

## **Doporučení pro zabezpečení kolabora- tivní platformy, včetně doporučení pro její pokročilé nastavení.**

Výstup č. 5

Popis výstupu č. 5 projektu SC C2 NPO.

Pracovní skupina PS2



## Obsah

|   |           |
|---|-----------|
| <b>Anotace výstupu.....</b>   | <b>3</b>  |
| <b>Kolaborativní platforma .....</b>  | <b>3</b>  |
| <i>Komunikační platforma.....</i>   | <i>4</i>  |
| <i>Learning Management System (LMS) .....</i>   | <i>4</i>  |
| <i>Studijní informační systém .....</i>   | <i>5</i>  |
| IS STAG.....  | 5         |
| IS MU.....  | 6         |
| UIS.....  | 6         |
| <i>Integrační mezivrstva .....</i>  | <i>6</i>  |
| <b>Analýza používání nástrojů pro podporu distančních forem výuky v prostředí VVŠ .....</b> | <b>8</b>  |
| <i>Distanční forma výuky a kyberbezpečnost.....</i>   | <i>8</i>  |
| <i>Learning Management Systém.....</i>  | <i>11</i> |
| <i>Studijní informační systém .....</i>   | <i>16</i> |
| <i>Komunikační platformy.....</i>   | <i>19</i> |
| <b>Doporučení pro zabezpečení kolaborativní platformy .....</b>                             | <b>24</b> |
| <i>Komunikační platforma.....</i>   | <i>24</i> |
| <i>Learning Management System (LMS) .....</i>   | <i>25</i> |
| Používání IdM pro běžné uživatelské účty .....  | 25        |
| Hesla pro manuální účty.....  | 25        |
| Zákaz logů pro učitele.....   | 26        |
| Force login pro fotografie.....   | 27        |
| <i>Studijní informační systém .....</i>   | <i>27</i> |
| <b>Závěr .....</b>  | <b>29</b> |

## Anotace výstupu

V rámci realizace výstupu č. 5 projektu SC C2 NPO, který byl zpracován pracovní skupinou PS2, došlo ve formě dotazníkového šetření k detailní analýze stávajících či pro nasazení vyhovujících komponent kolaborativní platformy pro podporu distančního vzdělávání na jednotlivých VVŠ. Primární důraz byl však po celou dobu realizace výstupu kladen na vytvoření doporučení pro jejich patřičné zabezpečení z pohledu kybernetické a informační bezpečnosti za pomoci implementace ověřených způsobů ochrany. Eliminace nežádoucích vnějších vlivů či systémových rizik plynoucích ze současné praxe bylo dosaženo za pomoci kombinace pokročilého nastavení bezpečnostních mechanismů zvolené kolaborativní platformy a uplatňování bezpečnostních politik splňujících požadavky na realizaci distančního vzdělávání.

V rámci níže uvedených kapitol jsou tak postupně popsány jednotlivé komponenty kolaborativní platformy, představeny výstupy z analytického dotazníkového šetření, jež bylo realizováno za účelem zpracování analýzy používání nástrojů pro podporu distančních forem výuky v prostředí VVŠ a následně pak detailně popsány způsoby a doporučení pro zajištění zabezpečení jednotlivých komponent kolaborativní platformy, včetně doporučení pro jejich pokročilé nastavení.

Jelikož se v rámci jednotlivých doporučení často jedná o komplexní a systematická nastavení jednotlivých komponent, jsou tyto informace součástí odkazovaných externě dostupných znalostních bází a úložišť, nejsou součástí tohoto dokumentu.

## Kolaborativní platforma

Již v rámci návrhu projektu SC C2 NPO byl definován plně integrovaný ekosystém nástrojů sloužící pro podporu a realizaci distančních forem výuky, který byl označen jako „kolaborativní platforma“. Tento název byl zvolen z důvodu akcentování podpory přímé spolupráce v rámci realizace distančního vzdělávání, které se stalo trendem během pandemie COVID-19. Komplexní řešení v podobě kolaborativní platformy se skládá z celkem tří základních komponent v podobě:

- **Komunikační platformy**
- **E-learningové platformy (LMS)**
- **Studijního informačního systému**

Nad těmito třemi komponentami je pak umístěna ještě i čtvrtá komponenta kolaborativní platformy, která plní roli **distribované integrační vrstvy** (v podobě tzv. mezivrstvy), jež se typicky nachází na úrovni propojení jednotlivých komponent či na úrovni API. Jejím smyslem je například umožnit zpřístupnění úložiště pro odevzdávání zadaných úkolů, založení prostoru vybrané seminární skupiny,

automatické přihlášení studentů do předmětu či odeslání pozvánky na schůzku jen účastníkům přihlášeným do konkrétního kurzu.

## Komunikační platforma

Komunikační platforma představuje komponentu kolaborativní platformy pro podporu online a hybridní výuky (v podobě online a hybridních přednášek a cvičení), která zajišťuje funkce související především se zajištěním operativní i plánované komunikace mezi vyučujícími a studenty, a to jak formou chatu (včetně bohatého formátování, možnosti posílání obrázků a předávání dokumentů), tak formou hlasových a videohovorů. Platforma umožňuje operativní ad hoc komunikaci mezi libovolnými dvěma nebo více učiteli/studenty, nebo komunikaci v rámci dlouhodobě existujících skupin odpovídajících například vyučujícím a studentům předmětu v konkrétním semestru. V těchto skupinách mohou být kromě možností komunikace k dispozici i další nástroje, například pro sdílení dokumentů a spolupráci nad dokumenty, zadávání a odevzdávání úkolů a podobně. Touto funkcí se komunikační platforma může částečně překrývat s nástroji pro *Learning Management System* (tzv. „LMS“).

Oblíbenými nástroji v této kategorii jsou MS Teams, Google Meet a Zoom, což také potvrdil průzkum realizovaný v rámci pracovní skupiny PS1 projektu SC C2 NPO. Každý z těchto nástrojů měl na jednotlivých VVŠ již od začátku poměrně širokou bázi uživatelů a umožňoval naplňovat potřeby, které na začátku pandemie náhle vyvstaly ve spojitosti s potřebou přejít do online prostředí.

Na druhou stranu však žádný z těchto nástrojů nebyl připraven na skokový nárůst jeho využití a otázka bezpečnosti byla rovněž řešena jen na nejnižší úrovni, což se velmi rychle stalo kritickým faktorem, který bylo potřeba urgentně řešit.

## Learning Management System (LMS)

LMS (*Learning Management System*) představuje komponentu kolaborativní platformy pro podporu online a hybridní výuky, která umožňuje práci v rámci online kurzů. Jeho klíčové vlastnosti lze najít již v samotné anglické zkratce, která v doslovném překladu znamená „systém pro řízení výuky“.

Mezi hlavní funkce LMS spadá vytváření a správa studijních materiálů formou online výuky, které lze pomocí integrovaných nástrojů distribuovat studentům, přidělovat jim uživatelská a administrátorská práva a řídit celý proces elektronického vzdělávání. Zároveň je také možné sledovat jejich postup při studiu připravených online materiálů pomocí připravených statistik a sestav a díky tomu efektivně řídit proces samostudia.

Kromě studijních materiálů ale LMS umožňují i vykonávání studijních aktivit jako např. skládání testů (a to jak za účelem sumativního, tak i formativního hodnocení) nebo odevzdávání a hodnocení úkolů. LMS nadto tak obsahují nástroje pro administraci studia a evidenci studijních výsledků – uživatelé umožňují jednoduše klasifikovat na studující a vyučující a na základě toho jim přidělovat pravomoci v rámci systému. Vždy se ale jedná o online aplikaci, ke které studenti přistupují pomocí internetového prohlížeče nebo mobilní aplikace.

Dle průzkumu realizovaného v rámci pracovní skupiny PS1 projektu SC C2 NPO patří mezi nejčastěji používané e-learningové platformy na českých VVŠ LMS nástroj Moodle.

## Studijní informační systém

Studijní informační systém (SIS) je jednou z hlavních a neoddělitelných komponent kolaborativní platformy každé VVŠ. SIS totiž typicky slouží nejen jako administrativní a podpůrný nástroj pro realizaci jak prezenční, tak i distanční výuky, ale také jako primární zdroj veškerých informací o studentech, vyučujících, předmětech, hodnoceních, místnostech a dalších důležitých agendách.

Dle prvotního průzkumu pracovní skupiny PS1 projektu SC C2 NPO jsou na českých VVŠ nejvíce rozšířeny 3 studijní systémy – IS STAG, IS MU a UIS jež jsou pak doplněny ještě řadou vlastních řešení, jako je například KOS v případě ČVUT Praha.

### IS STAG

Studijní agenda IS/STAG je informační systém určený pro administraci studijní agendy vysoké školy. Pokrývá funkce od přijímacího řízení až po vydání diplomu. Umožňuje evidovat studenty prezenční i kombinované formy studia, účastníky celoživotního vzdělávání i účastníky univerzity třetího věku. Poprvé se IS/STAG použil v roce 1993 na ZČU. V současnosti je na ZČU provozována v rutinním provozu již třetí vývojová verze tohoto systému. IS/STAG je celouniverzitní systém určený pro administraci studia, nikoliv pro podporu studia. IS/STAG je napojen na několik systémů pro podporu studia. IS/STAG eviduje jak kreditní, tak i nekreditní systém studia. Aplikace umožňuje prohlížení některých částí bez přihlášení – informace pro veřejnost a zároveň umožňuje zobrazení různého obsahu po přihlášení uživatele (administrátor, učitel, katedra, studijní referent atd.) a studenty. Aplikace IS/STAG je nepřetržitě aktualizována. Webové rozhraní aplikace (studijní portál) podporuje přihlášení pomocí SSO, díky kterému je plně integrován do prostředí organizace.

## IS MU

Významným zástupcem studijních informačních systémů na českých školách je Informační systém MU, který vyvíjí a pro několik škol provozuje Fakulta informatiky MU od roku 1999. Podporuje studijní administrativu, e-learning a komunikaci uvnitř školy a je masivně využíván desítkami tisíc přihlášených uživatelů denně. Základní funkcí systému je správa identit uživatelů (studentů, učitelů, pracovníků školy a externistů), jejich autentizace, včetně možnosti dvoufaktorového ověření s využitím Identity občana nebo časově závislého jednorázového hesla (TOTP). Uvnitř systému lze komplexně řídit přístupová práva, jak individuální a skupinová, tak na základě uživatelských rolí. Do IS MU je začleněn systém pro řízení výuky (LMS). Poskytuje několik komponent, zejména zabezpečené distribuované úložiště dat, systém pro testování znalostí studentů a nástroje pro komunikaci offline i online formou. Integrovaná je i vlastní kontrola podobností pro prevenci a odhalování plagiátorství textů. Provozovatelé v souvislosti s bezpečností také kladou důraz na vysokou dostupnost, systém sleduje počty provedených operací, brání přetěžování (anti-scraping), nevyžádané pošty a dokáže reagovat na zvýšenou zátěž.

## UIS

UIS je studijní informační systém, který byl vyvinut pro potřeby Vysoké školy ekonomické v Praze, ale následně byl rozšířen i na další vysoké školy, a to jak veřejné, tak soukromé. Studijní informační systém UIS je tak využíván jak na VŠE, tak i na Mendelově univerzitě a Česká zemědělská univerzita.

## Integrační mezivrstva

Integrační mezivrstva je poslední významnou komponentou kolaborativní platformy. Její primární funkcionalita spočívá v propojení jednotlivých komponent kolaborativní platformy v jedno funkční, rozšiřitelné a zabezpečené řešení zajišťující podporu a realizaci distančních forem výuky. Typicky se nejedná o jednotný systém, ale sadu komponent nebo samostatných systémů poskytujících níže uvedené funkce.

Integrační mezivrstva například zajišťuje propojení komunikační platformy s jinými komponentami kolaborativní platformy nebo i další ICT infrastrukturou vysoké školy. Může být reprezentována jednotným mechanismem pro přihlašování do několika nebo všech komponent kolaborativní platformy (ať už za pomoci protokolu *SAML 2.0* či *Open ID Connect – OIDC*).

Integrační mezivrstva je využíváno také při přihlašování do dalších systémů školy (např. za pomoci jednotného poskytovatele identit, Identity Provider, IdP), či při využití jednotného systému pro správu účtů učitelů a studentů v podobě identity managementu (IdM) a jejich vazby na předměty a

podobně. Zakládání skupin pro předměty a správa studentů a učitelů z nich mohou být realizovány z LMS, SIS nebo IdM.

Za pomoci integrační mezivrstvy tak může být zajištěno zakládání termínů online přednášek na základě rozvrhu z LMS nebo SIS, přenášení výukových materiálů mezi komunikační platformou a LMS nebo přenášení výsledků zkoušení z komunikační platformy do LMS/SIS.



## **Analýza používání nástrojů pro podporu distančních forem výuky v prostředí VVŠ**

Abychom byli schopni v rámci pracovní skupiny poskytnout vhodná doporučení zabezpečení a nastavení jednotlivých komponent kolaborativní platformy, byla provedena analýza současných nástrojů pro distanční výuku jednotlivých VVŠ, a to prostřednictvím online dotazníkového šetření za využití aplikace MS Forms. Cílovou skupinou byly všechny VVŠ v ČR a podařilo se nám získat odpověď od každé z nich.

Dotazníkové šetření se skládalo z 59 otázek zaměřených technicky, procesně i organizačně. Ty byly rozděleny do 4 tematických okruhů:

- **Distanční forma výuky a kyberbezpečnost**
- **Learning Management System**
- **Studijní informační systém**
- **Komunikační platformy.**

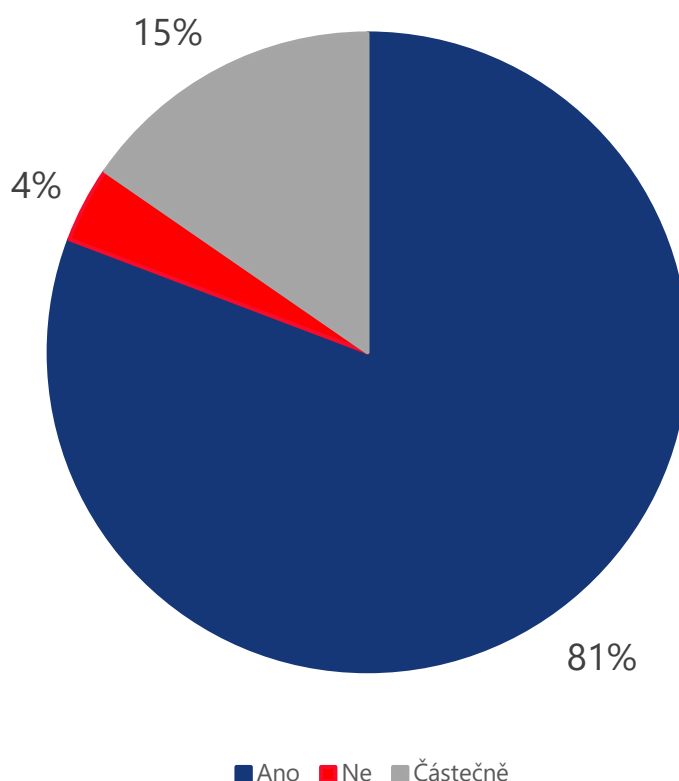
Došlo tak ke komplexnímu zmapování a následnému rozboru situace na jednotlivých VVŠ.

### **Distanční forma výuky a kyberbezpečnost**

Primárním cílem tohoto oddílu bylo zjistit podrobnosti o organizaci distanční výuky a identifikovat stav kybernetické bezpečnosti na dané instituci.

Úvodním a zároveň jedním ze stěžejních dotazů bylo, zda jednotlivé VVŠ jsou schopny přejít v případě nouzového stavu do distanční formy výuky. Ze získaných odpovědí, můžeme konstatovat, že 81 % VVŠ, což odpovídá počtu 21 institucí, je schopno přejít na distanční formu výuky. Z celkového počtu 26 VVŠ, pak 4 instituce mají možnost přejít na distanční formu výuky pouze částečně, a to dle charakteru jednotlivých studijních oborů. Možnost „Ne“ zvolila pouze jediná instituce.

## Jsou jednotlivé VVŠ schopné přejít do distanční formy výuky?



Graf 1: Jsou jednotlivé VVŠ schopné přejít do distanční formy výuky?

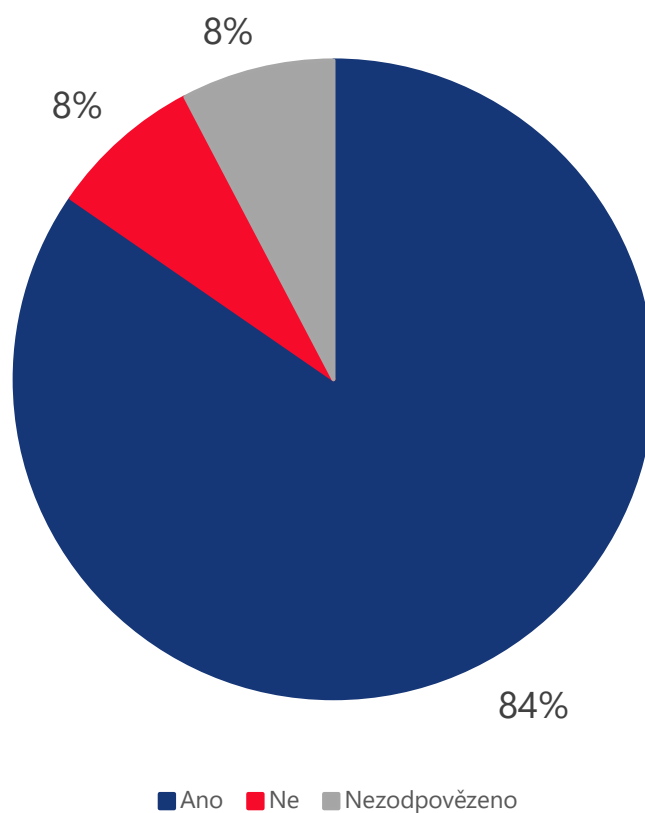
Další sada otázek v oddíle byla zaměřena především na metodiky, směrnice, politiky a sady doporučení na jednotlivých institucích regulující distanční systém výuky.

Z analýzy vyplynulo, že pouze 8 % VVŠ má uveřejněnou „Bezpečnostní politiku pro nástroje pro podporu distančního vzdělávání“ a pouze 12 % institucí disponuje „Souborem bezpečnostních politik“. Pouhých 23 % institucí pak má „Soubor technických opatření“ a 27 % „Soubor organizačních opatření“. K vyššímu číslu pak vedla otázka na „Metodiky, směrnice nebo doporučení pro využívání nástrojů distanční výuky“, ve které 42 % respondentů uvedlo, že dané dokumenty na jejich instituci existují. Z pohledu kyberbezpečnostních incidentů a reakcí na ně pak však pouze 38 % VVŠ odpovědělo kladně na otázku, zda mají „Soubor procesů, jak reagovat na kyberbezpečnostní incidenty a události v rámci distanční výuky“.

Aktivnímu řešení kyberbezpečnosti při distanční výuce se dle šetření věnuje 62 % VVŠ.

Základní technickou podporu studentů a zaměstnanců v průběhu distanční výuky je pak schopno poskytnout 84 % institucí. VVŠ, které tuto možnost neposkytují je 8 % rovněž, jako respondentů, kteří na tuto otázku odpověděli možností „Nezodpovězeno“.

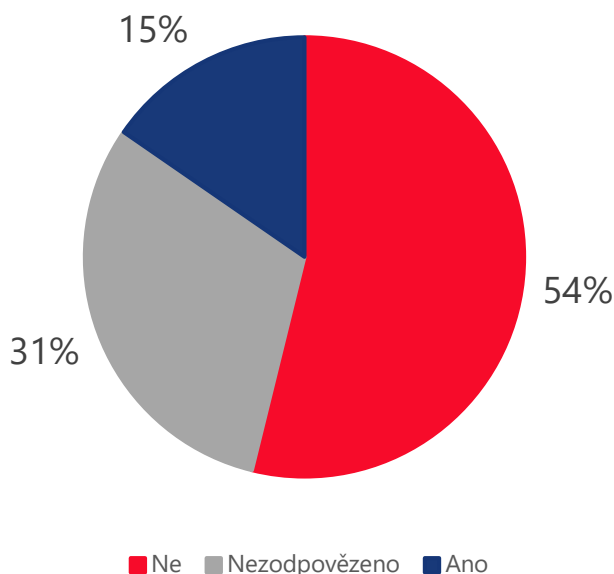
Zajišťujete během distanční výuky technickou podporu studentů a zaměstnanců?



Graf 2: Zajišťujete během distanční výuky technickou podporu studentů a zaměstnanců?

Na otázku „Řešili jste v minulosti kyberbezpečnostní incident spojený s distanční výukou?“ odpovědělo 15 % respondentů kladně, 54 % záporně a 31 % na danou otázku nechtělo odpovídat.

### Řešili jednotlivé VVŠ při distanční výuce kybernetické incidenty?



Graf 3: Řešili jednotlivé VVŠ při distanční výuce kybernetické incidenty?

Nejčastějšími formami kyberbezpečnostních incidentů, které respondenti uváděli bylo:

- Narušení videokonferenční výuky spammerem
- Narušení důvěrnosti
- Nedostupnost systémů z důvodu přetížení
- Podvody studentů při výuce/zkoušek/testů

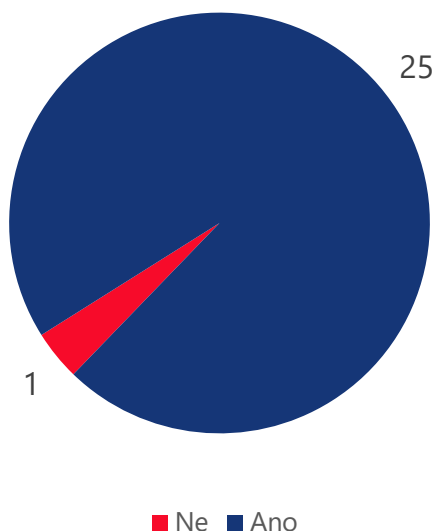
Otázkou zabezpečení integrační vrstvy jednotlivých komponent kolaborativní platformy se zabývá 65 % VVŠ. Nejčastějším uváděným způsobem zabezpečení je prostřednictvím API, šifrování dat a vícefaktorového ověření (MFA).

## Learning Management Systém

Hlavním cílem tohoto oddílu bylo zjistit využití LMS na jednotlivých VVŠ a jeho základní nastavení.

Z šetření vyplynulo, že pouze jedna instituce nevyužívá možnosti LMS, zbylé instituce využívají jeden či více LMS pro zajištění distanční výuky.

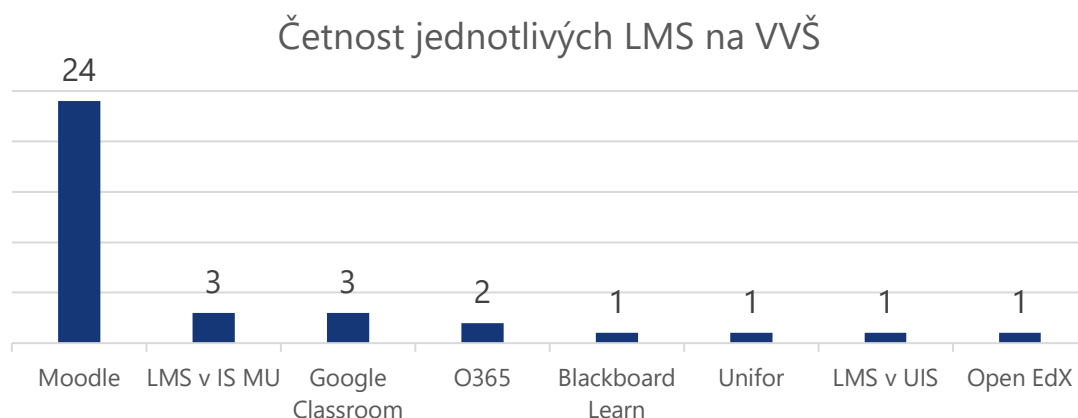
Využíváte v rámci Vaší VVŠ  
Learning Management System  
pro zajištění distanční výuky?



Graf 4: Využíváte v rámci Vaší VVŠ Learning Management Systém pro zajištění distanční výuky?

Následující otázky oddílu byly pokládány pouze respondentům, kteří využívají LMS, tedy 25 institucím.

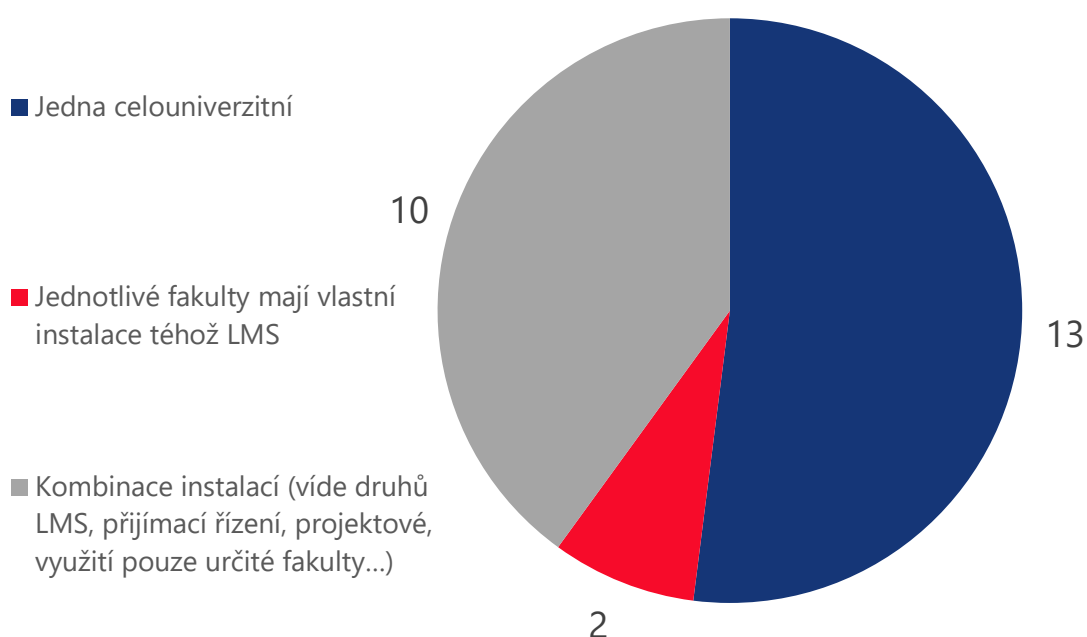
Další otázka cílila již na konkrétní typy LMS. Výsledky šetření nám potvrdily předpokládanou oblíbenost systému Moodle, který v současné době používá 96 % VVŠ využívajících LMS pro distanční formu výuky. Pouze jediná instituce nepracuje s nástrojem Moodle, ale namísto toho má LMS implementovaný v Informačním systému MU. Některé instituce také uvedly, že využívají více než jen jedno LMS.



Graf 5: Četnost jednotlivých LMS na VVŠ

V další otázce jsme se ptali „Využíváte jednu instalaci LMS pro celou univerzitu, nebo mají jednotlivé fakulty vlastní instalace?“ Z odpovědí vyplynulo, že 52 % institucí, které využívají LMS, mají jednu celouniverzitní instalaci. Dalších 40 % odpovědělo, že jednotlivé fakulty disponují svými vlastními instalacemi LMS. Zbýlých 8 % uvedlo, že instalace na jejich VVŠ jsou různé a to např. z důvodu využívání více druhů LMS, různých potřeb využití LMS (přijímací řízení, projekty atd.) případně dané LMS využívá jen určitá fakulta.

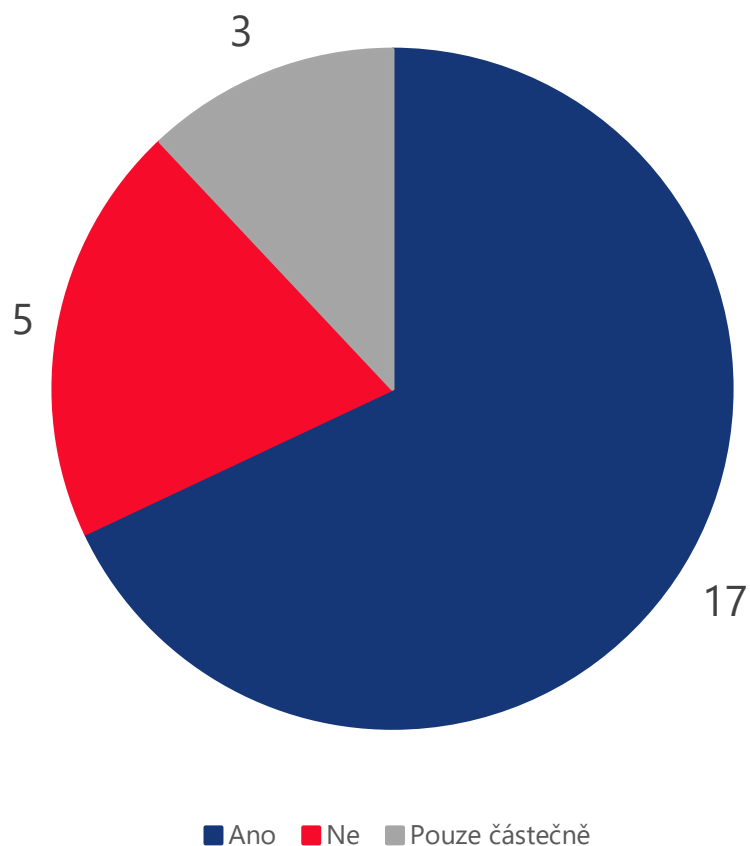
### Způsoby instalace LMS na jednotlivých VVŠ



Graf 6: Způsoby instalace LMS na jednotlivých VVŠ

Otázkou „Je Váš LMS integrován do studijního informačního systému?“ jsme zjišťovali propojenost jednotlivých komponent kolaborativní platformy pro distanční výuku, a to konkrétně LMS a SIS. Z šetření vyplynulo, že celkem 20 institucí má svůj LMS integrován do SIS, z toho 17 v plném rozsahu a 3 částečně (většinou byla uváděna implementace pouze jednoho z více LMS instituce případně pouze jednosměrná integrace). Zbýlých 5 respondentů odpovědělo, že tyto komponenty v rámci instituce nemají integrovány.

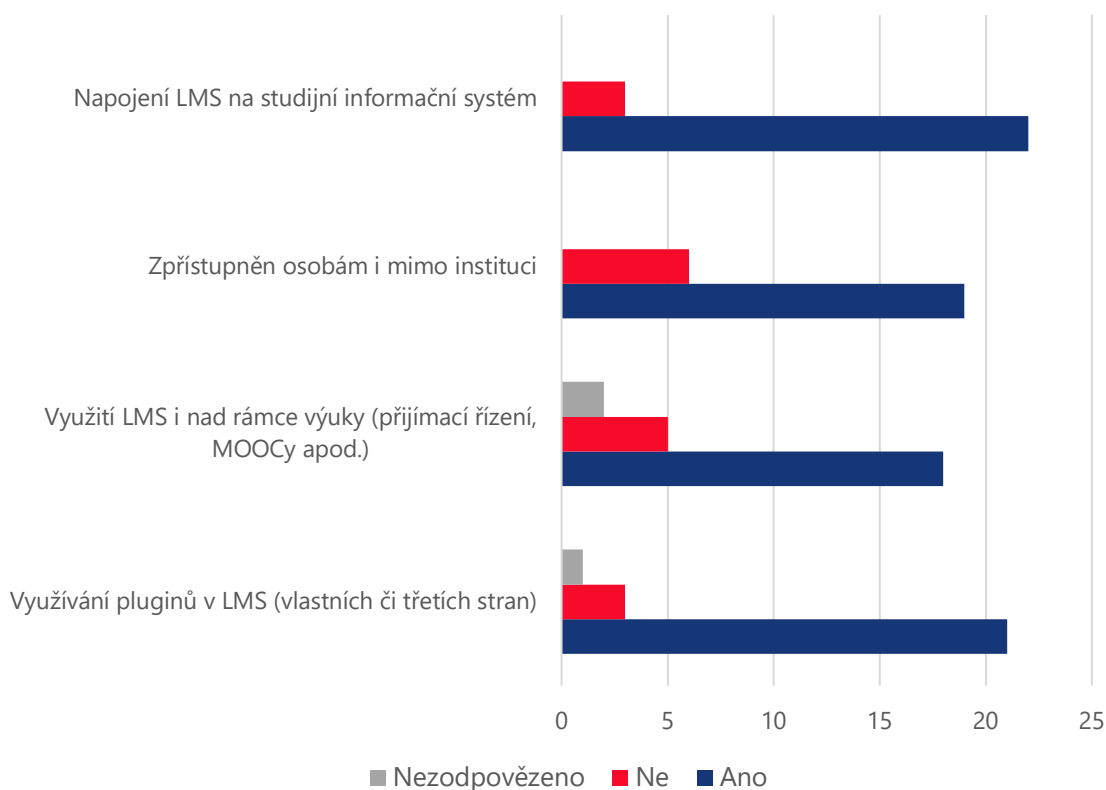
### Integrace LMS do SIS?



Graf 7: Integrace LMS do SIS

V další části oddílu jsme se zaměřili na způsoby využití LMS a jeho napojení na pluginy či SIS. Cílem bylo zjistit, propojení LMS s dalšími systémy a také jaké osoby mohou mít do systému přístup. Tyto informace nám pomohou zjistit rozsah využití LMS a možná bezpečnostní rizika spojená s přístupy.

## LMS a jeho využití



Graf 8: LMS a jeho využití

Na grafu vidíme, že většina VVŠ svůj LMS využívá i pro osoby mimo instituce a zároveň využívá možnosti napojení na SIS a pluginy, a to ať už vlastní, či třetích stran. Většina respondentů také uvedla, že LMS používají i nad rámec výuky, a to například při přijímacím řízení.

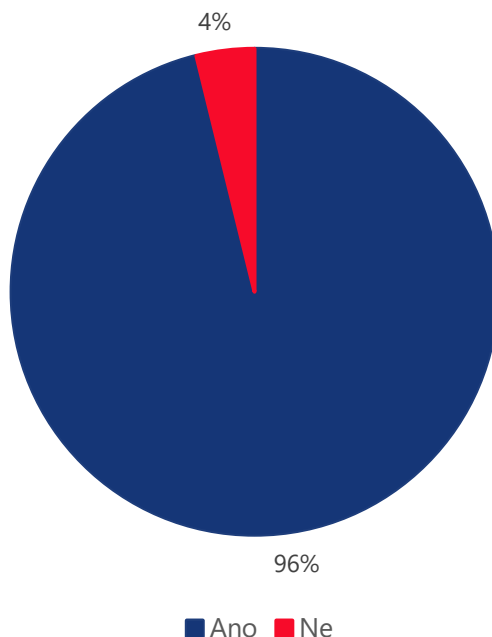
V doplňující otázce „Používá Vaše instituce ještě další systémy pro distanční výuku, které jsou napojené na LMS (případně na SIS či Microsoft 365)?“ respondenti uvedli využití následujících systémů:

- Turnitin – antiplagiátorský doplněk
- Mediasite
- BigBlueButton
- MS 365
- Medial
- Mahara

V poslední otázce tohoto tematického oddílu jsme se respondentů dotázali, zda by měli zájem o zpracování tématu zabezpečení LMS. Celých 96 % VVŠ odpovědělo kladně.



Měli byste zájem o zpracování tématu zabezpečení LMS?



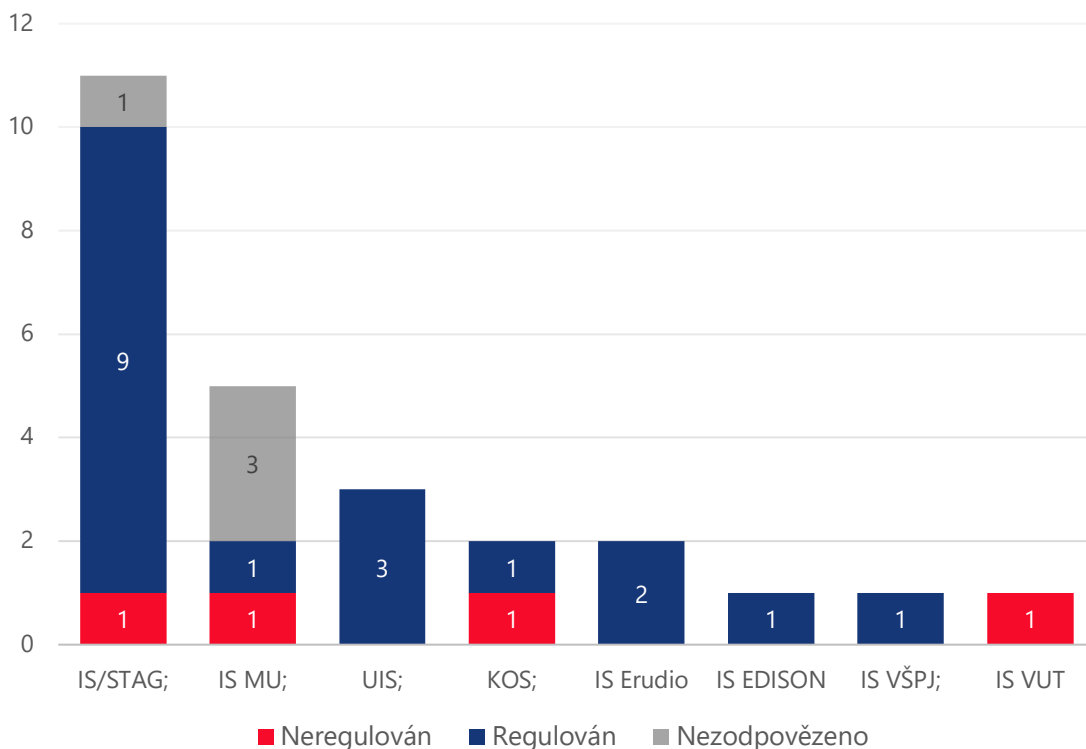
Graf 9: Mají VVŠ zájem o zpracování tématu zabezpečení LMS?

## Studijní informační systém

V oddíle zaměřeném na studijní informační systém (SIS) nás především zajímal druh využívaného SIS na jednotlivých institucích, zda je regulován dle ZoKB č. 181/2014 Sb. a zda jsou do něj integrovány další nástroje pro podporu distanční výuky jako je např. LMS či komunikační platforma.

Z průzkumu vyplynulo, že nejpoužívanějším SIS na českých VVŠ je IS/STAG, který využívá celkem 11 institucí a z toho na 9 z nich je regulován dle ZoKB. Druhým nejpoužívanějším SIS je IS MU a za ním následuje UIS. V menším počtu či jednotkách se pak objevují systémy KOS, IS Erudio, IS EDISON, IS VŠPJ a IS VUT. Z celkového počtu 26 SIS je 18 z nich regulováno dle ZoKB.

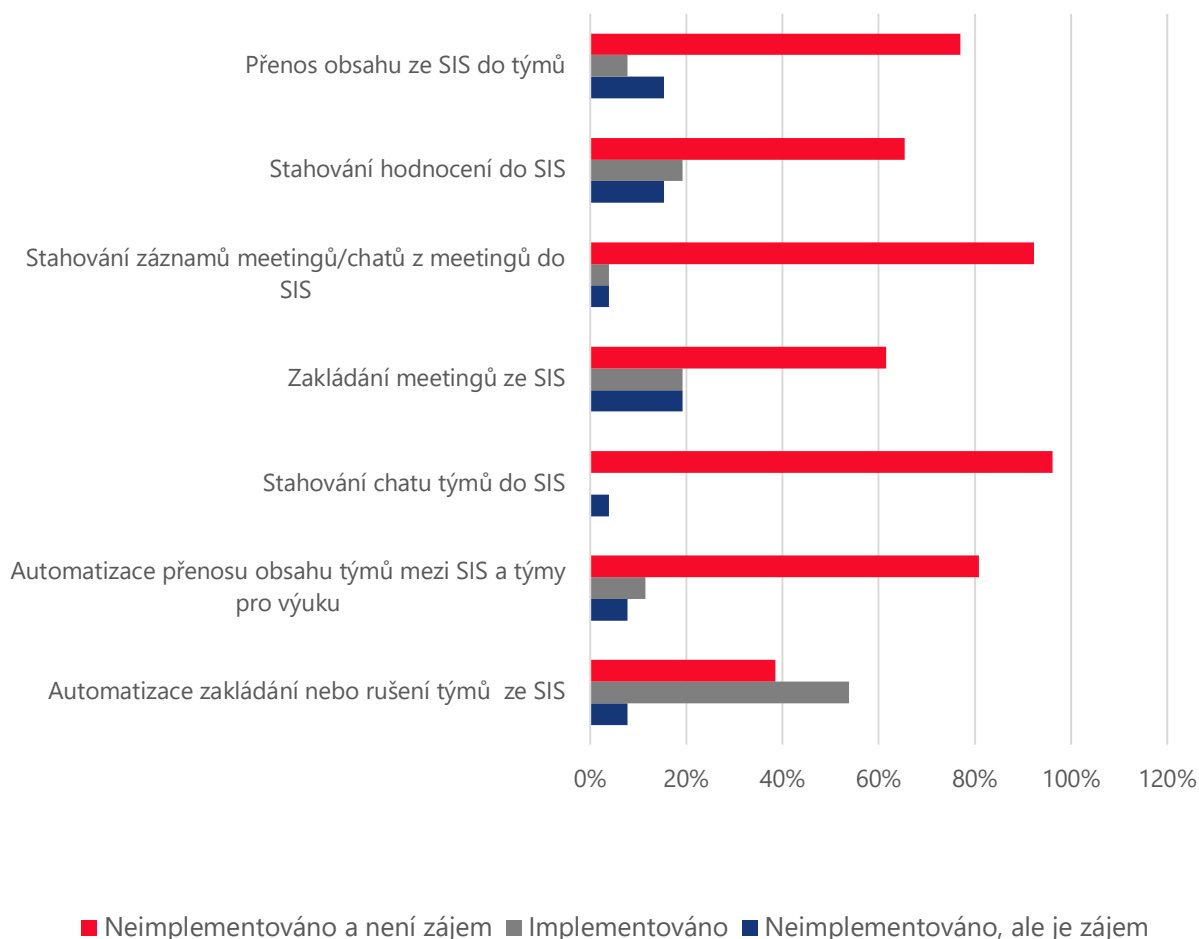
### Četnost použití jednotlivých SIS a jejich regulace dle ZoKB



Graf 10: Četnost použití jednotlivých SIS a jejich regulace dle ZoKB

V dalších otázkách jsme se zaměřili na zmapování funkcí mezi SIS a dalšími komunikačními platformami. Z šetření vyplynulo, že většina VVŠ dotazované funkce nemá implementované a zároveň o jejich nastavení nemá ani zájem. V grafu 11 můžeme vidět, že funkce, o kterou respondenti projevili největší zájem je „Zakládání meetingů ze SIS“ jež by uplatnilo ve svém SIS 5 institucí. „Automatizace a zakládání nebo rušení týmu ze SIS“ pak již implementovalo celkem 14 VVŠ. Jedná se tak o nejvyužívanější funkci napojenou na SIS z dotazovaných možností.

## Stav implementace a zájmu o jednotlivé funkce mezi SIS a komunikačními platformami



Graf 11: Stav implementace a zájmu o jednotlivé funkce mezi SIS a komunikačními platformami

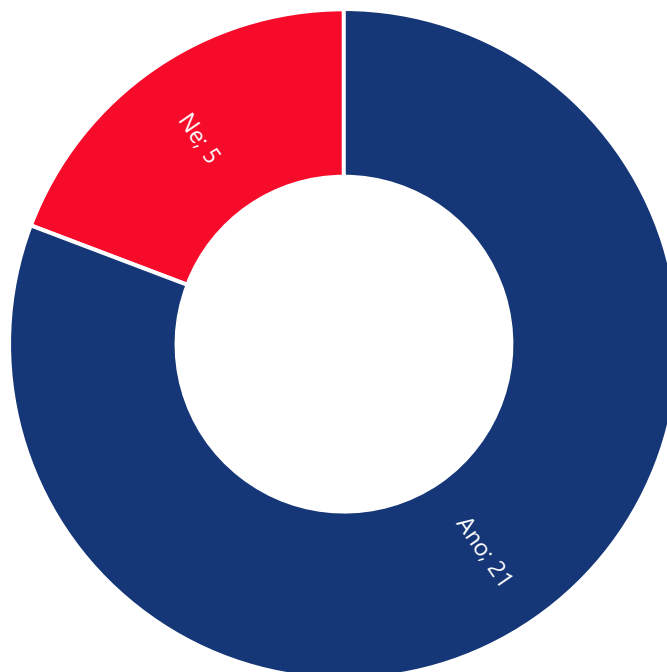
V otevřené otázce jsme se respondentů dotázali na to „Jaké nástroje pro podporu distančního vzdělávání jsou plně integrovány do Vašeho SIS?“. Z analýzy vyplynulo, že instituce integrovaly tyto nástroje (seřazeno od nejvyšší četnosti):

- MS Teams
- Moodle, LMS
- Google Classroom

Od 3 respondentů se nám pak dostalo odpovědi, že ve svém SIS žádné nástroje pro podporu distanční výuky nemají a jeden respondent označil možnost „Nezodpovězeno“.

V poslední otázce jsme se respondentů dotázali, zda by měli zájem o bezpečnostní doporučení k zabezpečení SIS. Celkem 21 institucí se vyjádřilo kladně. Tato problematika se však již řeší v projektu CRP-KYBER23, proto se jí v rámci tohoto projektu nebudeme věnovat.

Měly by VVŠ zájem o bezpečnostní doporučení k zabezpečení SIS?



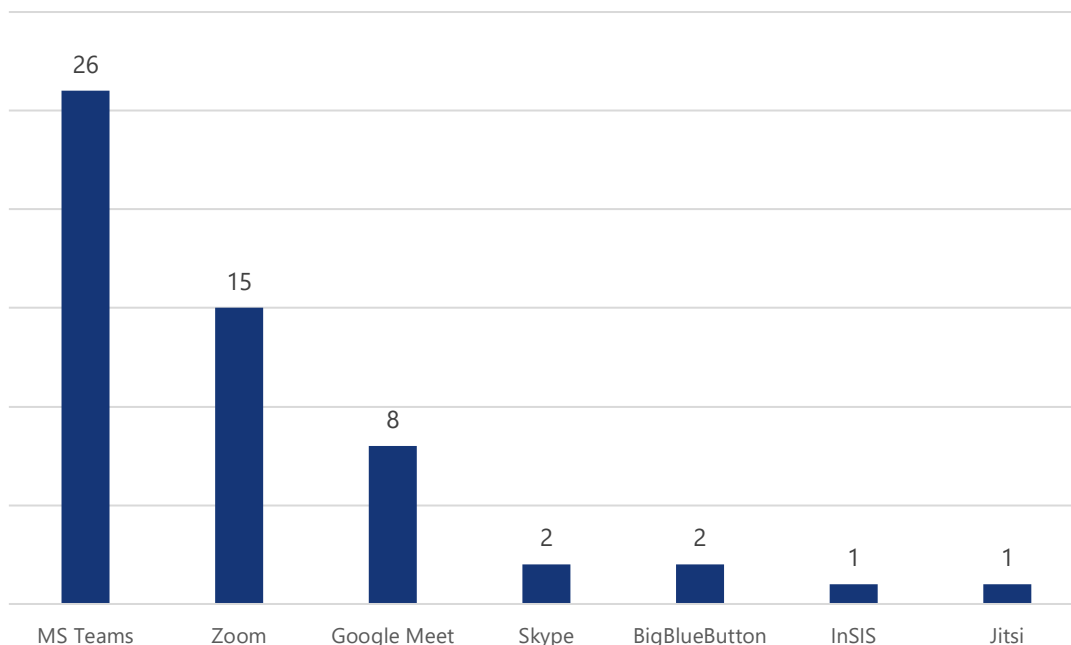
Graf 12: Mají VVŠ zájem o bezpečnostní doporučení k zabezpečení SIS?

## Komunikační platformy

V této tematické části jsme se zaměřili především na mapování formy a rozsahu využití cloudových služeb komunikačních platforem.

První dotaz byl zaměřen na samotné komunikační nástroje, a to konkrétně na jejich druhy, které jednotlivé VVŠ oficiálně využívají. Z šetření vyplynulo, že všech 26 institucí využívá služeb MS Teams a více než 50 % z nich využívá více než jednu komunikační platformu. Druhým nejčastějším nástrojem byl Zoom, který používá 15 respondentů. V 8 případech byl také označen za jednu z oficiálních komunikačních platforem Google Meet. V nízkých jednotkách se pak v odpovědích objevil i Skype, BigBlueButton, InSIS a Jitsi.

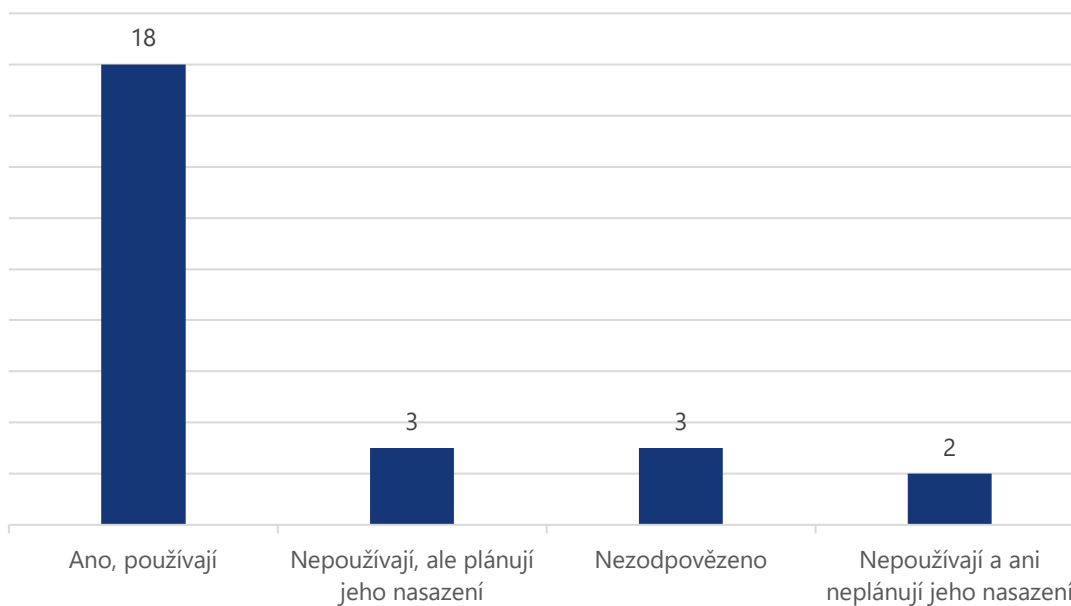
### Četnost používaných komunikačních nástrojů



Graf 13: Četnost používaných komunikačních nástrojů

Rutinní nasazení MS 365 pro účely výuky (běžná přístupnost studentům i vyučujícím) má 18 institucí. Ze zbylých respondentů pak 3 z nich nasazení plánují, 3 zvolili možnost „Nezodpovězeno“ a 2 rutinní nasazení neplánují.

### Používají nebo plánují VVŠ rutinní nasazení MS 365 pro účely výuky?



Graf 14: Používají nebo plánují VVŠ rutinní nasazení MS 365 pro účely výuky?

Dále jsme v rámci šetření zjišťovali i využitelnost jednotlivých nástrojů MS 365 nebo Azure pro zajištění/podporu/hodnocení výuky. Z výsledků vyplynulo, že nejvíce oblíbená je pošta v MS 365, kterou využívá 65 % dotazovaných. Zbylé nástroje používá méně než 50 % respondentů viz. Tabulka 1.

| Využití jednotlivých nástrojů MS 365/Azure na VVŠ |      |
|---|------|
| MS Azure  | 19 % |
| PowerAutomate/PowerApps                           | 12 % |
| Pošta v MS 365                                    | 65 % |
| Analytické nástroje (např. Power BI)              | 31 % |

Tabulka 1: Využití jednotlivých nástrojů MS 365/Azure na VVŠ

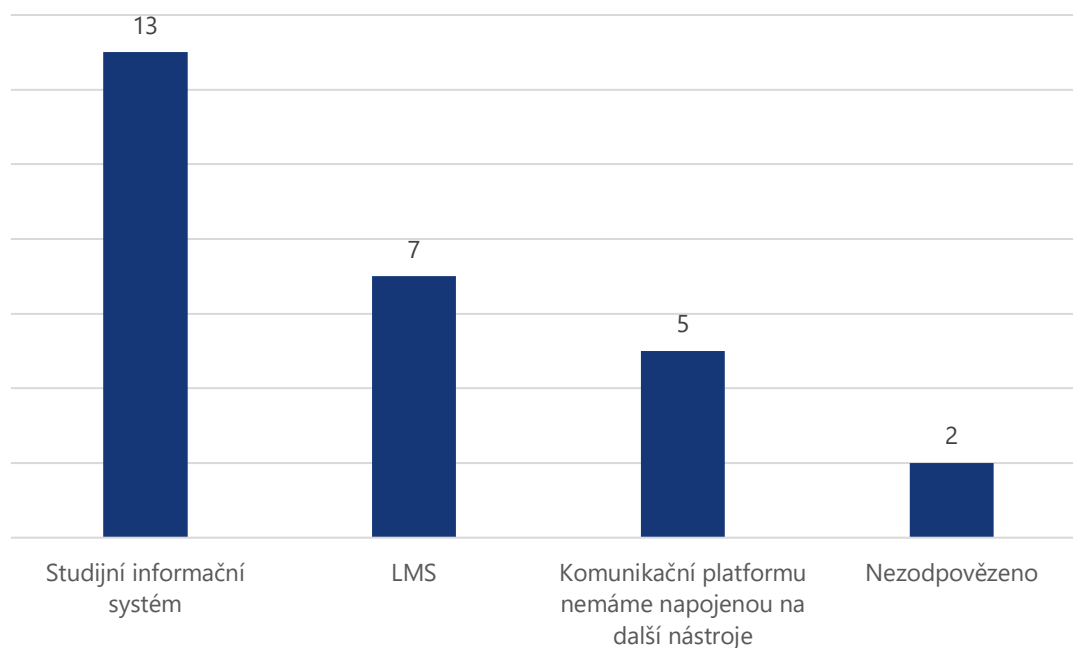
Další část oddílu byla zaměřena na zájem institucí o doporučení pro zabezpečení konkrétních nástrojů či procesů. Z výsledků vyplynulo, že největší poptávka je po doporučení pro práci s citlivými daty (81 %) a zabezpečení elektronické pošty (77 %). V případě práce s citlivými daty z dotazníkového šetření taktéž vzešlo, že 6 institucí již v prostředí MS 365 s daty pracuje nebo to plánuje.

| Zájem VVŠ o základní doporučení pro zabezpečení: |      |
|--|------|
| Rutinního nasazení MS365                         | 46 % |
| Práce s citlivými daty                           | 81 % |
| Elektronické pošty                               | 77 % |
| MS Azure   | 54 % |
| PowerAutomate/PowerApps                          | 46 % |
| Datová analytika (Např. Excel nebo Power BI)     | 58 % |

Tabulka 2: Zájem VVŠ o základní doporučení pro zabezpečení

Z pohledu integrace komunikačních nástrojů do dalších komponent kolaborativní platformy jsme se ptali na otázku „Na jaké další nástroje máte napojenou Vaši komunikační platformu?“. Z celkového počtu 26 odpovědí jsme zjistili, že 5 institucí nemá komunikační platformu napojenou na další nástroje, 2 respondenti zvolili možnost „Nezodpovězeno“ a ve 20 případech je komunikační nástroj napojen na SIS, LMS nebo kombinaci obojího.

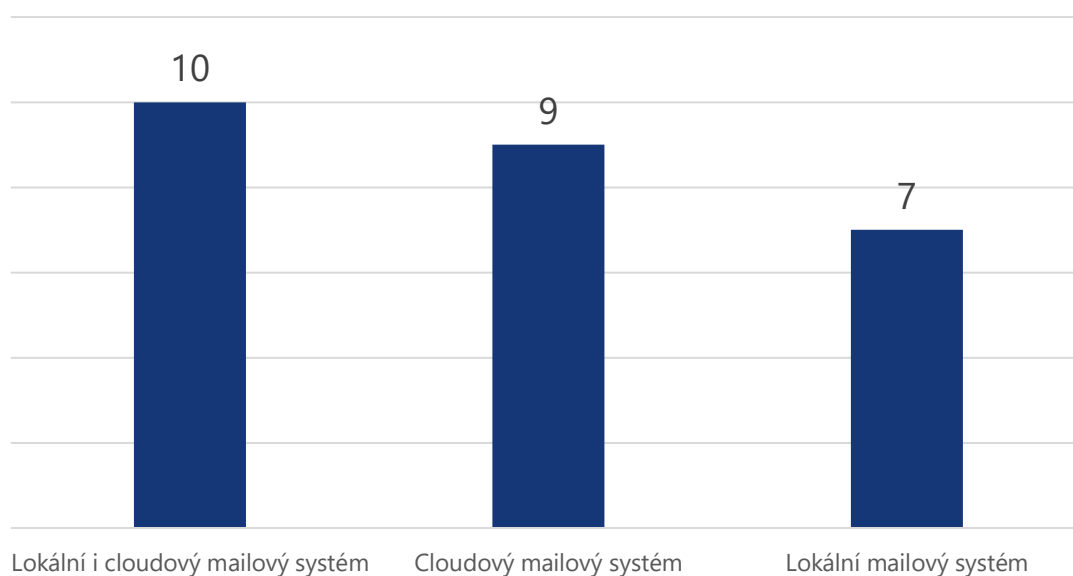
### Nástroje napojené na komunikační platformu VVŠ



Graf 15: Nástroje napojené na komunikační platformu VVŠ

Vzhledem k tomu, že pro velkou část elektronické komunikace VVŠ využívají email, jsme se zaměřili v šetření také na to, jaký typ mailového systému jednotlivé instituce používají. Z výsledků vyplynulo, že 10 institucí využívá kombinaci jak lokálního, tak cloudového systému, dalších 9 respondentů má cloudový mailový systém. Zbýlých 7 institucí pak využívá lokálního mailového systému.

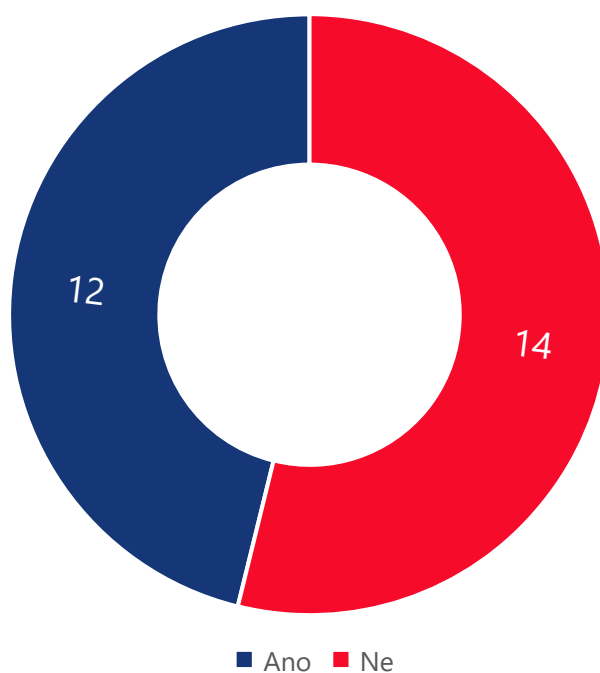
### Typy mailových systémů na jednotlivých VVŠ



Graf 16: Typy mailových systémů na jednotlivých VVŠ

Vzhledem k velké oblibě nástrojů od Google jsme se respondentů dotázali na jejich zájem o doporučení zabezpečení prostředí G Suite. Z celkového počtu 26 odpovědí se 12 z nich vyjádřilo kladně. Zbylých 14 respondentů o možná doporučení neprojevovalo zájem.

### Zájem o doporučení zabezpečení prostředí G Suite



Graf 17: Zájem VVŠ o doporučení zabezpečení prostředí G Suite



## Doporučení pro zabezpečení kolaborativní platformy

V rámci realizace výstupu č. 5 projektu SC C2 NPO byla z pozice pracovní skupiny PS2 zpracována doporučení pro zabezpečení kolaborativní platformy, včetně doporučení pro její pokročilé nasazení. Jednotlivá doporučení uvedená níže jsou tak definována jak pro komunikační platformu, Learning management systémy, tak i jejich vzájemné propojení v podobě integrační mezivrstvy.

### Komunikační platforma

Z dotazníkového šetření mezi jednotlivými VVŠ zapojenými do řešení projektu SC C2 NPO vyplynulo, že zdaleka nejvíce využívaným nástrojem v podobě komunikační platformy je cloudové prostředí MS 365 od firmy Microsoft. Toto prostředí nabízí celou řadu nástrojů a funkcí.

Z pohledu online a hybridní výuky je nejvýznamnější komponentou kolaborativní platformy aplikace MS Teams dostupná jako aplikace pro počítače (MS Windows, MacOS, Linux), mobilní zařízení (platforma iOS i Android), ale také jako webová aplikace. MS Teams umožňují ad-hoc komunikaci za pomoci chatu, audio a video hovorů mezi dvěma a více účastníky, vytváření pojmenovaných skupin účastníků pro dlouhodobější komunikaci a možnost vytváření „týmů“, neboli dlouhodobě existujících prostorů, do nichž mají přístup zavedení členové, a které kromě možností komunikace poskytují také místo pro ukládání dokumentů, spolupráci nad nimi a řadu dalších funkcí. Týmy je možné zakládat a spravovat manuálně. V případě potřeby je možné realizovat automatické zakládání ze SIS nebo LMS pomocí API nebo PowerShell skriptů. Existuje speciální typ týmů pro výuku, které je možné navíc zakládat a spravovat automaticky pomocí samostatného nástroje School Data Sync.

MS365 dále také poskytuje učitelům i studentům vlastní prostor pro ukládání výukových či jiných materiálů, poštovní schránku s kalendářem, kompletní sadu kancelářských aplikací MS Office. Za zmínku stojí také nástroj OneNote, což je digitální „blok“ vhodný například pro zápis poznámek na přednáškách. MS 365 dále také zahrnuje nástroj „MS Bookings“ vhodný například pro vystavování konzultačních hodin nebo termínů zkoušek a přihlašování na ně.

Vzhledem k množství uživatelů, kteří v rámci výuky prostředí MS365 využívají, je zabezpečení tohoto prostředí vysoce důležité. Potenciální útočníci se mohou zaměřit na tisíce až desítky tisíc uživatelů z nichž mnozí mají omezené IT znalosti a je významné riziko, že podlehnou například phishingovému útoku, odcizení dat či krádeži identity. V rámci pracovní skupiny PS2 byla proto připravena sada doporučení, jak postupovat při úvodní implementaci prostředí MS365 v organizaci, které jsou volně dostupné. Vzhledem k rozsahu materiálu a jeho průběžným aktualizacím je tento materiál umístěn online na

odkazu<sup>1</sup> - [Doporučení pro nasazení M365 – MS365Security – Confluence \(atlassian.net\)](https://servicedesk-muni.atlassian.net/wiki/spaces/MS365SEC/pages/808550432/Doporu+en+pro+nasazen+M365). Na materiál zaměřený na doporučení pro nasazení prostředí M365 navazujeme doporučeními pro další zabezpečení již nasazeného prostředí. Tato doporučení budou výstupem z další části projektu.

Dále proběhl seminář zaměřený na základní zabezpečení elektronické pošty (metody autentizace pošty – SPF, DKIM, DMARC a ARC), které napomáhají při rozlišování zpráv od legitimních a nelegitimních odesílatelů. Uvedená opatření jsou v případě systému spadajících pod ZoKB povinná, my je doporučujeme i pro poštovní systémy využívané pro výuku nespadající pod ZoKB.

## Learning Management System (LMS)

Jelikož z iniciálního dotazníku vyplývá, že nejčastěji používaným LMS v rámci českých VVŠ je Moodle, představíme zde několik doporučení pro zvýšení bezpečnosti tohoto systému a zlepšení ochrany soukromí jeho uživatel. V listopadu 2022 vyšla major verze 4.1, která je vydána v režimu long-term support<sup>2</sup>, takže bezpečnostní podpora pro tuto verzi trvá až do prosince 2025 (oproti nejnovější major verzi 4.2, která má bezpečnostní podporu pouze do října 2024). Doporučení jsou proto specifická pro verzi 4.1, ačkoli je bude možné aplikovat i na verze novější.

### Používání IdM pro běžné uživatelské účty

Preferovanou metodou pro přihlašování uživatelů do LMS Moodle je využití některé z autentizačních metod využívajících univerzitního nástroje pro správu identit (např. Shibboleth nebo OAuth 2).

### Hesla pro manuální účty

Manuálně vytvářené účty doporučujeme používat pouze v nezbytně nutných případech (např. pro systémové administrátory). V případě vytváření těchto účtů doporučujeme upravit výchozí nastavení požadavků na hesla v sekci

***Správa stránek > Obecná nastavení > Zabezpečení > Zabezpečení stránek***

*[Site administration > General > Security > Site security settings]* následovně:

---

<sup>1</sup> <https://servicedesk-muni.atlassian.net/wiki/spaces/MS365SEC/pages/808550432/Doporu+en+pro+nasazen+M365>

<sup>2</sup> <https://moodledev.io/general/releases>.

| Nastavení  | Doporučená hodnota | Komentář  |
|--|--------------------|---|
| <b>Délka hesla</b><br>[Password length]<br>minpasswordlength   | 17                 | Aktuální minimální hodnota pro administrátorské heslo podle Vyhlášky č. 82/2018 Sb., § 19, odst. 5, písm. a), bod 2.3 |
| <b>Zkontrolovat heslo při přihlášení</b><br>[Check password on login]<br>passwordpolicycheckonlogin  | Ano [Yes]          | Uživatel se slabým heslem bude po přihlášení donucen k jeho změně za heslo vyhovující.                                |
| <b>Omezení opakování hesla</b><br>[Password rotation limit]<br>passwordreuselimit  | 2 <sup>4</sup>     | Udává počet změn hesla, který musí proběhnout do doby, než je povoleno opětovné použití hesla.                        |
| <b>Odhlásit po změně hesla</b><br>[Log out after password change]<br>passwordchangelogout  | Ano [Yes]          | Zapnutím tohoto nastavení dojde k ukončení všech relací prohlížeče, vyjma té, v níž je nastaveno nové heslo.          |
| <b>Odstranit přístupové tokeny webové služby po změně hesla</b><br>[Remove web service access tokens after password change]<br>passwordchangetokendeletion | Ano [Yes]          | Po vytvoření nového hesla budou odstraněny všechny přístupové tokeny uživatele webové služby.                         |

Tabulka 3: Nastavení požadavků na hesla

## Zákaz logů pro učitele

Ve výchozím nastavení mají učitelské role v rámci kurzů (Učitel, Učitel bez práva upravovat) možnost nahlížet do protokolů činnosti. Ty obsahují kromě záznamu akcí provedených na stránce i časovou značku a IP adresy uživatelů. Protokoly tak představují riziko pro soukromí uživatelů a přístup k nim by měl být limitován.

Odebrat pravomoci pro zobrazování protokolů mohou správci stránek v nastavení

**Správa stránek > Uživatelé > Oprávnění > Definovat role**

[Site administration > Users > Permissions > Define roles].

<sup>3</sup> <https://www.zakonyprolidi.cz/cs/2018-82#p19>.

<sup>4</sup> Jelikož změna hesla je defaultně možná jednou za 30 minut, znamená to, že stejné heslo jde použít nejdříve za 1,5 hodiny, což nám přijde jako dostatečný čas pro odrazení od recyklace hesel.

Ovlivněné role:

- **Učitel** [Teacher] | *editingteacher*
- **Učitel bez práva upravovat** [Non-editing teacher] | *teacher*

U požadovaných rolí se po jejich vybrání zvolí možnost Upravit [Edit] a změní se nastavení následujících tří položek:

| Nastavení   | Doporučená hodnota                      |
|---|---|
| <b>Zobrazit protokoly kurzu</b><br>[View course logs]<br>report/log:view        | Nepovolit/zakázat<br>[Prevent/Prohibit] |
| <b>Zobrazit dnešní protokoly</b><br>[View today's logs]<br>report/log:viewtoday | Nepovolit/zakázat<br>[Prevent/Prohibit] |
| <b>Zobrazit aktuální protokoly</b><br>[View live logs]<br>report/loglive:view   | Nepovolit/zakázat<br>[Prevent/Prohibit] |

Tabulka 4: Změna nastavení pro odebrání pravomocí pro zobrazování protokolů

## Force login pro fotografie

Zatímco uživatelské profily se standardně zobrazují pouze autentizovaným uživatelům, u profilových fotografií je toto nastavení potřeba dodatečně zapnout:

| Nastavení   | Doporučená hodnota | Komentář  |
|---|--------------------|---|
| <b>Pro zobrazení uživatelských fotografií vnutit přihlášení</b><br>[Force users to log in to view user pictures]<br>forceloginforprofileimage | Ano [Yes]          | Profilové obrázky se budou zobrazovat pouze přihlášeným uživatelům. |

Tabulka 5: Force login pro fotografie

## Studijní informační systém

V rámci realizace činností pracovní skupiny PS2 projektu SC C2 NPO nebyla pro studijní informační systémy vytvářena žádná doporučení pro zabezpečení kolaborativní platformy z důvody

potenciálního výskytu uplatnění dvojího financování, jelikož tato oblast je směrem k studijním informačním systémům komplexně a systematicky zpracovávána v projektech CRP-KYBER<sup>5</sup>, v rámci Centralizovaného rozvojového programu MŠMT, z důvodu regulace těchto informačních systémů dle Zákona o kybernetické bezpečnosti<sup>6</sup> a souvisejících vyhlášek<sup>78</sup>.

---

<sup>5</sup> <https://www.crp-kyber.cz>

<sup>6</sup> <https://www.zakonyprolidi.cz/cs/2014-181>

<sup>7</sup> <https://www.zakonyprolidi.cz/cs/2018-82>

<sup>8</sup> <https://www.zakonyprolidi.cz/cs/2020-360>

## Závěr

---

Díky dotazníkovému šetření se nám podařilo získat informace o nástrojích podporujících distanční formy výuky od všech 26 zapojených VVŠ. Šetření potvrdilo některé naše iniciační představy o technologickém vybavení a jeho využívání při online a distanční výuce na VVŠ, a to jak v době pandemie COVID-19, tak i po jejím skončení. Komunikační nástroje jako MS Teams nebo Zoom byly na VVŠ využívány již před pandemií COVID-19, nicméně s jejím propuknutím došlo k výraznému nárůstu jejich využívání pro realizaci nouzové distanční výuky, a to i bez jakéhokoliv zabezpečení či pokročilého nastavení. Nejvíce používaným komunikačním nástrojem se podle našeho průzkumu ukázala platforma MS 365. Potvrdil se náš předpoklad, že prevalentním LMS je v rámci zapojených škol Moodle, což nám umožnilo konkretizovat bezpečnostní doporučení právě pro tento LMS. Dotazníkové šetření rovněž potvrdilo i zájem o zpracování tématu zabezpečení různých komponent kolaborativní platformy. Jednotlivá doporučení se tak díky podrobné analýze zaměřují na přímé požadavky a potřeby VVŠ a komplexně řeší případné nedostatky jež při zajištění distanční formy výuky mohou nastat.