravotní data, citlivé osobní údaje, 18) přístupové údaje
- Důraz na **celkový životní cyklus informací**:
  - vznik (v jakých informačních systémech informace vznikají)
  - přenos (jakými způsoby jsou informace předávány a chráněny)
  - ukládání (jakými způsoby jsou informace ukládány a chráněny)
  - Likvidace (v jakých informačních systémech a jak se informace odstraňují)

V8 – výstup



UNIVERZITA KARLOVA

Závěrečná zpráva

CRP KYBER 2023: ANALÝZA SOUČASNÉHO STAVU POTŘEB V OBLASTI KLASIFIKACE ZABEZPEČOVANÝCH INFORMACÍ

5. ZÁVĚR

Analýza současného stavu prostředí poskytla ucelený přehled o zpracovávaných informací na Univerzitě. V rámci dotazníkového šetření byla sesbírána, zkonsolidována a vyhodnocena data od jednotlivých fakult. Ze získaných dat lze s jistotou získat více pohledů a souvislostí.

Tato závěrečná zpráva měla za cíl poskytnout holistický pohled na prostředí Univerzity. Začlenění veškerých detailů by znamenalo enormní nárůst počtu stran a ztrátu přehlednosti zprávy. V případě potřeby provedení dalších analýz lze využít excelovský soubor analýza informací, který je uveden v příloze č. 2.

Celkem se do projektu zapojilo 15 fakult z celkových 17, přičemž byl kladen důraz ze strany zástupců jednotlivých fakult v rámci svých možností, co nejpřesněji odpovědět na co nejvíce otázek. Dané fakulty, vyplnily minimálně část pro správce ICT. Detailní přehled projektové řízení a procentuální vyplnění dotazníku jednotlivých fakult lze najít v dokumentu Harmonogram v příloze č. 3.

Při sebelepší snaze mohou být vstupy zkreslené či neúplné z rozličných důvodů, jako je například nedostatečné porozumění obsahu či smyslu otázek, nevhodný výběr dotazovaných osob dané kategorie informací či problematiky, časové a personální vytížení z důvodu aktuálně probíhajícího zkouškového období v době vyplňování dotazníků a v neposlední řadě přirozenou chybovost lidského faktoru. Shromážděná data a návazné grafy tedy nelze považovat za 100% přesný obraz reálného stavu daných oblastí a při jejich interpretaci je vhodné zachovat určitý odstup a rezervu pro nepřesnosti.

Projekt naplnil své cíle. Byly identifikovány informační systémy a aplikace, ve kterých se citlivé kategorie informací zpracovávají. I když nelze s jistotou říct, zda došlo k identifikaci veškerých systémů a aplikací, poskytují výsledky velmi dobrý základ pro rozhodování a návrh vhodných bezpečnostních opatření.

Z výsledků byla identifikována potenciální rizika prostředí a byly odhaleny nedostatky v oblasti bezpečnosti informací. Přestože má kybernetická bezpečnost silnou podporu rektorátu, aktuálně je způsob řízení životního cyklu informací na Univerzitě decentralizovaný, což znamená, že každá fakulta má svůj

vlastní způsob řízení a postupy pro klasifikaci informací. Tento decentralizovaný model má určité výhody, jako je například schopnost přizpůsobit se specifickým potřebám jednotlivých fakult a oddělení. Pro efektivní implementaci tohoto modelu v současnosti chybí univerzální předpis nebo politika, která by stanovila základní bezpečnostní principy napříč celou Univerzitou. Fakulty by pak mohly formulovat a uplatňovat své předpisy v souladu s centrálním dokumentem.

Nicméně v poslední době dochází k tvorbě dokumentace. Příkladem je dokument Data Management Guidelines popisovaný v kapitole Režim práce s dokumenty, který vznikal souběžně a nezávisle s touto zprávou. V případě úspěšné distribuce napříč součástmi Univerzity lze předpokládat, že i podobné dílčí dokumenty mohou znatelně zlepšit bezpečnost i produktivitu Univerzity.

Na základě identifikovaných zjištění a vstupních informací doporučujeme navázat na tento projekt a vypracovat seznam doporučení bezpečnostních opatření pro zajištění bezpečnosti informací v rámci jejich životního cyklu.

V9 – výstup a zhodnocení

- Výstup V9 vznikl na základě výstupu V8 a obsahuje soubor vhodných a praktických technických a organizačních opatření
- Zaměřeno na **11 identifikovaných nosičů informací**:
  - 1) koncová zařízení (počítač, notebook), 2) mobilní zařízení (tablet, mobil), 3) USB externí disk, 4) CD/DVD, 5) Google Workspace (Google Disk) 6) Microsoft365/Office 365 (OneDrive, SharePoint, Teams), 7) Cesnet, 8) Dropbox, Ulož.to a další cloudová úložiště bez smluvního vztahu, 9) Git, GitHub, Bitbucket a další úložiště zdrojového kódu, 10) NAS, 11) SAN
- Opatření jsou navržena u nosičů informací vždy v rámci všech oblastí celého životného cyklu pro:

  a) vznik informací

  b) přenos informací

  c) ukládání informací

  d) likvidaci informací
- **Organizační a technická opatření** obsahují:
  - Školení zaměstnanců, řízení přístupů, odchod zaměstnance (off-boarding), řízení dodavatelů, řízení mobilních a koncových zařízení, řízení zranitelností, log management, kryptografie, přístupové údaje

V9 – výstup

UNIVERZITA KARLOVA

Závěrečná zpráva

CRP KYBER 2023: NÁVRH A DEFINICE POSTUPŮ V RÁMCI ŽIVOTNÍHO CYKLU ZABEZPEČOVANÝCH INFORMACÍ V DIGITÁLNÍ PODOBĚ

5. ZÁVĚR

V tomto dokumentu byla navržena řada opatření s cílem zvýšit bezpečnost informací v rámci jejich životního cyklu. Navrhovaný soubor opatření byl snahou se stát komplexním, avšak zároveň srozumitelným a snadno proveditelným a praktickým průvodcem pro zlepšení bezpečnosti i produktivity práce na UK.

Každý aspekt zabezpečení, od řízení dodavatelů, přes řízení mobilních zařízení až po správu certifikátů a používání kryptografických prostředků, byl pečlivě zvážen s ambicí o významné zlepšení dané oblasti. Mimo jiné byla také představena opatření pro bezpečné zacházení s různými technologiemi a platformami včetně repozitářů zdrojového kódu, NAS, SAN, cloudových platforem CESNET a Microsoft 365 a interních aplikací.

Prostřednictvím správné klasifikace informací je možné lépe rozumět, jaké informace jsou pro UK nejcennější a jak je také nejlépe ochránit. Navrhovaná opatření se zaměřují na pravidelnou revizi a aktualizaci klasifikačních schémat, což je klíčové pro zajištění, že tato schémata zůstanou relevantní a efektivní v dynamickém prostředí UK.

Podrobná klasifikace informací také umožňuje větší kontrolu nad přístupem k citlivým informacím. Použitím klasifikace informací a souvisejících přístupových práv lze zlepšit ochranu důvěrných informací před neoprávněným přístupem osob nebo únikem informací.

V rámci navrhovaných opatření je kladen na vytváření jasných a konzistentních pravidel pro klasifikaci a manipulaci s informacemi.

Projekt splnil své cíle a zadání. Navrhovaná opatření pokrývají širokou škálu témat a poskytují konkrétní a praktické rady pro zlepšení bezpečnosti na UK. Autoři dokumentu se snažili zohlednit celý životní cyklus informací, od jejich vzniku, přes přenos a ukládání, až po likvidaci. Také přidali množství obecných opatření, která přímo nesouvisí s konkrétní fázi životního cyklu informací.

UNIVERZITA KARLOVA

V další fázi tohoto projektu bude vypracována studie proveditelnosti, která se podrobněji zabývá otázkami, zda je implementace navržených opatření proveditelná a jakými způsoby je lze implementovat.

V10 – výstup a zhodnocení

- Výstup V10 vznikl na základě výstupu V8 a V9 a představuje zpracovanou studii proveditelnosti ve formátu dotačních titulů pro potřeby klasifikace informací
- Cílem projektu bylo, na základě výstupů z předchozích dílčích fází V8 a V9, ověřit implementaci navržených bezpečnostních opatření v oblasti klasifikace informací a ochrany dat, a to zejména ověření zavedení nástroje pro klasifikaci informací v prostředí Univerzity

V10 – výstup

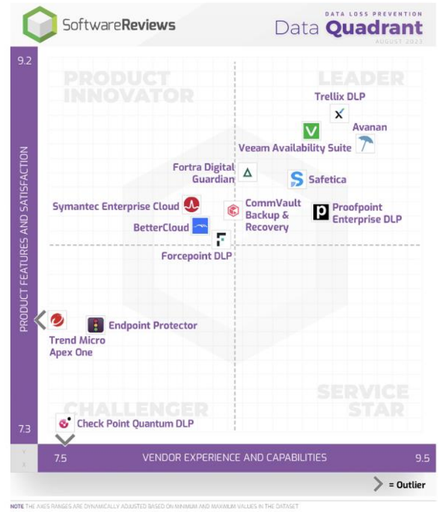
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

UNIVERZITA KARLOVA

CENTRALIZOVANÝ ROZVOJOVÝ PROGRAM PRO VEŘEJNÉ VYSOKÉ ŠKOLY

CRP Kyber 2023: Studie proveditelnosti klasifikace informací doplněná o organizační i technická opatření

OBSAH



Obrázek 3: Magický kvadrant DLP 2023

Obrázek 4: Srovnávač DLP Gartner

V11 – výstup a zhodnocení

- Výstupem V11 jsou tři dokumenty, které mohou být implementovány v rámci závazných dokumentů VVŠ:
  - Směrnice klasifikace informací
  - Průvodce klasifikace informací
  - Průvodce pro bezpečné nakládání s informacemi
- Cílem projektu bylo zpracovat návrh závazného dokumentu ve formě směrnice klasifikace informací použitelné pro VVŠ

VII – výstup

Interní TLP:GREEN

Opatření rektora č. XX/2023

Název: Směrnice klasifikace informací

Gestor: DOPLNIT

Účinnost: TBD

ČÁST I. ÚVODNÍ USTANOVENÍ

Čl. 1 Účel dokumentu

1. Tato Směrnice klasifikace informací (dále jen „Směrnice“) je navazujícím dokumentem Politiky ISMS a má za cíl stanovit pravidla a postupy pro ochranu informací v celém jejich životním cyklu. Tj. stanovit pravidla pro klasifikaci aktiv (informací), určit vhodná ochranná opatření k manipulaci, likvidaci a používání aktiv a zajistit kontrolu a dodržování těchto opatření.
2. Směrnice naplňuje požadavky vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat podle § 4 písm. h) – j) této vyhlášky.

Čl. 2 Rozsah

1. Rozsah Směrnice je vymezen pro Univerzitu (dále jen „Univerzita“) a všechny její součásti. Směrnice je závazná pro všechny zaměstnance (dále i „uživatel“), kteří přicházejí do styku s aktivy Univerzity. Směrnice je především určena pro garanty aktiv a vedoucí zaměstnance, kteří pravidla a postupy aplikují v praxi a kteří zaměstnancům poskytují podporu během životního cyklu informací.

Čl. 3 Struktura dokumentu

Směrnice je rozdělena na následující části:

a. Část II. popisuje a znázorňuje vztah bezpečnostních rolí k ochraně a klasifikaci aktiv. Role a odpovědnosti vychází z Politiky ISMS a Směrnice je dále rozvádí.
b. Část III. určuje požadavky na správu a inventarizaci informací.
c. Část IV. určuje úrovně klasifikace informací z pohledu důvěrnosti, popisuje dopady a další aspekty, podle kterých uživatelé určí odpovídají stupeň důvěrnosti.
d. Část V. určuje pravidla pro nakládání s aktivy během jejich životního cyklu včetně konkrétních scénářů, a to nejen z pohledu důvěrnosti, ale také z pohledu integrity a dostupnosti.
e. V přílohách jsou vytvořeny dva průvodce, které jasně, stručně a přehledně poskytují souhrn pravidel a postupů klasifikace a značení informací a manipulaci s nimi. Jedná se o přílohu č. 10 – Průvodce klasifikace informací a příloha č. 11 – Průvodce pro bezpečné nakládání s informacemi.

ČÁST II. ROLE A ODPOVĚDNOSTI

Veřejné TLP:CLEAR

Bezpečnost informací – Průvodce klasifikace informací

***Poznámka**: Traffic Light Protocol (TLP) slouží ke snadnému určení míry důvěrnosti informací a možností jejich dalšího sdílení.*
Během životního cyklu informace může dojít ke změně klasifikačního stupně pouze se souhlasem tvůrce informace.

Klasifikace		
L1 (Veřejné) Informace jsou veřejně přístupné nebo byly určeny ke zveřejnění.	L2 (Interní) Interní informace mohou být sděleny v rámci univerzitu a případně také s dalšími partnerskými subjekty.	L3 (Chráněné) Chráněné informace, určené pouze pro omezenou skupinu osob s potřebou vědět (need-to-know).
Narušení důvěrnosti informací neohrožuje oprávněné zájmy univerzity.	Zpřístupnění mimo univerzitu nezpůsobí přímou škodu (finanční, morální, právní apod.).	Zpřístupnění mimo danou skupinu oprávněných osob velmi pravděpodobně způsobí škodu velkého rozsahu.
Značení: „Veřejné TLP:CLEAR“	**Značení**: „Interní TLP:GREEN“	**Značení**: „Chráněné TLP:AMBER“ a „TLP:AMBER+STRICT (omezení sdílení mimo univerzitu)“
Příklady • Výzkumná data / zprávy – data získaná výzkumem, výsledky experimentů, analytické zprávy, která **jsou** určená ke zveřejnění. • Prezentace z přednášek – informace, grafy, obrázky a texty používané pro vzdělávací nebo informační účel. • Smlouvy - smlouvy, dohody a další právní dokumenty, které **jsou** určené ke zveřejnění. • Marketingové materiály – propagační brožury, letáky, webové stránky, prezentace nebo jiné materiály používané k propagaci produktů, služeb nebo značky univerzity. • Informace o poskytovaných službách – služby mimo výuku (např. knihovny, stravování, poradenství).	**Příklady** • Interní e-mailová korespondence – e-maily a komunikace mezi zaměstnanci nebo studenty pro interní účely včetně diskusí, sdílení dokumentů a dalších interních informací, různá e-mailová řešení a SW. • Zápisy z jednání – záznamy, poznámky a protokoly z jednání, schůzek a porad vedení. • Vnitřní plány práce, poznámky – plány, organizační struktury a činnosti na další období. • Vnitřní směrnice a předpisy – interní dokumenty, směrnice, politiky a předpisy, které stanovují pravidla a postupy pro chod univerzity a zajištění souladu s předpisy.	**Příklady** • Výzkumná data / zprávy – data získaná výzkumem, výsledky experimentů, analytické zprávy, která **nejsou** určená ke zveřejnění. • Informace o projektech a grantech – jejich popis, cíle, finanční plány, harmonogramy. • Ekonomické údaje, mzdy, rozpočty. • Smlouvy – smlouvy, dohody a další právní dokumenty, které **nejsou** určené k zveřejnění. • Osobní údaje studentů, zaměstnanců, spolupracovníků. • Čísla kreditních karet. • Software, zdrojové kódy aplikací – software, včetně zdrojových kódů aplikací a knihoven. • Bezpečnostní a provozní dokumentace IT systémů. • Zdravotní data, citlivé osobní údaje. • Přístupové údaje (např. hesla či šifrovací klíče) k důležitým systémům a citlivým datům.
Seznamte se s pravidly: Kompletní pravidla Směrnice klasifikace informací ODKAZ	**Vyhledejte pomoc**: Pokud máte dotazy nebo si nevíte rady, jak informace oklasifikovat, obraťte se na svého vedoucího.	**Používejte správný úsudek**: Výše uvedené seznamy jsou pouze příklady, nikoliv definitivní klasifikace!

Veřejné TLP:CLEAR

Bezpečnost informací – Průvodce pro bezpečné nakládání s informacemi

Obecná opatření pro neveřejné informace:
- Sdílejte informace pouze s autorizovanými osobami a používejte k tomu výhradně pracovní uživatelský účet univerzity.
- Dokumenty ukládejte do zabezpečených prostor jako stůl/kancelář/skříň.
- Ztrátu nebo zneužití informací okamžitě hlaste svému vedoucímu.

Povolené způsoby nakládání s informacemi		
Aktivita	L2 (Interní)	L3 (Chráněné)
Sdílení informací se zaměstnanci univerzity	Používejte oficiálně schválený nástroj MS O365 (Outlook e-mail, Teams, SharePoint, OneDrive), sdílené disky univerzity, cloudovou službu CESNET a **nepoužívejte** veřejná úložiště (DropBox, Uložto, Úschovna…). Ke sdílení **nepoužívejte** veřejné odkazy, ale e-mail adresáta, pokud je to možné.	Používejte **pouze** oficiálně schválený nástroj MS O365 (Outlook e-mail, MS Teams, SharePoint, OneDrive), sdílené disky univerzity, cloudovou službu CESNET a **nepoužívejte** veřejná úložiště (DropBox, Uložto, Úschovna…). Ke sdílení **nepoužívejte** veřejné odkazy, ale e-mail adresáta. Pokud chcete použít veřejný link, tak se obraťte na svého nadřízeného.
Sdílení informací mimo univerzitu	Stejné jako „Sdílení informací se zaměstnanci univerzity“. Univerzita **musí** mít s třetí stranou podepsanou smlouvu o mlčenlivosti (NDA) nebo uvedené ustanovení o mlčenlivosti přímo ve smlouvě. Informace lze sdílet **pouze** se souhlasem tvůrce informace.	Stejné jako „Sdílení informací se zaměstnanci univerzity“. Univerzita **musí** mít s třetí stranou podepsanou smlouvu o mlčenlivosti (NDA) nebo uvedené ustanovení o mlčenlivosti přímo ve smlouvě a sdílet informace lze **pouze** ve smluvně definovaném rozsahu se souhlasem tvůrce informace.
Přenos informací	Informace posílejte autorizovaným příjemcům pomocí e-mailu (MS Outlook), nebo použijte OneDrive/Teams/SharePoint/CESNET, která jsou vhodné pro sdílení velkých souborů.	**Pouze zašifrované** informace posílejte autorizovaným příjemcům pomocí e-mailu (MS Outlook), nebo použijte OneDrive/Teams/SharePoint/CESNET… K šifrování lze použít např. nástroje WinRAR, ZIP, PGP.
Sdílení listinných dokumentů	V uzavřené obálce/krabici.	V zapečetěné obálce/krabici.
Ukládání informací v mobilních telefonech/PC	Pouze na pracovních zařízeních univerzity.	Pouze na pracovních zařízeních univerzity.
Ukládání informací na přenosná média	Pouze na pracovních a označených zařízeních univerzity.	Pouze na pracovních a označených zařízeních univerzity, které **musí být šifrované.**
Likvidace informací	Listinné dokumenty skartujte. Nefunkční zařízení odevzdejte IT oddělení.	Listinné dokumenty skartujte. Nefunkční zařízení odevzdejte IT oddělení.
Seznamte se s pravidly: Kompletní pravidla Směrnice klasifikace informací ODKAZ	**Vyhledejte pomoc**: Pokud máte dotazy nebo si nevíte rady, jak s informacemi nakládat, obraťte se na svého vedoucího.	

Cíl č. 11 Řízení rizik dodavatelského řetězce - obecné

- Vydefinování rizik spojených s dodavateli aktiv, určení typických smluvních vztahů v prostředí VVŠ a návrh vhodných bezpečnostních opatření pro smluvní vztahy s dodavateli.

- **Délka projektu**: 09-12/2023

- **Projektový tým**: Projektové řízení a koordinace v rámci CRP: Mgr. Hostek
  Projektový dohled: externí
  Hlavní řešitel: Mgr. Jindra
  Řešitelský tým UK: Mgr. Jindra
  Řešitelský tým externí: dodavatel

V12 – výstup a zhodnocení

- Výstupem V12 je identifikace běžných smluvních vztahů s dodavateli. Dále pak definování rizikových scénářů vyplývajících ze smluvních vztahů s dodavateli.
- Závěrem dojde k vytvoření seznamu vhodných bezpečnostních opatření pro smluvní vztahy.

- Stav: – **dokončeno**

Implementace výstupů ostatní pracovních skupin

- Převzetí a implementace společných výstupů vytvořených pracovními skupinami ostatních VVŠ.

- **Délka projektu**: 01-12/2023

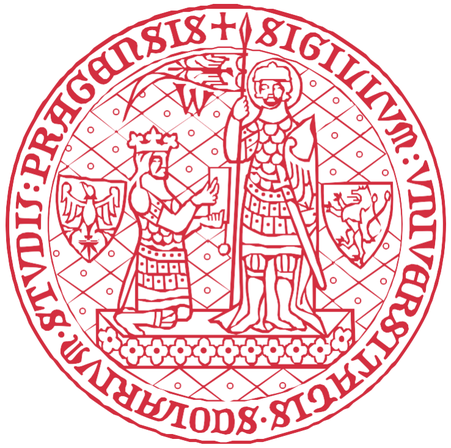
- **Projektový tým**: Projektové řízení a koordinace v rámci CRP: Mgr. Hostek

  Hlavní řešitel: Ing. Horák

  Řešitelský tým UK: Ing. Horák, Mgr. Gruber, Mgr. Voců, PhDr. Víšek

Implementace výstupů ostatní pracovních skupin

1. Validace postupů pro ověřování dodržování vybraných bezpečnostních politik v prostředí UK
2. Využití analýzy dopadů nové směrnice NIS 2 pro přípravu UK na nové legislativní změny a dopady
3. Využití výstupů rešerše nástroje pro řízení aktiv pro volbu vhodného nástroje (instalace a otestování potenciálně vhodných opensource nástrojů z přehledu - Netbox, Snipe-IT, SySAid, Spiceworks) a doporučení vhodného postupu pro nasazení v prostředí UK
4. Využití návrhu postupu nasazení automatizovaného nástroje pro vyhledávání a evidenci aktiv
5. Využití výstupů v oblasti řízení privilegovaných účtů systémem PIM/PAM pro výběr vhodného nástroje v prostředí UK
6. Využití výstupů rešerše současných řešení pro nasazení MFA autentizace pro výběr vhodného nástroje v prostředí UK
7. Ověření použitelnosti krizových plánů pro zajištění kontinuity činností UK
8. Využití výstupu sada analytických pohledů pro potřeby zajištění efektivní reakce na provozní anomálie a bezpečnostní události – implementace vybraných v prostředí univerzity (platforma SIEM QRadar)



Děkuji Vám za pozornost

Mgr. František Hostek
Manažer kybernetické bezpečnosti