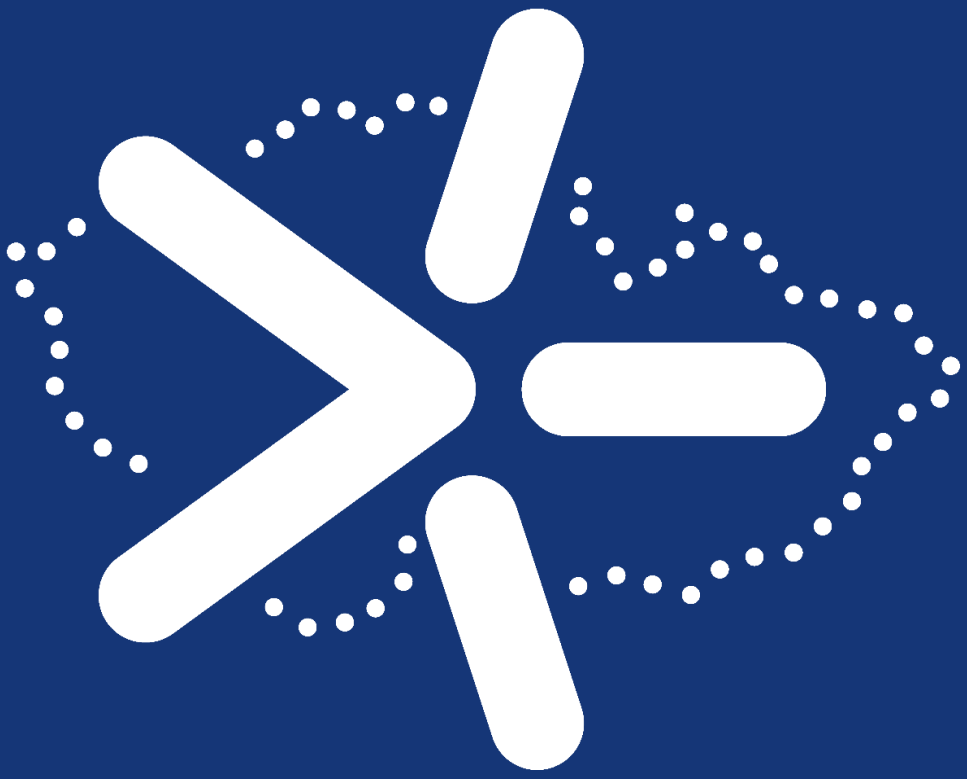

VÝSTUP Č. 13

Popis procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů.

Cíl: Nastavení procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů prostřednictvím zabezpečeného úložiště s cílem eliminace systémových rizik a působení nežádoucích vnějších vlivů.

Pracovní skupina 3 NPO-C2
vlachynsky@rektorat.czu.cz

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

Studijní dokumenty v kontextu výstupu č.13

Studijní dokumenty lze pro účely tohoto výstupu chápat jako záznamy událostí souvisejících s jednotlivými studenty a jejich studiem na VVŠ. Tyto dokumenty byly v tradičním pojetí uchovávány v listinné podobě v tzv. „složce studenta“. Pojem studijní dokumenty může být v současnosti poněkud matoucí, neboť mimo tradiční písemnosti zahrnuje také data, která jednotlivé události zaznamenávají ve studijních informačních systémech (SIS), obvykle ve formě databázových záznamů (typickým případem jsou záznamy o absolvovaných zkouškách studenta). Z těchto dat často vznikají dokumenty (listiny) pouze v reakci na konkrétní žádosti studentů (např. potvrzení o studiu, výpis studijních výsledů) nebo v případě, kdy univerzita vystupuje vůči studentovi jako orgán veřejné moci, a forma dokumentu je tedy při komunikaci vyžadována (např. rozhodnutí o ukončení studia).

Studijní dokumenty pro potřeby tohoto projektu nezahrnují veškeré materiály, které slouží jako podpora vzdělávání (skripta, prezentace, záznamy přednášek, aj.), slouží pro potřeby akreditace (sylaby předmětů, struktura studijního programu/oboru).

Procesy bezpečného předávání a dlouhodobého uchování studijních dokumentů

Pro nastavení procesů bezpečného předávání a dlouhodobého uchování studijních dokumentů je nezbytné zvážit několik základních faktorů a provést nejméně následující činnosti:

- Identifikace a klasifikace sledovaných dokumentů
- Přístupová kontrola
- Zajištění bezpečného přenosu
- Dlouhodobé uchování a archivace, zálohování a obnova ze zálohy

Dílčí procesy vzniku a následné manipulace s jednotlivými dokumenty se mohou v rámci jednotlivých VVŠ lišit, následující pasáže se tedy zaměřují na obecné kroky, které by měly být pro všechny VVŠ společné.

Identifikace základních studijních dokumentů

Pracovní skupina v rámci výstupu vytvořila **přehledový dokument**, který obsahuje přehled základních studijních dokumentů, které vznikají během studia na VVŠ se zařazením do kontextu studijní agendy. Tento seznam nemusí být úplný, obsahuje však základní dokumenty, které by měly být pro jednotlivé VVŠ společné. Pro každý studijní dokument jsou evidovány rámcové informace, jako například kdo a jak dokument vytváří, komu slouží, jaké ochranné mechanismy se doporučují pro zajištění původu a integrity dokumentu, nebo jaká je doba archivace. Pro stanovení pravidel na ochranu jednotlivých dokumentů je také vhodné dokumenty klasifikovat, např. dle vodítek v příloze č. 1 k vyhlášce č. 82/2018 Sb.

Tento přehledový dokument slouží jako nezávazný informační materiál pro VVŠ, který lze využít při kontrole shody s požadavky na elektronickou evidenci studijních dokumentů a pro audit vlastních vnitřních procesů a práce s dokumenty.

Kompletní tabulka je k dispozici jako část výstupu s názvem „Studijní dokumenty".

[Sem zadejte text.]

Analýza rizik v souvislosti se zpracováním studijních dokumentů

Pro stanovení vhodných metod zabezpečení přenosu studijních dokumentů, úložiště studijních dokumentů a aktiv, která tyto 2 služby podporují je vhodné vycházet ze standardního přístupu založeném na hodnocení rizik. Pracovní skupina v rámci této činnosti vytvořila tabulkovou šablonu, která je nazvána „Analýza rizik spojená se studijními dokumenty". Tento dokument vychází z požadavků norem řady ISO/IEC 27000, Zákona o kybernetické bezpečnosti a Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Cílem šablony je umožnit snadnou identifikaci relevantních opatření na základě hodnocení primárního a souvisejícího podpůrného aktiva, dle přiložené metodiky pro hodnocení aktiv a identifikovat tak oblasti, které mohou vést k mitigaci systémových rizik.

Pojmy vyskytující se v analýze rizik:

Opatřeními budou pokryta rizika od úrovně včetně – nastavení základní hranice pro pokrytí rizik relevantními opatřeními, rizika pod rozhodnou hranicí jsou v souvislosti s hodnoceným systémem považována za nevýznamná a jsou akceptována.

Kategorie rizika – stupnice hodnot pro kategorie rizika k příslušné hodnotě opatření.

Primární aktivum – PriA – proces nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém. Pro příklad je uvedeno archetypální primární aktivum „Studijní dokumenty".

Důležitost aktiva – součet hodnot dostupnost, důvěrnost a integrita pro výpočet hodnoty aktiva.

Podpůrné aktivum – PodA – technické aktivum (typicky informační systém, software, hardware a.j.) podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. Pro příklad uvedeno podpůrné aktivum „Studijní informační systém" (SIS).

Hrozba – potenciální příčina kybernetické bezpečnostní události nebo incidentu, která může způsobit škodu.

Riziko – možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.

Riziko aktiva – výpočet hodnoty aktiva součinem Důležitosti aktiva, dopadu, hrozby a zranitelnosti.

[Sem zadejte text.]

Tabulková šablona analýza rizik – popis jednotlivých listů

Hodnocení primárního aktiva – na uvedeném listu je nutno vyplnit hodnoty pro „Dostupnost", „Důvěrnost" a „Integrita" dle přiložené **Metriky pro hodnocení PriA a PodA** na samostatném listu. Tyto hodnoty lze také vyvodit dle detailnějšího rozboru těchto kritérií v přehledové tabulce níže, na základě maximalizačního kritéria. Dané aktivum hodnotí vlastník/správce aktiva společně s manažerem kybernetické bezpečnosti nebo jiným určeným pracovníkem. Důležitost aktiva je výsledná suma vyplněných hodnot, která je dále propisována do listu **Aplikovatelnost opatření**.

Hodnocení podpůrného aktiva – na uvedeném listu je nutno vyplnit hodnoty pro „Dopad", „Hrozba" a „Zranitelnost" v kombinaci s jednotlivými hrozbami dle přiložené **Metriky pro hodnocení PriA a PodA** na samostatném listu. Dané podpůrné aktivum hodnotí vlastník/správce aktiva společně s manažerem kybernetické bezpečnosti nebo jiným určeným pracovníkem. Hodnoty jsou dále propisovány do listu **Aplikovatelnost opatření**.

Aplikovatelnost opatření – na uvedeném listu je dále pracováno s kombinací vyplněných hodnot pro primární a podpůrné aktivum. Výsledná hodnota „Riziko aktiva" je součinem těchto hodnot. Pokud výsledná hodnota překročí definovanou hranici z listu **Parametry**, stane se daná hrozba relevantní pro dané aktivum a budou navržena relevantní opatření. Tyto opatření se dle důležitosti seřadí na listu **Doporučená opatření**.

Doporučená opatření – na uvedeném listu jsou seřazena vybraná opatření podle výsledku hodnocení. Opatření jsou seřazena dle důležitosti sestupně. Tabulka obsahuje ID opatření, název opatření, definici opatření a účel opatření dle definicí norem řady ISO/IEC 27000. S těmito opatřeními je doporučeno dané VVŠ dále pracovat pro eliminaci systémových rizik a působení nežádoucích vlivů z vnějšího prostředí.

Doporučené parametry pro bezpečné předání studijních dokumentů

Pro bezpečné předání dokumentů je vhodné využívat možnosti šifrovaného přenosu dat. V případě zabezpečené komunikace pomocí protokolu HTTP je doporučeno využívat protokoly TLS 1.2 a vyšší (TLS 1.3), starší protokoly SSL 2.0, SSL 3.0, TLS 1.0 a TLS 1.1 již nejsou považovány za bezpečné, a nejsou tak již doporučovány pro použití. Dále jsou doporučeny následující šifrovací sady použité v rámci těchto protokolů (zdroj: SSL/TLS Recommended Cipher Suites | Tenable®):[1]

TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

V případě nutnosti podpory starších klientů, kteří mohou mít problém s navázáním zabezpečené komunikace, mohou být vyžadovány méně bezpečné šifrovací sady.

Neméně důležité je rovněž udržovat aktuální verzi knihoven zajišťujících šifrování (např. OpenSSL) s bezpečnostními opravami.

Privátní klíč a odpovídající certifikát by měl po celou dobu své životnosti být dostatečně silný, doporučuje se tak využívat velikost klíče minimálně 2048 bitů. Privátní klíč je nutné zabezpečit na úrovni systému souborů pomocí oprávnění, případně jinými technickými a administrativními

[1] https://www.tenable.com/plugins/nessus/156899

opatřeními kvůli ochraně proti neoprávněnému získání a potenciálnímu zneužití klíče. Certifikát by měl využívat hashovací algoritmus minimálně SHA-256, starší algoritmy (MD5, SHA-1) již nejsou doporučovány. Certifikát by měl být vydán certifikační autoritou, která je pro všechny klienty důvěryhodná.

U citlivých dokumentů je též doporučeno zabránit ukládání těchto informací do cache internetového prohlížeče nebo webové proxy, které mohou být správci nakonfigurovány, aby prováděli dešifrování zabezpečené komunikace. V tomto případě je třeba do HTTP hlaviček odpovědi na straně serveru nastavit následující:

Cache-Control: no-cache, no-store, must-revalidate

Pragma: no-cache

Expires: 0

Dalším doporučením je vyžadovat pouze zabezpečené připojení pomocí nastavení konfigurace HSTS (HTTP Strict Transport Security).

Doporučené parametry pro bezpečné uchování studijních dokumentů

Dokumenty uložené v rámci informačního systému je doporučeno šifrovat v závislosti na jejich charakteru jejich dat. Ne všechny dokumenty mohou totiž obsahovat citlivé údaje. Pro šifrování citlivých dokumentů doporučuje NÚKIB následující symetrické blokové šifrovací algoritmy:

Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů

Twofish s využitím délky klíčů 128 až 256 bitů

Serpent s využitím délky klíčů 128, 192, 256 bitů

Camellia s využitím délky klíčů 128, 192 a 256 bitů

Vedle těchto algoritmů je také důležité určit doporučené režimy, ve kterých budou použity:

XTS (XEX-based tweaked-codebook mode with ciphertext stealing) – délka jednotky dat (sektoru) nesmí přesáhnout 220 bloků šifry.

[Sem zadejte text.]

EME (ECB–mask–ECB).

Pro úložiště, resp. informační systémy které umožňují přístup ke studijním dokumentům by měly existovat systém řízení přístupu k dokumentům. To zahrnuje definování oprávněných osob, které mají přístup k dokumentům, a nastavení vhodných úrovní oprávnění pro různé role. Důležité je také sledovat a zaznamenávat všechny přístupy k dokumentům za účelem auditu.

Nezbytnou součástí ochrany úložiště je také zajištění pravidelného zálohování dokumentů a testování obnovy dat, aby se zajistilo, že dokumenty mohou být obnoveny v případě havárie nebo ztráty. Pro nastavení parametrů služby lze jako vodítko použít data z šablony: „Analýza rizik spojená se studijními dokumenty" na listu „Metriky pro hodnocení PriA a PodA".

Pro dlouhodobé uchování dokumentů je důležité zvolit vhodný formát a médium pro jejich archivaci. Elektronické dokumenty by měly být uloženy ve standardních formátech, které jsou nezávislé na konkrétním softwaru a hardwaru. Archivní média, jako jsou pevné disky, pásky nebo cloudové úložiště, by měla být odolná proti selhání a zabezpečena proti neoprávněnému přístupu.

Dlouhodobé uchovávání v elektronické podobě může vyžadovat pravidelnou aktualizaci prostředků pro zajištění integrity a původu dokumentu (např. časová razítka). Je nutné zajistit, aby byl ten proces zajištěn a v ideálním případě automatizován.