UNIVERZITA
KARLOVA

Prezentace projektu CRP 2022

Podpora zavedení systému řízení bezpečnosti informací v prostředí VVŠ

Ing. Vladimír Horák
Ústav výpočetní techniky UK vhor@cuni.cz

21. 2. 2023

Univerzita Karlova

SŘBI alias ISMS

Systém řízení bezpečnosti informací (Information Security Management System - ISMS) je **dokumentovaný systém**, ve kterém jsou chráněna definovaná **informační aktiva**, jsou **řízena rizika bezpečnosti informací** a zavedená **opatření jsou kontrolována**.

(wikipedia.org)

Proč musí UK zavést SŘBI?

- Vykonává agendy orgánu státní moci
- Neodkáže ji vykonávat bez počítačů
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat
- NÚKIB (Národní úřad kybernetické bezpečnosti)

Stav zavedení SŘBI na UK ke konci 2022

- Určené VIS (Významné informační systémy) a nahlášené NÚKIBu
- Obsazené pozice Manažera KB a Architekta KB
- Ustanovený výbor kybernetické bezpečnosti
- Připraveny zastřešující dokumenty SŘBI (neschválené!)
- Probíhá identifikace a analýza rizik
- Probíhá příprava bezpečnostních politik

Představení projektu

- Navazuje na CRP-KYBER21
- Koordinující VŠ: MU
- Pracovní skupiny:
  - Procesní aspekty SŘBI
  - Bezpečnostní politiky
  - Osvěta a vzdělávání
  - Technicko-personální
- Pravidelné workshopy (jednou za 2 týdny)
  - Přehled aktuálního dění v oblasti KB
  - Prezentace pracovních skupin
  - Prezentace bezpečnostních technologií, CESNET, NÚKIB…

Výstupy dílčí části projektu

1. Nasazení vybraných doporučených nástrojů na podporu zavedení SŘBI (systému řízení bezpečnosti informací)

V rámci projektu jsme se s nástroji na podporu zavedení SŘBI seznámili a některé otestovali. Kvůli zpoždění nasazení SŘBI (zatím nebyly schválené zastřešující dokumenty) jsme zatím žádný nenasadili v ostrém provozu. Předpokládáme nasazení v roce 2023.

Výstupy dílčí části projektu

2. Implementace vybraných bezpečnostních politik

Kvůli zpoždění nasazení SŘBI (zatím nebyly schválené zastřešující dokumenty) jsme zatím žádnou bezpečnostní politiku neimplementovali. Předpokládáme implementaci v roce 2023.

Připravili jsme dvoufaktorovou autentikaci ve významném informačním systému CAS (Centrální autentizační služba) (aplikace, token, sms). Předpokládáme nasazení v roce 2023 v návaznosti na příslušnou bezpečnostní politiku.

Výstupy dílčí části projektu

3. Přizpůsobení a nasazení vzdělávacích kurzů pro specifické cílové skupiny

Základní kurzy obecného charakteru pro zaměstnance jsou funkční a používané. Řešili jsme napojení základního kurzu na systém personalistiky pro možnost kontroly jeho absolvování.
Plánovaná pravidelná školení dalších cílových skupin (garantů VIS a vedoucích pracovníků) zatím neprobíhala kvůli zpoždění nasazení SŘBI. Proběhla jednorázová školení IT pracovníků a vedoucích pracovníků univerzity.

Výstupy dílčí části projektu

4. Audit/penetrační test systému CAS (Centrální autentizační služba)

Vzhledem k dlouhým objednacím lhůtám penetračních testů byl v roce 2022 proveden jen audit významného informačního systému CAS (Centrální autentizační služba).

Na nejbližší možný termín v roce 2023 byl objednán penetrační test systému dalšího významného informačního systému ESS (Elektronická spisová služba).

Výstupy dílčí části projektu

5. Pokročilé zabezpečení prostředí MS 365

Byla provedena analýza aktuálních smluvních podmínek a smluvních vztahů univerzita - Microsoft a analýza celouniverzitního tenantu MS 365, ze které vyplynuly požadavky na další rozvoj včetně zabezpečení.
Byly využity materiály projektu a doporučení, především související s ochranou proti phishingu.
Napojili jsme MS 365 na systém SIEM a CSIRT tým si doplnil interní postupy pro řešení incidentů v tomto prostředí.

Čerpání rozpočtu

Přidělená (a vyčerpaná) dotace	380
Mzdy	227
Dohoda o pracovní činnosti	44
Pojistné…	97
Drobný materiál (tokeny, síťové karty)	12

Přínosy projektu

- Vzorové dokumenty k SŘBI, vzorové bezpečnostní politiky
- Výukové materiály ke kyberbezpečnosti – k dispozici
- Informace o aktuálních kyberbezpečnostních hrozbách, diskuse a výklady k reaktivním opatřením NÚKIBu
- Přehled o stavu kyberbezpečnosti na jiných vysokých školách, kontakty

Děkuji vám za pozornost a za podporu!