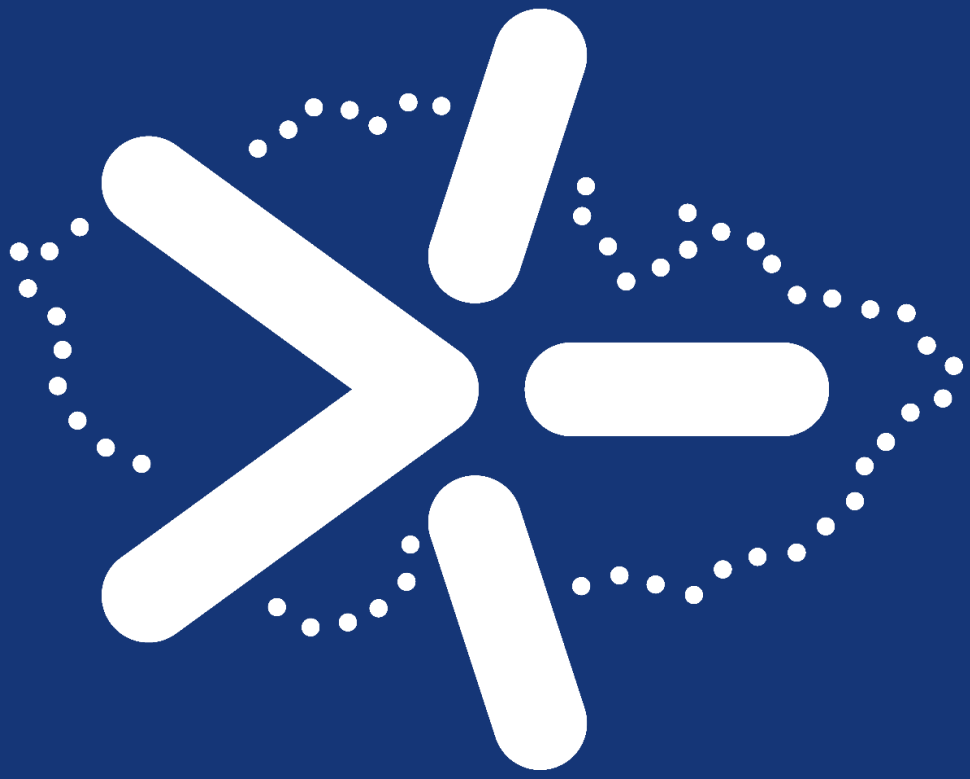


VÝSTUP Č. 5 ČZU

Pravidla pro zabezpečené přiřazení, přístup a evidenci relevantních studijní materiálů v závislosti na zvoleném předmětu.

Cíl: Definice požadavků a doporučení pro zabezpečené přiřazení, přístup a evidenci relevantních studijních materiálů v závislosti na zvoleném předmětu.

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

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

Obsah

1. Úvod

Výstup č. 5 ČZU slouží jako metodické doporučení v oblasti zabezpečení přístupu ke studijním materiálům. Na začátku dokumentu je definován pojem relevantní studijní materiál, jak je na takový dokument v rámci plnění cíle dále pohlíženo. Dále je pro základní pochopení problematiky vysvětleno, jak vůbec vznikají jednotlivé předměty, kdo je garantem dané entity a jaké činnosti jsou s tím spojeny.

V další kapitole jsou obecně definovány výukové systémy pro řízení výuky, včetně příkladů takových systémů. Jsou uvedeny možnosti a postupy zápisu studentů do předmětu, jak se studijním materiály v systémech evidují, jak lze zabezpečit validitu nahraného dokumentu, úrovně práv a tomu odpovídajících uživatelských rolí, tvorba kurzů mezi semestry, zabezpečení, logování a zálohování výukového systémů a také je zde pojednáno o dalších podpůrných systémech pro LMS.

Další část je věnována možnostem přístupu studentů k literatuře poskytované knihovnami. Pro celistvé pojetí problematiky je zde pojednáno ve zkratce jak o poskytování tištěných, tak především elektronických publikací. Jsou zde vyjmenovány možné způsoby online poskytování materiálů včetně jejich hodnocení.

V dokumentu je také uveden alternativní způsob přístupu ke studijním materiálům v případech potřeby přístupu studentům k interním prostředkům univerzity a jaké nutné komponenty jsou pro takovou možnost nutné. Dále je zde uveden příklad procesu poskytnutí takového přístupu, včetně procesu přihlášení. Na závěr kapitoly je uvedeno hodnocení takové alternativy.

Z důvodu potřeby přihlašování do interní sítě univerzity je v dokumentu také uveden způsob přístupu uživatele do síťového prostředí, jeho autentizace ve smyslu rozboru problematiky 802.1x.

Na závěr je rozebrána problematika logování a práce s informacemi včetně názorných příkladů.

2. Relevantní studijní materiál

Za pojem „relevantní studijní materiál“ lze z akademického hlediska a také pohledu MŠMT označit publikace vycházející ze sylabu jednotlivých předmětů, dále skripta, cvičebnice, ale i ostatní odbornou literaturu dostupnou fyzicky v knihovnách či online. Z širšího hlediska sem lze zařadit také přednáškové prezentace, prezentace na cvičeních, pracovní dokumenty, šablony a další materiály, se kterým v rámci svého studia přijde student do kontaktu. Dále je možné do tohoto širšího pohledu řadit i materiály z tzv. „šedé literatury“, což mohou být bakalářské práce, diplomové práce nebo také protokoly z měření a podobné. Sylaby a další doporučená literatura jsou dostupné ve výukovém systému v kurzu vytvořeném pro daný předmět.

[Sem zadejte text.]

Za skladbu sylabu předmětu je odpovědný garant, který by měl podobu a případné změny hlásit na knihovnu dané instituce. Snahou knihovny by pak měla být co nejširší nabídka této odborné literatury. Zároveň by vše mělo být pro potřeby distanční formy výuky dostupné také v elektronické podobě, například na stránkách knihovny, nebo jiných univerzitou podporovaných serverech. Za dostupnost sylabu a dalších výukových materiálů v kurzech daného předmětu je společně s garantem předmětu odpovědný také vyučující.

3. Hierarchie vzniku předmětů a přiřazení zodpovědnosti

Student VŠ je zařazen do studijního programu, který je akreditován Národním akreditačním úřadem, případně může mít vysoká škola tzv. institucionální akreditaci. Od roku 2019 již existují pouze studijní programy, nikoli studijní obory (novela zákona o vysokých školách).

Student plní určitý studijní plán, kde má do jisté míry možnost si jej přizpůsobit – ten se obvykle skládá z povinných kurzů, resp. předmětů (*A předměty*), určitého množství povinně volitelných kurzů/předmětů (*B předměty*) a také volitelných kurzů/předmětů (*C předměty*), přičemž povinný objem práce, kterou musí student vynaložit, se obvykle měří kredity.

Entita	Garant, zřizovatel či arbitr	Záběr, rámec	Činnost
Akreditace VŠ (studijního programu)	Akreditační komise MŠMT ČR	VŠ, Studijní programy	Institucionální akreditace VŠ, akreditace stud. programů
Oblasti vzdělávání	Nařízení vlády č. 275/2016 Sb.	Oblasti vzdělávání - např. Ekonomické obory, Informatika, Zemědělství, Biologie, ekologie a životní prostředí	Definuje vymezený úsek vysokoškolského vzdělávání, v jehož rámci jsou připravovány, schvalovány a uskutečňovány vysokoškolské studijní programy
Studijní program	Vytváří ho garant stud. programu ve spolupráci s děkanem fakulty. Schvaluje akreditační komise MŠMT nebo RVH	Obor vzdělávání	Je uceleným plánem vzdělávání v konkrétním oboru na konkrétní VŠ. Program je souhrn předmětů, které musí student splnit.

[Sem zadejte text.]

Předmět	Garant předmětu (katedra). Vedoucí katedry definuje nového garanta v případě změny	Odborné předměty specifické podle zaměření katedry	Výuka konkrétních odborných předmětů, poskytnutí studijních
Sylabus předmětu	Garant předmětu – kontrola literatury podle směrnic akreditační komise	Konkrétní předmět	Učební osnova nebo studijní plán. Popisuje cíle, obsah a **doporučenou či povinnou studijní literaturu (studijní materiály)**
Studijní materiály	Garant předmětu, vyučující	Materiály poskytované katedrou v souladu se sylabem předmětu	Garant předmětu zajišťuje sylabus předmětu (tj. co a jak se bude vyučovat). Vyučující poté zprostředkovává vhodným způsobem materiály studentům (přednášky, sdílení materiálů v IS..)

Zdroj: https://www.msmt.cz/vzdelavani/vysoke-skolstvi

4. Výukové systémy pro řízení výuky (LMS)

Název vychází z anglického „Learning Management System“, kdy se především jedná o softwarové aplikace či webové technologie, které se používají k plánování a celkové administraci systému online výuky. LMS se zaměřují na distribuci a administraci vzdělávacích elektronické materiálů, dále také může sloužit k prověřování znalostí formou testů apod. Jako příklad LMS lze uvézt Moodle, Blackboard, Unifor, TalentLMS, atd.

V dokumentu bude pojednáno především o LMS Moodle (Modular Object–Oriented Dynamic Learning Environment), který byl prostřednictvím dotazníkového šetření shledán jako nejvíce využívaným výukovým systémem.

5. Přiřazení studenta do předmětu

Studenti jsou do konkrétních předmětů / kurzů zařazeni automaticky, pokud to systém umožňuje, případně se k zápisu využívají takzvané klíče. Studentovi je na první přednášce či cvičení představen kód předmětu / kurzu a následně klíč. Po jeho vyplnění se pak student zapíše do daného kurzu a má tak tím k dispozici připravené studijní materiály k danému předmětu. Klíč k zápisu vůbec nemusí být pro kurz nastaven, pak se do kurzu může přihlásit jakýkoliv uživatel (typicky student), který má přístup do výukového systému. Kurzy odpovídají např. jednotlivým cvičením či přednáškám

z předmětů, studijním či projektovým skupinám apod. Tyto skupiny mohou být tvořeny přímo garanty předmětu, případně vyučujícími, dle předem definovaných rolí. Ti pak také dále editují obsah kurzu, tedy včetně studijních materiálů a informací určených pro studenty.

6. Evidence studijních materiálů z výukového systému

V návaznosti na druhou kapitolu dokumentu, relevantní studijní materiály by měly vycházet ze sylabu předmětu a materiálů dostupných ve výukových systémech např. LMS Moodle. Pro možné fungování výukového systému je třeba napojení na další univerzitní systémy. Pro ověřování uživatelského přihlášení a dalších informací o studentovi jako kontaktní email, identifikační číslo studenta, obor studia atd., je nutné propojení na např. Active Directory nebo tomu obdobné autentizační databáze. Další nezbytností je propojení na univerzitní informační systém, odkud lze získat:

- přehled předmětů, ke kterým lze v daném akademickém roce vytvořit kurz
- přehled předmětů, které má student v daném akademickém roce studovat
- přehled předmětů garantovaných garantem oboru/programu v rámci akreditačního řízení
- pokud je systém využíván také k plnění zkouškových testů, tak je nutný přehled studentů přihlášených na termín zkoušky v SIS
- přehled všech aktivních studentů a osob v SIS.

7. Zabezpečení nahrávání validních souborů do výukového systému

Veškeré dokumenty nahrávané do výukových systémů a jejich úpravy by měly procházet procesem kontroly ze strany garanta předmětu, případně jím pověřených osob, aby nedocházelo k neautorizovaným změnám a byla tak chráněna integrita a validita dokumentu. K naplnění předchozího lze doporučit využití dvou-faktorového ověření uživatele pro režim úpravy, kdy každá tato úprava projde procesem kontroly odpovědných osob a zanechá také auditní stopu / záznam.
Z hlediska integrity lze doporučit využití možnosti elektronického podpisu a časového razítka u uveřejňovaných dokumentů.

8. Uživatelské role ve výukovém systému

V rámci výukového systému je nutné si definovat role a tomu odpovídající práva a odpovědnosti, který uživatel a jak může pracovat s různými daty v systému. Níže je uveden výčet takových rolí v systému LMS Moodle:

- **Správce** – může tvořit a mazat kurzy, může vstupovat do všech kurzů a editovat je

- **Vedoucí** – je uživatel např. ve funkci proděkan, vedoucí katedry apod., který může nahlížet do kurzů své přidělené kategorie (katedra, fakulta)
- **GAELP** – má práva na tvorbu, editaci i odstranění kurzů ve své kategorii kurzů (fakulta, katedra)
- **Garant** – má stejná práva jako vyučující, ale navíc může resetovat kurz a přidělovat role v rámci kurzu, nemůže ale kurzy vytvářet
- **Pedagog** – má práva na editaci kurzů, kde je přiřazen jako vyučující
- **Asistent** – neboli vyučující bez práva upravovat, může známkovat studenty, ale nemá právo přidávat nebo editovat studijní materiály a činnosti v kurzu
- **Student** – má právo na zobrazování materiálů a využívání činností (test, úkol, fórum, …) v kurzech, kde má přiřazenou roli student
- **Host** – má minimální práva, obvykle vstupovat pouze do kurzů, které jsou jim otevřené, host se ale nemůže účastnit zpětné vazby v kurzu (tesy, úkoly, fóra, …), protože nemá v kurzu jednoznačnou identitu
- **Garant oboru/programu** – má přístup a právo náhledu na obsah předmětů oboru/programu, který garant garantuje v rámci akreditace

9. Tvorba kurzů ve výukovém systému mezi semestry

Tvorbu kurzů do nového semestru / akademického roku provádí ve výukovém systému LMS Moodle z pravidla uživatel v roli GAELP (Garant Elektronické Podpory) katedry (či jiného dílčího pracoviště). Zpravidla ponechává staré kurzy a prostřednictvím modulu SemesTraK (Semestrální Transformace Kurzů) tvoří jejich prázdnou kopii do nového semestru. Výhodou tvorby kopie kurzu je, že ve starém kurzu zůstávají data studentů (výsledky testů, odevzdané a opravené odevzdané práce apod.) a nový kurz se převede jako čistý, tedy bez uživatelů a jejich dat. Následně se do něj zapíší pouze aktuální studenti.

10. Zabezpečení přístupu do výukového systému včetně síťové komunikace

Standardní síťová komunikace mezi uživatelem a serverem výukového systému probíhá prostřednictvím internetového připojení. Uživatel může komunikovat se serverem pomocí webového rozhraní, které je poskytováno prostřednictvím webového prohlížeče. K tomu uživatel zadává adresu serveru výukového systému do svého prohlížeče a po zadání správných přihlašovacích údajů může začít používat e-learningový systém.

Zabezpečení síťové komunikace mezi uživatelem a serverem výukového systému (software) by mělo být zajištěno pomocí protokolu HTTPS, který používá šifrování TLS 1.2 a vyšší (Transport Layer

Security). Server by tedy měl mít platný TLS certifikát. Zároveň by mělo být vynucováno použití HTTPS namísto HTTP, čehož lze docílit za použití přesměrování. Při použití protokolu HTTPS jsou data přenášena mezi uživatelem a serverem šifrována, což zajišťuje, že nikdo jiný než uživatel a server nemohou číst nebo upravovat data během samotného přenosu. Přístup k serveru výukového systému by měl být nakonfigurováno tak, aby byl omezen přístup k citlivým datům pouze na oprávněné uživatele. Toho lze dosáhnout pomocí rozdělení rolí a nastavení oprávnění pro každou z rolí. Servery výukového systému by měly být také pravidelně zálohovány a zálohy testovány pro případné obnovení.

Dále je vhodné využít silná hesla a dvoufaktorovou autentizaci pro přihlašování do e-learningového systému, aby se minimalizovala rizika útoků na účty uživatelů. Další možností je využití proxy serveru, na kterém by probíhalo multifaktorové ověřování uživatelů a po přihlášení přesměrování do interních systémů. Uživatel by měl mít silné heslo a měl by být povinen ho pravidelně měnit. Server výukového systému by měl také implementovat mechanismy pro ochranu hesel, jako je hashování a kryptografické „solení". Uživatelé by měli mít také aktuální antivirový nástroj na svých počítačích, aby zabezpečili své zařízení před možnými hrozbami z internetu. V neposlední řadě je důležité pravidelně aktualizovat server výukového systému a jeho pluginy na nejnovější verze, které obsahují opravy chyb a bezpečnostní aktualizace.

11. Podpůrné výukové systémy v distanční výuce

Kromě primárního e-learningového systému Moodle se s příchodem onemocnění Covid-19 začaly v rámci výuky využívat kolaborativní platformy jako MS Teams, Zoom, Google Meet, Skype, atd. Tyto sloužily především k online výuce a sdílení studijních / pracovních materiálů formou videokonferencí pedagoga a studentů.

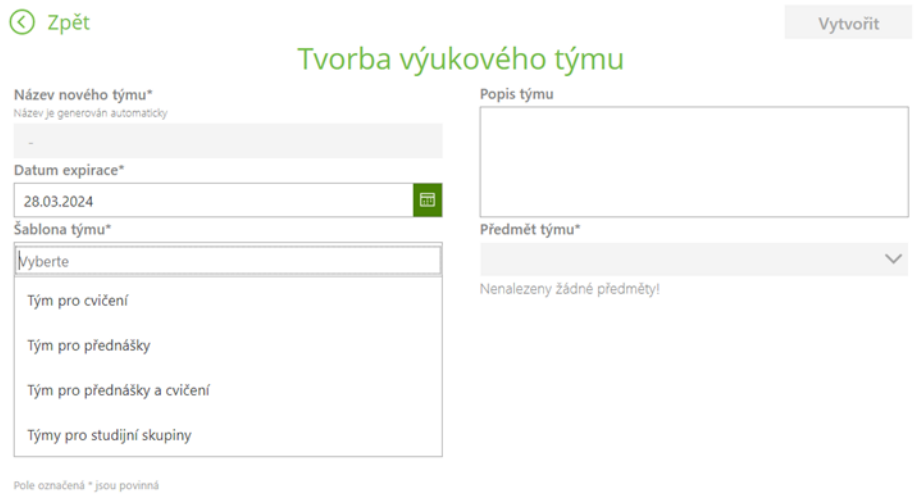
Z důvodu usnadnění a zefektivnění práce jak pedagogů a integrátorů při vytváření týmů je vhodné zřídit formuláře, které pedagog vyplní se všemi potřebnými náležitostmi vždy před začátkem semestru, ve kterém je daný předmět vyučován. Příkladem může být níže uvedený formulář z prostředí České zemědělské univerzity, kdy je v rámci univerzitou využívaných M365 nástrojů vytvořena interní aplikace M365 manager pro vytváření studentských týmů pro výuku. V ní si mohou vyučující/garanti předmětu sami vytvářet studentské týmy v MS Teams na základě vlastních požadavků. Tým je primárně určený pro výuku na základě kódu předmětu, zapsaného v aktuálním rozvrhu. Role v týmu jsou rozděleny na vyučujícího (teacher) a studenta (student) na základě existence skupin v Azure Active Directory. V rámci těchto týmů je k dispozici automatické naplnění a synchronizace týmů studentů a pedagogů, kteří daný předmět vyučují.

Pro vytvoření nového studentského týmu vyučujícím se používají následující informace:

[Sem zadejte text.]

I. Název nového týmu - vygeneruje se automaticky na základě výběru šablony týmu a předmětu týmu.
II. Datum expirace - každý tým má omezenou platnost – je nutné vybrat datum, do kterého má být tým přístupný.
III. Šablona týmu - volba předdefinovaných šablon týmů:
    - Tým pro cvičení
    - Tým pro přednášky
    - Tým pro přednášky a cvičení
    - Týmy pro studijní skupiny
IV. Popis týmu – popis, k čemu a pro koho bude tým sloužit.
V. Předmět týmu – výběr, co bude předmětem týmu. Lze vybrat více možností.

Po vyplnění všech parametrů dojde k vytvoření studentského týmu v MS Teams a vytvoření skupiny v AAD.



Obrázek č. 1 M365 manager (Intranet ČZU)

U vytvořeného výukového týmu je přidána knihovna „Výukové materiály“, kterou může editovat (přidávat materiály) pouze vlastník týmu (pedagog). Ve výchozím nastavení mají studenti v týmu možnost zobrazení/stažení přidaných materiálů. Každý pedagog ale může požádat o změnu oprávnění studentů k přístupu k materiálům, např., aby student mohl materiály pouze číst.

Z hlediska množství vytvářených týmů a tomu odpovídající velikosti dat je také důležitá archivace. Ta může probíhat buď na konci, případně na začátku dalšího akademického roku na omezenou dobu, dle interně nastavených pravidel a politik.

[Sem zadejte text.]

12. Zálohování a logování LMS

Zálohování e-learningového systému probíhá na vybraném příkladě univerzity následujícím způsobem (LMS Moodle):

- na úrovni databáze – každý den se vytváří dump databáze, který se kopíruje na zálohovací server, kde se drží 30 dní. Poté se nejstarší záznamy odmazávají.
- na úrovni Hypervisoru (vSphere) - vytváří se záloha celého serveru, která se drží po dobu 30 dní nazpět. Poté se drží jedna záloha z měsíce až po dobu půl roku zpětně.
- v rámci upgrade systému – při každém upgradu e-learningového systému (cca každé 2-4 roky) se uloží verze před updatem a archivuje se s retencí 10 let.
- krátkodobá záloha (kopie provozního prostředí) - jednou týdně se provádí kopie provozního systému na separátní backup server, který slouží pro testování nových funkcí a update.

Logy z webového serveru (Apache + Nginx) se drží 21 dní, poté se nejstarší odmazávají. Zároveň jsou logy posílány na do centrálního nástroje pro sběr logů LOGmanager.

Všechny výše uvedené časové údaje odráží nastavenou politiku vybrané instituce, není zde obecný předpis, který by jednotlivé doby upravoval.

13. Odborná literatura poskytovaná knihovnami a přidruženými systémy

Je-li student úspěšně přijat ke studiu určitého studijního programu, a podstoupí-li proces zápisu do předmětů studijního programu, měl by mít i přístup k doporučené a povinné literatuře definované v sylabu předmětu. Tato literatura je v současnosti obvykle ve formě tištěných publikací či skript, které podléhají autorskému zákonu (předpis 121/2000 Sb. a Listina základních lidských práv a svobod). Student si literaturu buď musí zakoupit nebo má možnost zapůjčení v knihovnách. Knihovna může poskytovat rozmnoženiny děl, je-li zaplacena odměna, která přísluší autorům. Právo autora udělit oprávnění dílo užít (vytvořit kopii) trvá po dobu autorova života a 70 let po jeho smrti. V případě elektronické formy musí knihovna nějakým způsobem zajistit, aby publikace nemohla být snadno zcizena a dále kopírována. Je třeba na elektronické formy publikace uplatnit ochranu DRM (Digital Rights Management), která jednak zajistí omezení kopírování, tisku nebo období použitelnosti, a také umožní neoddělitelnou identifikaci majitele či zařízení, ke kterému se publikace váže.

14. Tištěné publikace

Rezervace publikací je možná v knihovním systému. Studenti mají obvykle následující možnosti přístupu k tištěné literatuře:

- Absenční výpůjčka – publikace, které lze zapůjčit mimo prostory knihovny. Ověření výpůjčky studentskou kartou. Obvyklá doba výpůjčky 1 měsíc s možností prodloužení.
- Prezenční výpůjčka – publikace, které lze zapůjčit pouze do prostor studovny nebo prostor čítárny knihovny. Ověření výpůjčky studentskou kartou.
- Speciální výpůjčka – vypůjčení za speciálních podmínek, např. technické normy.

15. Elektronické publikace

V souvislosti s vynucenou online výukou vznikla též potřeba zpřístupnit studentům literaturu vzdáleně. Z výše uvedených legislativních omezení vyplývá, že nelze jednoduše předat publikaci v elektronické podobě např. v systému LMS Moodle nebo Teams. Dochází proti chůdným požadavkům – poskytnout literaturu ve snadno dostupné elektronické formě, ale musí být zamezeno nakládání s literaturou neoprávněným způsobem. Tyto protichůdné požadavky byly v mnoha případech příčinou, že univerzitní knihovna neposkytovala literaturu v době vynucené online výuky (lockdown COVID) jinak než fyzicky. Výjimkou jsou např. externí informační zdroje (tzv. e-zdroje) dostupné např. prostřednictvím federace eduID. Jednotliví poskytovatelé služeb mají soulad s autorskými právy ošetřeny – například přístup k odborným časopisům a elektronickým publikacím (Cambridge Core, OEDC library…).

Garanti předmětů obvykle řešili situaci poskytnutím materiálů, které vznikly na základě uvedených publikací, nicméně studenti byli v tomto ohledu určitým způsobem omezeni. Neměli reálně přístup k doporučené a povinné literatuře z důvodu omezení pohybu osob a také otevírací doba knihovny byla omezena.

Univerzity byly postaveny před poměrně složitý úkol, jak tištěnou literaturu studentům v této době poskytnout. Neexistovala žádná legislativní výjimka z autorských práv pro tuto situaci, tudíž univerzitní knihovny musely použít některé již osvědčené a používané řešení. Například systém elektronických výpůjček veřejných knihoven, systémy zajišťující DRM nebo online čtečky na webu s limitovanou dobou přístupu. V některých případech může jít o provozní rozhodnutí které je třeba prověřit z právního hlediska – např. zda může univerzitní knihovna poskytovat souběžné časově omezené čtení určitého počtu publikací ve webové čtečce, pokud má tento počet k dispozici v knihovně ve fyzické formě. Legislativa v tomto ohledu není pevně definována, a je třeba vždy ji konzultovat individuálně.

[Sem zadejte text.]

16. Možné způsoby poskytování online materiálů studentům

a. Webový časově omezený přístup (např. e-prezencka)
   - Výhody:
     - Funkční v různých prohlížečích, na velké škále zařízení
     - Není třeba instalovat žádnou aplikaci
     - Snadná kontrola přístupnosti, jednoduchá implementace časového zámku
     - Auditovatelnost způsobu použití a přístupů
     - Snadná autorizace čtenáře
     - Relativně levná a snadná implementace
   - Nevýhody:
     - Nutnost online připojení
     - Obtížné zamezení některých operací – např. tisk či snímky obrazovky

b. Specializovaná aplikace pro čtení na mobilním zařízení či čtečce (např. Palmknihy, eReading)
   - Výhody:
     - Možnost offline čtení
     - Snadná kontrola přístupnosti, jednoduchá implementace časového zámku
     - Auditovatelnost způsobu použití a přístupů
     - Snadná autorizace čtenáře
     - Relativně snadná implementace, možnost koupit již hotové řešení
   - Nevýhody:
     - Nutná instalace aplikace na zařízení, podpora jen novějších operačních systémů mobilních zařízení (primárně iOS a Android)
     - Nákladnější pořízení z důvodu tvorby specializované aplikace

c. Formáty mobi, ePub, pdf s integrovanou DRM ochranou
   - Výhody:
     - Možnost offline čtení
     - Velká škála aplikací pro čtení, jen některé ale podporují DRM
   - Nevýhody:
     - Obtížná kontrola přístupnosti, implementace časového zámku
     - Obtížný audit způsobu použití a přístupů
     - Obtížná autorizace čtenáře

[Sem zadejte text.]

Může jít i o kombinace výše uvedených způsobů, např. systém bookport podporuje webový přístup a aplikaci pro čtečky. Distribuce dokumentů ve formátech mobi, ePub či pdf již není tak častá, neboť neumožňuje plnou kontrolu nad tím, co se s dokumentem děje.

17. Shrnutí

Do budoucna je třeba počítat u knihoven s přechodem od tištěné literatury k elektronickým formám. Z licenčních a autorských důvodů bude zřejmě nutné nadále poskytovat i tištěné dokumenty. Webový přístup s časovým omezením se jeví jako optimální způsob poskytnutí studijních materiálů elektronickým způsobem. V kombinaci s aplikací pro mobilní zařízení jde o systém pro studenta snadno použitelný a ověřený v provozu veřejných knihoven.

18. Alternativní způsob přístupu ke studijním materiálům – VPN

Pokud student ke svému studiu potřebuje prostředky univerzity, které jsou dostupné výhradně v interních sítích, vzniká problém, jak tyto zdroje zpřístupnit během lockdownu. Z hlediska licencí a bezpečnosti univerzita nechce a ani nemůže dané prostředky poskytovat veřejně z internetu, například pokud je jejich autentizace vázána na autentizaci do Active Directory domény. Dalším příkladem takových prostředků může být použití specializovaných statistických nebo grafických software s licencí na počet připojení instalovaných pouze v učebnách, přístup na On Premise souborová úložiště protokolem Samba, nebo též literatura z univerzitní knihovny přístupná pouze ze sítí univerzity. Tato literatura je licenčně vázána na poskytnutí přístupu v prostorách univerzity, tj. pouze na jejích vnitřních sítích.

Jedním z možných řešení takového požadavku je použití připojení Virtual Private Network (VPN), které zprostředkuje uživateli vybrané vnitřní sítě univerzity. Uživatel se poté může vzdálenou plochou připojovat na „svůj" fyzický nebo virtualizovaný počítač na univerzitě, ze kterého již má přístup k potřebným zdrojům a pracuje jako kdyby „byl na svém PC". Toto je obvyklá situace u zaměstnanců, studenti mohou mít v rámci určitého vyučovaného předmětu možnost připojení v definované časy na desktopy na učebnách. Tato myšlenka vznikla v době COVID lockdownu, kdy bylo nutné vyučovat určité předměty prezenčně v učebnách, ale studenti měli zakázaný přístup na univerzitu.

Z důvodu bezpečnosti je požadována u VPN připojení povinně více faktorová autentizace, například heslo doplněné o token zaslaný na mobilní zařízení prostřednictvím SMS. Tím je dostatečně zajištěno jednoznačné ověření identity (autentizace) uživatele oprávněného VPN používat. Pouhá autentizace uživatelským jménem a heslem není dostatečně kvalitní pro takto citlivou službu.

Problém v případě požadavku na mobilní telefonní číslo nastává v souvislosti se zpracováním tohoto osobního údaje. Aby bylo možné využívat studentovo soukromé číslo, musí ke konkrétním

úkonu zpracování existovat jasně definovaný účel. Univerzity doposud převážně zpracovávaly telefonní číslo studenta pouze v průběhu přijímacího řízení na základě oprávněného zájmu kvůli možnosti kontaktování uchazeče. S požadavkem na vzdálený přístup do univerzitní sítě a k univerzitním aktivům v době pandemie vznikl nový rozpor mezi potřebou zabezpečené výměny informací/ochranou univerzitních aktiv a problematikou ochrany osobních údajů. Ten souvisí především s tím, že řada technik vicefaktorové autentizace využívá dosud jako jediný druhý faktor telefonní číslo. V takovém případě je nutné myslet na fakt, že vzniká nové zpracování osobních údajů a brát v potaz všechny povinnosti univerzity s tím související. Pokud by se zpracování mobilních čísel týkalo všech studentů dané univerzity, lze doporučit založit zpracování na základě oprávněného zájmu univerzity. Pokud by se jednalo pouze o vybranou skupinu studentů, kteří potřebují vstupovat na zařízení univerzity za využití VPN přístupu, je možné zpracování podmínit souhlasem dotyčných studentů se všemi potřebnými náležitostmi s tím související. Tento souhlas je vhodné z hlediska požadavků na zpracování a možnosti logování této operace vhodné realizovat ve studijním informačním systému pomocí modulu, který umožní studentovi manuálně vložit telefonní číslo pro konkrétní účel zpracování (např. MFA/VPN). V praxi se často využívá tištěný formulář a vyplněné telefonní číslo, nicméně to není vhodná a doporučovaná varianta.

19. Komponenty nutné pro vybudování VPN systému

a. VPN server (např. Forti Authenticator).
   - Zprostředkovává autentizaci uživatele VPN, nutně vícefaktorově (např. vůči Active Directory).
   - Zprostředkovává vlastní VPN připojení uživatele
   - Umožňuje TLS konfiguraci, která zabezpečuje šifrování připojení.
   - Poskytuje logování a monitoring přístupů.

b. Síťový firewall
   - Uplatňuje nastavení povolených přístupů do sítí univerzity.
   - V případě VPN připojení definuje přístupová pravidla definovaným skupinám uživatelů (např. pravidla asociovaní na skupiny Active Directory).

c. VPN klient pro desktopy (např. Forti Client).
   - Umožňuje samotné připojení desktopu k VPN serveru.
   - Autentizuje uživatele, nutně vícefaktorově.
   - Odpojuje uživatele po uplynutí definované maximální doby připojení.
   - Upravuje síťové nastavení desktopu, aby bylo možné připojení do sítí univerzity (přidává síťové cesty do prostředí desktopu – routes).
   - Může provádět základní bezpečnostní kontrolu, aby nedošlo k zavlečení škodlivého softwaru do sítí univerzity. (např. kontrola typu OS na PC)

[Sem zadejte text.]

d. Autentizační adresář nebo databáze (např. ActiveDirectory)
   - Obsahuje účty uživatelů, jejich atributy (informace o účtech)
   - Umožňuje autentizaci uživatelů na základě jména a hesla.
   - Obsahuje skupiny, které mají povolené VPN připojení a k nim definovaná síťová pravidla. Uživatelé jsou přidáni do patřičných skupin, pokud mají mít přístup VPN k definovaným zdrojům. Tyto skupiny mohou být definované např. na úrovni fakult.
   - Poskytuje VPN serveru další atributy pro více faktorovou autentizaci (mobilní tel. číslo)
   - Poskytuje logování a monitoring přístupů.

e. Systém aktivování VPN přístupu u studentů
   - Aktivace znamená např. zařazení uživatelského účtu do skupiny, která povoluje VPN připojení a zároveň definuje přístup VPN k určitým zdrojům. Může být realizováno správcem skupiny, příp. vazbou na identity management a zařazování na základě zápisu do předmětu, vč. schvalovacího procesu.
   - Portál pro správu atributů uživatelských účtů
     - Umožňuje autentizovanému uživateli nastavení a změnu atributů účtu (informace vedené u účtu. Například přidání mobilního telefonního čísla jako dalšího faktoru pro více faktorovou autentizaci VPN.
     - Portál by sám měl mít dostatečně bezpečné a důvěryhodné ověření a neměl by být dostupný z internetu. Pokud někdo zcizí heslo uživatele a portál umožní přístup jen heslem, je tím degradována bezpečnost více faktorového přihlášení.

f. Cílové desktopy pro vzdálené připojení
   - Jedná se o spravované desktopy v síti univerzity (obvykle Windows), ke kterým se uživatelé připojují vzdálenou plochou přes VPN připojení.
   - Mohou to být i virtuální desktopy (RDS, VDI…)
   - Poskytují prostředí pro práci uživatele jako kdyby pracoval přímo v síti– přístupy jsou stejné.

20. Příklad procesu poskytnutí přístupu VPN studentovi

- Pedagog (vyučující předmětu) zjistí ze studijního systému, pro který předmět bude potřebovat VPN připojení pro určité studenty a na které fakultě. Podá žádost o aktivaci VPN pro studenty, příp. může být aktivace součástí studijního systému. Požaduje tímto VPN přístup na desktopy umístěné v učebnách konkrétní fakulty.
- Studentské účty jsou zařazeny do patřičné Active Directory skupiny, která povoluje použití VPN a zároveň nastavuje síťová pravidla přístupu k desktopům v učebnách konkrétní fakulty.

[Sem zadejte text.]

- K aktivaci musí student dodat mobilní tel. číslo jako další faktor autentizace. To je možné realizovat zapsáním atributu do Active Directory administrátorem. Ale z hlediska zpracování osobních údajů je nutné, aby měl student nad tímto údajem kontrolu a souhlasil s jeho použitím k odesílání autentizačních tokenů. Je tedy vhodnější použít již existující rozhraní pro správu atributů uživatele, a odtud tento atribut synchronizovat do autentizační databáze, např. Active Directory.

21. Proces přihlášení k VPN a k desktopu na učebně

- Student dostane instrukce od vyučujícího s návodem, jak postupovat s připojením VPN a ke kterému desktopu na učebnách fakulty se bude připojovat (DNS název nebo IP adresa desktopu).
- Student si nainstaluje VPN klienta na svůj osobní desktop.
- Po instalaci a spuštění nakonfiguruje VPN server, ke kterému se bude připojovat (příp. může být instalace upravena tak, že je server před-konfigurován).
- Student se přihlásí svým přiděleným uživatelským účtem a heslem VPN.
- VPN server se pokusí autentizovat uvedeným uživatelským účtem do Active Directory, a pokud uspěje, pošle studentovi na mobilní číslo registrované u účtu SMS token (např. 6-ti místné náhodné číslo).
- VPN klient vyzve studenta k zadání SMS tokenu.
- Číslo zadané studentem je porovnáno se SMS tokenem, který VPN server odesílal. Pokud souhlasí, pokračuje autentizace VPN. Pokud ne, je ukončena.
- VPN klient nastaví prostředí na desktopu studenta tak, aby měl dostupné sítě učeben definované u VPN skupiny.
- Student spustí standardní program pro připojení ke vzdálené ploše RDP protokolem (mstsc) a přihlásí se svým ActiveDirectory účtem k desktopu na učebně, který mu přidělil vyučující. Po přihlášení pracuje na desktopu vzdáleně.

22. Zhodnocení alternativního řešení pomocí VPN

- Plusy:
  - Vysoká bezpečnost připojení, šifrovaný kanál, jednoznačná identifikace díky dvou faktorové autentizace. Možnost monitoringu přístupů a upozornění při anomáliích. Vynucení bezpečnosti desktopu, který používá student pro práci.
  - Využití vyzkoušené a používané infrastruktury VPN pro zaměstnance.

[Sem zadejte text.]

- Možnost definice různých oprávnění do sítě z jednoho bodu, možnost vazby na identity management.
- Nezávislost na distribuci licencí, licence zůstávají interně, jen se přidává skupina uživatelů, kteří je využívají.
- Možnost používat jakékoli zdroje bez ohledu na typ (licence, mapované disky, informační zdroje v rámci vnitřních sítí atd..).

- Mínusy:
  - Nutná instalace klientské části SW na osobní desktop studenta.
  - Minimální kontrola stavu zabezpečení osobního desktopu studenta, možnost zavlečení malware při nevhodné konfiguraci (z tohoto důvodu raději nepovolovat některé protokoly, např. Samba sdílení přes VPN kanál. Ideálně povolit jen RDP protokol).
  - Nutnost zpracovávat osobní údaj mobilní tel. číslo pro dvou faktorovou autentizaci. Je třeba zabezpečeným způsobem umožnit zadání, editaci a smazání mobilního tel. čísla pro připojení VPN. Vhodné je toto číslo vést ve zvláštním atributu, který není veřejně publikován (tj. není vhodné používat standardní atribut Active Directory „mobile“).
  - Potřeba většího počtu licencí pro VPN připojení, možné vyšší náklady na licencování.

Použití kombinace VPN přístupu a vzdálené plochy pro zajištění online výuky v učebnách při lockdownu bylo tím nejrychlejším a nejdostupnějším řešením, které mohlo být studentům poskytnuto takřka ihned. Nemusí se jevit jako optimální v době poskytování virtuálních desktopů, nicméně uspokojivě řeší bezpečnost i přes nutnost instalovat software na osobních desktopech studentů a bylo pro daný účel použitelné. Problematická část je správa 2. faktoru pro autentizaci, jelikož může být nutné zpracovávat další osobní údaj (mobilní tel. číslo) a je třeba tomuto požadavku systém přizpůsobit.

23. Zásady licencování specifických SW

Z pohledu licencování je běžným modelem pro instituci využití centrálního nákupu software, který je v rámci organizace konzumován. Z pohledu licenční politiky a licenčního manažera je na univerzitním kampusu pořizován typ licence:

- Multilicence určené k instalaci na licenční server, který zajišťuje verifikaci a autorizaci konkrétnímu stroji k udělení pro provoz na koncovém zařízení.
- Multilicence bez omezení na konkrétní počet strojů. Počty strojů jsou v pravidelném cyklu auditovány a následně je proveden jednorázový nákup na konkrétní časové období.
- Licence na konkrétní obvykle malý počet strojů pro specifický typ výuky instalované na konkrétní koncové zařízení bez možnosti licence instalovat jinde.

[Sem zadejte text.]

- Licence na libovolný počet strojů pro specifický typ výuky s možností využívat software pouze v jeden okamžik na zakoupený počet strojů – tzv plovoucí licence.
- Licence instalované na centrálním výkonném serveru s provozem software jako komunikace klient-server (typicky licence na databáze s omezením na výkon konkrétního stroje v datacentru).
    - Licence je blokována na konkrétní procesor CPU
    - Licence je blokována na konkrétní patici pro procesor (socket)
    - Licence je vázána na konkrétní stroj PC/server jako serverový OS

Z pohledu studijních materiálů je jako absolutní základ přístup ke zdrojům lokálně na fakultách a učebnách univerzity pomocí PC v učebně. Za účelem výuky jsou instalovány specifická programová vybavení na stroje v konkrétním místě nebo na stroje, které jsou pro tuto výuku upraveny svým výkonem nebo vybavením. V situaci, kdy je provoz univerzity v omezeném režimu, jako je například výjimečná situace státu, je nutné, aby student měl zajištěn přístup ke zdrojům i z jiného místa, než je lokálně. Za tímto účelem je využíváno:

- Otevřená multilicence pro studenta – typicky za minimální náklady nebo po doložení studentského statutu (ISIC karta) lze SW provozovat.
- Vzdálený přístup pomocí VPN – typické pro drahé software které nejsou možné provozovat na domácím stroji z důvodů výkonu nebo typu licence.

24. Zabezpečení přístupu do interní sítě

Z hlediska přístupů k dokumentům je také nutné pohlížet na důležitou složku bezpečnosti z hlediska přistupování do interní sítě.

25. Způsob přístupu uživatele do síťového prostředí, jeho autentizace ve smyslu rozboru problematiky 802.1x

a. Výchozí síťové požadavky v systému 802.1x

Hlavní faktory, na kterých jsou postaveny síťové služby a omezení přístupu k relevantním datům příslušného předmětu. Princip omezení je postaven tak aby bylo možno zabránit přístupu neautorizovaných počítačů a zařízení do počítačové sítě. Dále je předmětem ověřování počítačů režimem 802.1x pomocí účtu počítače v Active Directory.

[Sem zadejte text.]

Síťové prostředí je postaveno na principu segmentace sítě pomocí IP adres. Na příkladu níže byla síť rozsegmentována do VLAN a „readresována" podle nového schématu. V rámci rozhodnutí dané univerzity došlo k rozdělení PC na základě organizační struktury do úrovně jednotlivých kateder.

Ukázka segmentace sítě dle organizační struktury:

Číslo VLAN	Název-VLAN	Název AD skupiny	Název OU v AD	DNS suffix	Kód
2100	R-SR	802.1x-R-SR		sr.r.czu.cz	99100
2101	R-SK	802.1x-R-SK		sk.r.czu.cz	99200
2102	R-OI	802.1x-R-OI		oi.r.czu.cz	99810
2103	R-PRO	802.1x-R-PRO		pro.r.czu.cz	99740
2104	R-CITT	802.1x-R-CITT		citt.r.czu.cz	99130
2105	R-EO	802.1x-R-EO		eo.r.czu.cz	99400
2106	R-ORP	802.1x-R-ORP		orp.r.czu.cz	99910
2107	R-PTO	802.1x-R-PTO		pto.r.czu.cz	99300
2108	R-OMZ	802.1x-R-OMZ		omz.r.czu.cz	99920
2109	R-OB	802.1x-R-OB		ob.r.czu.cz	99500
2110	IVP	802.1x-IVP		ivp.czu.cz	61000

Tabulka č. 2 Ukázka segmentace sítě

Jednotlivé VLANy jsou rozděleny dle odhadovaného provozního modelu na odpovídající velikosti v adresním prostoru. Katedra/středisko představuje nejmenší organizační jednotku segmentace sítě. Odbor, případně vyšší stupeň organizační složky představuje v adresním rozsahu agregovanou složku pro sdružení adresního rozsahu tak, aby bylo možné útvary členit ve struktuře podobné stromu. Ukázka adresáře:

- Hlavní adresní prostor 10.0.0.0 /8 – Celá univerzita
- Podřízený adresní prostor 10.128.0.0 /16 – Úroveň Rektorátu a Fakult
- Adresní prostor pro útvary na stejné úrovni 10.128.0.0 /18 – Úroveň odborů a agregovaných celků
- Adresní prostor pro útvary na stejné úrovni 10.128.X.0/24 – Úroveň středisek rektorátu a kateder fakulty

[Sem zadejte text.]

b. Management server

V rámci implementace 802.1x je v rámci zmiňovaného případu zavedeno centrální řízení sítě pomocí Management MASTER serveru. Dle navrženého schématu systémových serverů je zvolen jeden server jako ovládací pro všechny ostatní. Na Master serveru jsou uložena všechna data, prováděna veškerá editace a konfigurace. Provedené změny jsou pak automaticky synchronizovány na jednotlivé podřízené SLAVE servery (DHCP, DNS, RADIUS). Při výpadku MASTER serveru fungují veškeré služby včetně ověřování bez omezení. Jediné, co není možné je provádět konfigurační změny.

- Služby DHCP a DNS – mimo jiného jsou na síti provozovány ještě provozní služby sítě. Jako první je na uvedeném případu implementována služba DHCP. Pro účely vysoké dostupnosti je na infrastruktuře provozován provozní režim active/active dvou samostatných DHCP serverů. Druhou službou je DNS zastávající různé role v architektuře clusteru 2 interních DNS serverů a 2 externích DNS serverů s cílem zvýšení redundance celého řešení.
- Active directory – Microsoft Active Directory je v rámci zpracovaného případu použita jako centrální autorizační databáze obsahující účty všech Windows počítačů univerzity. Dotazem do Active Directory se zjistí, zda má daný počítač vytvořený účet, zda je tento účet povolený, zda má správné heslo, do jaké skupiny patří apod. Smazání či zakázání účtu počítače v Active Directory způsobí, že se tento počítač do sítě nepřipojí.
- SMTP server a Certification services – je třeba k posílání e-mailů administrátorům i uživatelům (alerty, informační zprávy, zprávy pro uživatele o vytvoření BYOD účtu apod.) V AD doméně musí existovat Microsoft Windows Server s nainstalovanou roli Certification Authority. Z pohledu 802.1x je Certifikační Autorita potřeba pouze pro vystavení certifikátů pro NPS servery. Těmito certifikáty se potom podepisuje a šifruje 802.1x komunikace mezi klientem a NPS serverem.
- NPS servery (Network Policy Services – Microsoft implementace RADIUS) – jsou v autentizačním schématu RADIUS serverů nutné pro ověřování doménových PC. NPS má navázaný trust relationship s AD a je tím pádem jako jediný produkt schopen přímo ověřovat doménové účty.

26. Logování a práce s informacemi

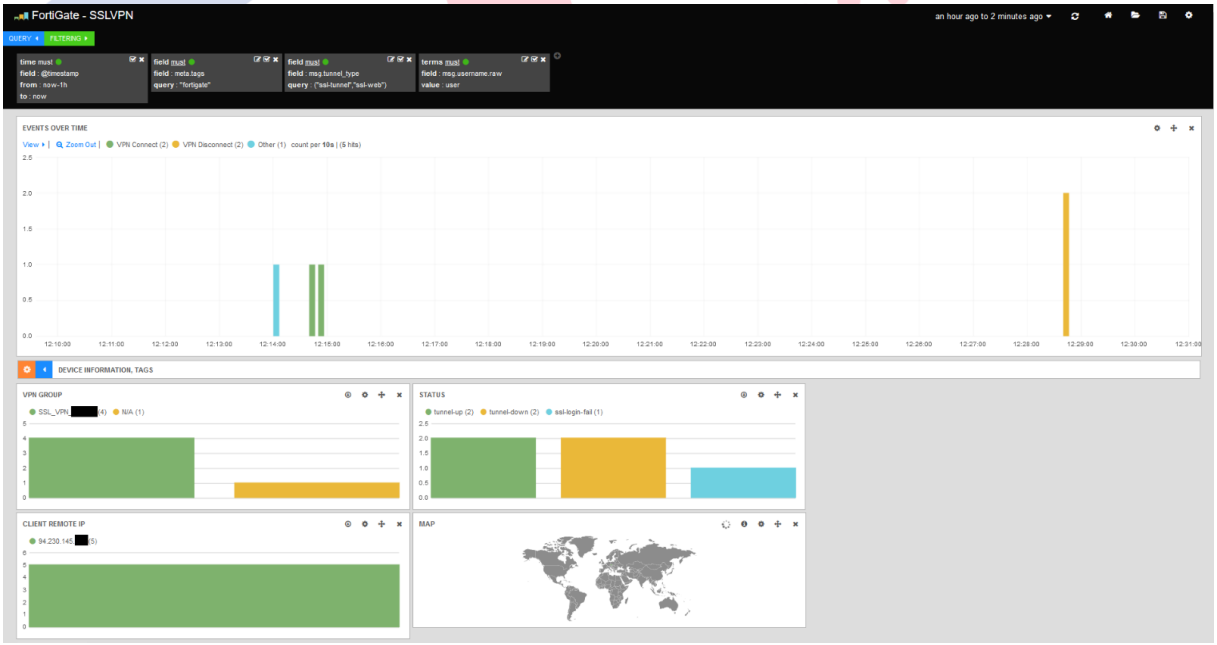
LOGmanager (viz. kapitola „Zálohování a logování LMS“) je syslog (server) přijímající data z různých zdrojů síťového zařízení za účelem sběru informací (Fortigate firewall, Windows, Office 365, atd.) a sloužící jako centrální uložiště. Formát těchto logů pak sjednocuje do definované struktury a interpretuje formou dashboardů. Každý záznam má svůj jedinečný otisk, každý index má svůj digitální součet, každý export má svůj digitální podpis.

[Sem zadejte text.]

Obrázek č. 22 LOGmanager

Z uživatelského pohledu jsou na infrastruktuře sdružovány záznamy o tom, jak se zařízení pohybuje a komunikuje v síti. Vztaženo k relevantním datům lze aplikovat na systému LOGmanager princip filtrace a vizualizace (parser). Filtrace je aplikována souhrnným způsobem na úložisti o kapacitě 120TB. Z přijmutích dat dochází k uživatelem definovanému parsování dat. Např. pro Fortigate rozdělení na DHCP žádosti, VPN, traffic log atd. Minimální nastavené podmínky na retenci dat je 6 měsíců. V závislosti na provozu univerzity se retence mění dle obsazení kapacit úložiště.

Příklad navázání VPN tunelu pro daného uživatele

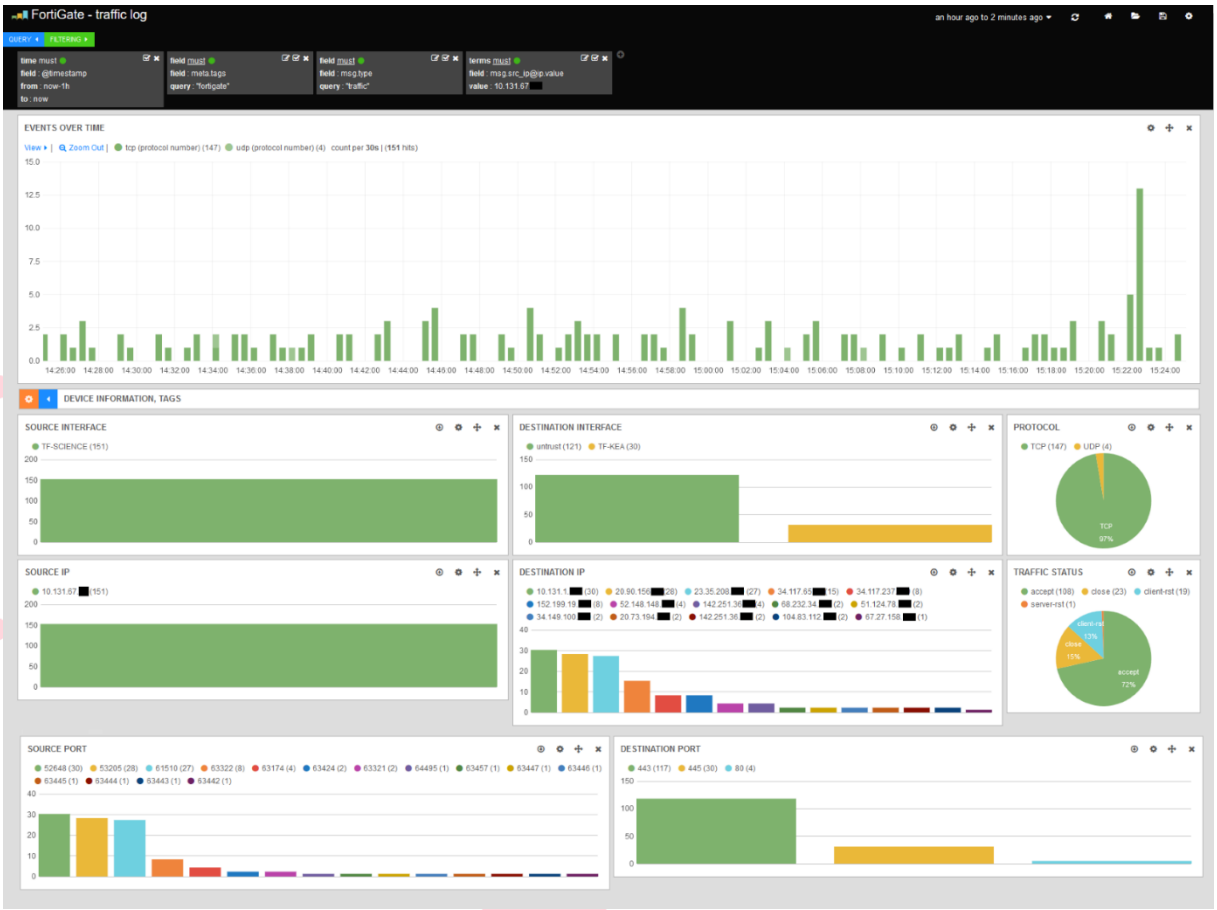


Obrázek č. 3 VPN tunel pro LOGmanager

[Sem zadejte text.]

Ze zaznamenaných dat je vidět, zjaké IP adresy a VPN skupiny se uživatel připojil. Dále uživatel ve 12:14 zadal při pokusu o VPN připojení chybné přístupové údaje a později úspěšně navázal VPN spojení, které bylo ve 12:28 ukončeno. Mapa ukazuje zeleně zvýrazněnou pravděpodobnou polohu uživatele pro každé připojení.

Příklad analýzy síťového provozu ze specifické IP adresy



Obrázek č. 4 LOGmanager síťový provoz

Mimo cílovou IP adresu lze pozorovat i čas komunikace, protokol, zdrojový a cílový port, povolení či zakázání provozu.