

Popis procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů

Výstup č. 8

Popis výstupu č. 8 za Janáčkovu akademii múzických umění

Janáčkova akademie múzických umění

Obsah

Anotace výstupu	2
Studijní informační systém JAMU	2
Procesy pro uchování studijních dokumentů	3
<i>Identifikace a klasifikace sledovaných dokumentů.</i>	<i>3</i>
<i>Přístupová kontrola.....</i>	<i>4</i>
<i>Zajištění bezpečného přenosu.....</i>	<i>4</i>
<i>Dlouhodobé uchování a archivace, zálohování a obnova</i>	<i>6</i>
Analýza rizik v souvislosti se zpracováním studijních dokumentů	6

Anotace výstupu

V rámci výstupu č. 13 dílčí části projektu SC C2 NPO za Janáčkovu akademii múzických umění jsme se zabývali procesy bezpečného předávání a dlouhodobého uchovávání studijních materiálů z pohledu studijního informačního systému Janáčkovy akademie (využíváme systém Masarykovy univerzity), dle doporučení a definice procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů zpracovaných pracovní skupinou PS3 v rámci výstupu č. 13 společného projektu SC C2 NPO.

Studijní dokumenty lze 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“ a archivovány po nezbytně dlouhou dobu tak, aby vyhověly platné legislativě. Pojem studijní materiály může být v současné době poněkud matoucí, jelikož mimo klasické písemnosti zahrnuje také data, která jednotlivé události zaznamenávají ve studijních informačních systémech (SIS), obvykle ve formě databázových záznamů. Z těchto dat pak často vznikají dokumenty v listinné podobě pouze v reakci na konkrétní žádosti studentů (např. potvrzení o studiu, výpis studijních výsledků) 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).

V úvodu je pak ještě nutné zmínit, že v rámci provedeného ověření nebyly za studijní materiály v tomto výstupu považovány veškeré materiály, které slouží jako podpora vzdělávání (skripta, prezentace, záznamy přednášek, aj.), nebo materiály, které slouží pro potřeby akreditace (syllaby předmětů, struktura studijního programu/oboru).

Studijní informační systém

Studijním informačním systémem v prostředí Janáčkovy akademie múzických umění je Informační systému Masarykovy univerzity, také nazývaný jako „IS JAMU“¹. V rámci IS JAMU existuje sada agend s podobným principem a ovládáním – strom se složkami, do nichž lze vkládat materiály a nastavovat práva pro přístup:

1. Manipulace se studijními materiály

¹ <https://is.jamu.cz>

- Vystavení různých typů studijních materiálů učitelem (světu, uživatelům IS, studentům předmětu).
 - Otevírání odevzdávacích složek, kam student vkládá svoje elektronické práce pro hodnocení vyučujícím.
2. Archiv závěrečných prací
 - Vystavení bakalářské, diplomové, disertační práce studentem.
 - Prohlídka vystavených prací.
 3. Dokumentový server
 - Vystavení vyhlášek, směrnic, zápisů z jednání široké fakultní veřejnosti.
 - Zpřístupnění materiálů menší skupině osob (kolegium děkana, akademický senát, ...).
 4. Úschovna
 - Odložení si souboru pro následné vyzvednutí.
 - Krátkodobé vystavení souborů osobám ze školy nebo z internetu.
 - Možnost přijímat velké soubory, které e-mail odmítne.

Procesy pro uchování studijních dokumentů

Dle doporučení v rámci výstupu č. 13 společného projektu SC C2 NPO je pro nastavení procesů bezpečného předávání a dlouhodobého uchování studijních dokumentů nezbytné zvážit hned několik faktorů a provést nejméně následující činnosti:

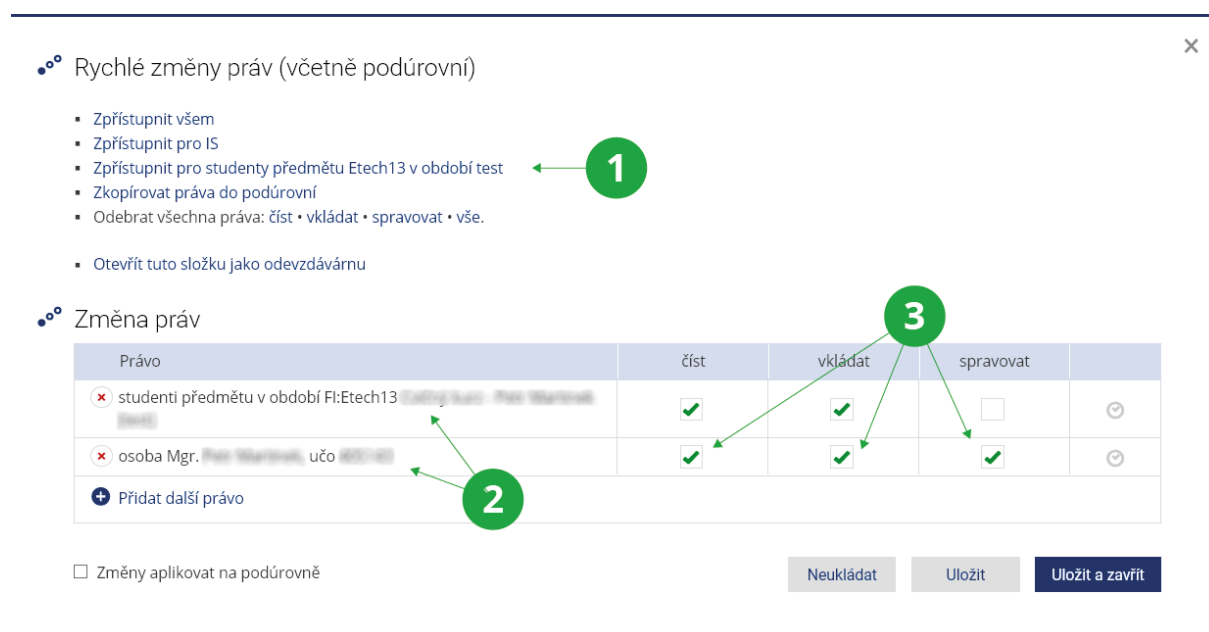
- Identifikace a klasifikace sledovaných dokumentů.
- Přístupová kontrola.
- Zajištění bezpečného přenosu.
- Dlouhodobé uchování a archivace, zálohování a obnova ze zálohy.

Identifikace a klasifikace sledovaných dokumentů.

V rámci provedené analýzy bylo ověřeno, že studijní informační systému IS JAMU podporuje z pohledu identifikace a klasifikace sledovaných dokumentů různé možnosti klasifikací dokumentů, včetně vlastních klasifikací specifikovaných uživateli a zajišťuje rovněž také i verzování studijních dokumentů. Z pohledu klasifikace na základě zákona č. 412/2005 Sb. o ochraně utajovaných informací, ale evidenci těchto dokumentů v souladu se Spisovým řádem studijní systém IS nezajišťuje.

Přístupová kontrola

Co se týče zajištění kontroly přístupu, v rámci IS existuje hned několik typů implicitních i explicitních práv, která jsou řešena mimo jiné i na úrovni skupin nebo práv přidělených uživatelům jednotlivě, viz *Obrázek 1*. Odebírání práv probíhá pak probíhá jak automaticky, tak ručně. Logování v rámci IS probíhá na několika úrovních – jeden ze způsobů je například transakční protokol spisové služby.



• Rychlé změny práv (včetně podúrovní) ×

- Zpřístupnit všem
- Zpřístupnit pro IS
- Zpřístupnit pro studenty předmětu Etech13 v období test ← 1
- Zkopírovat práva do podúrovní
- Odebrat všechna práva: číst • vkládat • spravovat • vše.
- Otevřít tuto složku jako odevzdávárnu

• Změna práv

Právo	číst	vkládat	spravovat	
studenti předmětu v období FI:Etech13	✓	✓	<input type="checkbox"/>	⊘
osoba Mgr. ... učo ...	✓	✓	✓	⊘
+ Přidat další právo ← 2				

Změny aplikovat na podúrovně

Neukládat Uložit Uložit a zavřít

Obrázek 1: Ukázka nastavení práv v IS

Zajištění bezpečného přenosu

Z pohledu bezpečného 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:

TLS v1.3:

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

TLS v1.2:

- 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 rámci ověření parametrů pro zabezpečené předání studijních dokumentů bylo využito nástroje pro testování nastavené úrovně zabezpečení informačních systémů a webových aplikací z pohledu zajištění šifrovaného přenosu dat od společnosti SSL Labs – *SSL Server Test*².



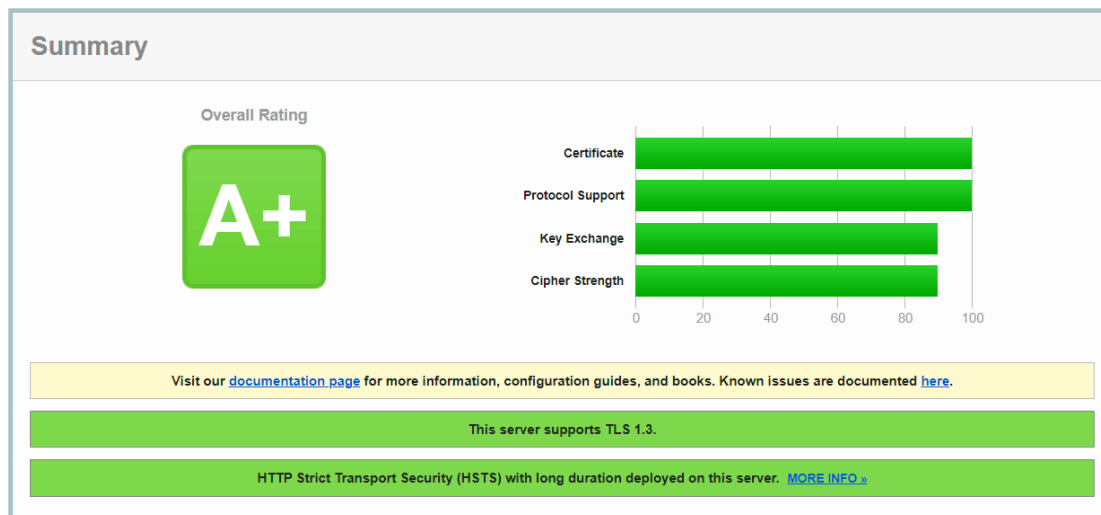
Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > is.jamu.cz

SSL Report: is.jamu.cz (147.251.49.82)

Assessed on: Fri, 19 Jul 2024 13:19:50 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



Obrázek 2: Test parametrů úrovně zabezpečení IS

V rámci provedených testů za pomoci nástroje *SSL Server Test* bylo zjištěno, že IS splňuje veškerá doporučení až na podporu již zastaralých protokolů TLS 1.0 a TLS 1.1, za což došlo ke snížení celkového

² <https://www.ssllabs.com/ssltest/>

hodnocení zabezpečení IS MU na hodnotu B. Kompletní report z tohoto testu je pak možné si zobrazit na adrese³.

Dlouhodobé uchování a archivace, zálohování a obnova

IS má v rámci svého prostředí řešení archivaci/skartaci studijních dokumentů. Skartace dokumentů, které podléhají evidenci v elektronickém systému spisové služby probíhají na základě vydaného spisového a skartačního plánu, případně na základě vydaného trvalého skartačního souhlasu. Problematika Data Loss Prevention je řešena hned na několika úrovních různými způsoby. Skartační značka se u konkrétních dokumentů neudržuje, nicméně je evidováno více údajů, mimo jiné také skartační lhůtu (dobu) a spisový znak. U spisů se pak eviduje mimo jiné spisová značka.

Analýza rizik v souvislosti se zpracováním studijních dokumentů

Dle výstupu č. 13 společného projektu SC C2 NPO je pro stanovení vhodných metod zabezpečení přenosu studijních dokumentů, úložiště studijních dokumentů a aktiv, která tyto 2 služby podporují, vhodné vycházet ze standardního přístupu založeném na hodnocení rizik. Tento přístup vychází z požadavků norem řady ISO/IEC 27000, Zákona č. 181/2014 Sb. o kybernetické bezpečnosti (ZoKB), Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VoKB) a doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Jelikož je Informační systém Masarykovy univerzity regulovaným informačním systémem z pohledu ZoKB, identifikovaným jako významným informačním systémem (VIS), je k tomuto systému zpracována bezpečnostní dokumentace a nastaven systém řízení bezpečnosti informací (dále je „SRBI“), jehož základem je právě výše uvedená analýza rizik, na základě které dochází v rámci kyberprostředí Janáčkovy akademie múzických umění k nastavování patřičných technických a procesních opatření. Jelikož se ale z pohledu bezpečnostní dokumentace k zavedenému SRBI jedná o interní dokumentaci organizace, může být tato dokumentace zpřístupněna pouze na vyžádání.

³ <https://www.ssllabs.com/ssltest/analyze.html?d=is.jamu.cz>