MUNI
ICS

Doporučení pro užívání úložišť MUNI

Revize 1.2.0

1. března 2021

Zpracoval:

Ústav výpočetní techniky MUNI

Oddělení bezpečnosti a správy dat <BaSD@space.muni.cz>

Revize dokumentu

Revize 1.0 (5. prosince 2018)

- Interní vydání.

Revize 1.1 (11. prosince 2018)

- První veřejné vydání.

Revize 1.1.1 (14. prosince 2018)

- Upřesnění statusu Google G Suite for Education.
- Licence CC-BY.

Revize 1.2.0 (1. března 2021)

- Upřesnění statusu Microsoft O365.
- Upřesnění statusu Google G Suite for Education.
- Přidání podrobného statusu Grammarly.
- Náhrada zkratky MU na MUNI.

Licence

Obsah

1 Účel dokumentu

Cílem tohoto dokumentu je návrh klasifikace dat, se kterými přichází do styku studenti i zaměstnanci MUNI. Dokument současně poskytuje přehled nejčastějších úložišť dat, která jsou na univerzitě i mimo ni k dispozici a představuje mapování kategorií dat na jednotlivé typy úložišť z hlediska vhodnosti jejich použit. Současně uvádí základní doporučení pro bezpečné použití úložišť.

Dokument je věnován běžně zpracovávaným datům, se kterými se zaměstnanci a studenti setkávají ve výzkumu, při zajištění provozních a administrativních činností univerzity či v rámci výuky. Většina studentů i zaměstnanců univerzity se s jiným typem dat v rámci své práce nesetkává.

Dokument se pouze okrajově věnuje práci s vysoce citlivými daty (zdravotnictví apod.), případně vysoce cennými daty, kde hrozí vysoké škody při jejich zničení či úniku (výzkumná data s [potenciálně] vysokou finanční hodnotou, data vysokého strategického významu z hlediska národních a bezpečnostních zájmů státu apod.). Ve všech těchto případech je nutné postupovat individuálně a pro volbu vhodného úložiště dat zpracovat samostatnou analýzu. Data utajovaná ze zákona jsou zcela mimo rámec tohoto dokumentu a je u nich třeba postupovat podle specifických pravidel.

2 Bezpečnost uložených dat

Při práci s daty řešíme dva základní problémy s jejich bezpečností: ochranu dat před vyzrazením neoprávněné osobě a ochranu dat před neoprávněnou modifikací a ztrátou.

2.1 Ochrana dat před vyzrazením neoprávněné osobě

Chráníme se zde před „krádeží dat hackery“, zkopírovaní dat náhodným nálezcem flash disku, zneužitím dat zlodějem notebooku apod.

Ochranou je v první řadě volba odpovídajícího úložiště pro daný typ dat, dále používání přihlašovacích hesel pro přístup k datům v zařízeních, omezení přístupu k souborům pomocí přístupových práv, ochrana dat šifrováním apod.

2.2 Ochrana dat před modifikací či ztrátou

Bráníme se zde ztrátě dat z důvodu nechtěného smazání / změně obsahu souboru (neoprávněným) uživatelem, selhání úložiště s daty v zařízení, vyděračskému zašifrování/smazání dat počítačovým virem apod.

Opět je důležitá volba vhodného úložiště, respektive úložišť, která sama o sobě mohou obsahovat mechanismy chránící před ztrátou dat. Obecnými metodami ochrany jsou zálohování dat (uložení více kopií stejných souborů na různá, na sobě nezávislá, úložiště) a dlouhodobé držení jejich historických kopií, mazání „do koše“, používání pokročilých úložišť s integrovanou ochranou dat (např. uložení v cloudu, uložení na profesionálních datových serverech používajících redundantní uložení) apod.

3 Kategorizace dat

KATEGORIE DAT	POPIS	PŘÍKLADY
ZELENÁ: VEŘEJNÁ DATA	• Data zpřístupnitelná komukoliv bez jakýchkoliv omezení, např. veřejně vystavena na internetu. • Jejich zveřejnění nepředstavuje žádné ohrožení pro MUNI nebo jiné instituce či osoby.	• Prezentace z veřejných přednášek; • veřejně přístupné výzkumné zprávy; • open-source software; • veřejná výzkumná data; • propagace, veřejné informace o službách; …
MODRÁ: INTERNÍ DATA	• Data určená jen pro vnitřní potřebu obecně definované skupiny osob (např. spolupracovníci projektu, pracovníci instituce apod.). • Nevyžadují však zvláštní regulaci nebo ochranu (ze zákona, dle smlouvy apod.). • Zpřístupnění mimo danou skupinu nezpůsobí přímou škodu (finanční, morální, právní apod.).	• Interní korespondence; • zápisy z jednání; • vnitřní regulace a předpisy; • vnitřní plány práce, poznámky apod.; • nedokončené/nepublikované výzkumné zprávy; …
ORANŽOVÁ: DISKRÉTNÍ DATA	• Data určená výhradně pro vnitřní potřebu přesně definované skupiny osob (např. zaměstnanec a jeho přímý nadřízený, pracovník HR oddělení a uchazeč o zaměstnání, skupina správců IT systému s administrátorskými právy k němu). • Vyžadují ze své povahy regulaci nebo ochranu, typicky jsou data chráněná ze zákona nebo na základě nějaké smlouvy/licence (jedná se např. o osobní údaje osob, data spadající pod obchodní tajemství apod.). • Zpřístupnění mimo danou skupinu osob velmi pravděpodobně způsobí škodu (finanční, morální, právní apod.).	• Ekonomické a personální údaje osobní povahy; • osobní údaje studentů/zaměstnanců/spolupracovníků/…; • čísla identifikačních průkazů, rodná čísla apod.; • čísla kreditních karet; • cenná výzkumná data (poskytující např. konkurenční výhodu) nebo data obsahující jinak citlivé informace; • rozsáhlé kolekce interních dat; • přístupové údaje (např. hesla či šifrovací klíče) k málo významným systémům a interním datům; …
ČERVENÁ: CITLIVÁ DATA	• Data určená striktně jen pro vnitřní potřebu přesně definované skupiny osob (např. zdravotník a jeho pacient, řešitelé projektu pracující s daty podléhajícími komerčnímu či podobnému tajemství apod.). • Vyžadují ze své povahy zvláštní regulaci nebo obzvláštní ochranu, typicky jsou data přísně chráněná ze zákona nebo na základě smlouvy/licence (jedná se např. o velmi cenná data spadající pod obchodní tajemství, citlivé osobní údaje apod.). • Zpřístupnění mimo danou skupinu oprávněných osob velmi pravděpodobně způsobí škodu (finanční, morální, právní apod.) velkého rozsahu se závažnými/nevratnými následky. • *V univerzitní praxi do této kategorie spadá jen velmi málo dat a uživatelé jsou si vysoké citlivosti zpravidla explicitně vědomi.*	• Zdravotní data, citlivé osobní údaje; • velmi cenná výzkumná data (poskytující např. unikátní a těžko opakovatelnou konkurenční výhodu) nebo výzkumná data obsahující vysoce důvěrné údaje; • rozsáhlé kolekce diskrétních dat; • přístupové údaje (např. hesla či šifrovací klíče) k důležitým systémům a datům kategorie diskrétní nebo citlivá; …

4 Kategorizace úložišť

TYP ÚLOŽIŠTĚ	POPIS
PŘENOSNÁ MÉDIA	Např. flash disky, paměťové karty, externí HDD/SSD, CD, DVD, … Tj. externí paměťová média, která nejsou pevnou součástí žádného zařízení a uživatelé je používají k přenášení informací mezi zařízeními nebo pro off-line uložení dat.
LOKÁLNÍ ÚLOŽIŠTĚ	
V POČÍTAČÍCH	Datová úložiště pevně zabudovaná ve stolních počítačích/noteboocích (typicky interní HDD/SSD apod.) v kancelářích zaměstnanců, ve studovnách apod.
V MOBILNÍCH ZAŘÍZENÍCH	Datová úložiště pevně zabudovaná v mobilních zařízeních, tj. mobilních telefonech, tabletech apod. (typicky interní nevyjímatelná paměť, v zařízení instalovaná paměťová karta apod.) v použití zaměstnanců/studentů.
SÍŤOVÁ A CLOUDOVÁ ÚLOŽIŠTĚ ÚVT	Datová úložiště provozovaná ÚVT a zpřístupněná koncovým uživatelům přes datovou síť – tzv. standardní a střední síťové úložiště. Do této kategorie spadají také datová úložiště CERIT-SC pro velkoobjemová výzkumná data.
ÚLOŽIŠTĚ IS MUNI	Dokumentový server, Úschovna a podobné úložné kapacity integrované v systému IS MUNI.
ÚLOŽIŠTĚ CESNET	Datová úložiště provozována Oddělením datových úložišť sdružení CESNET. Do této kategorie spadají i služby, které tato úložiště využívají pro fyzické uložení dat, např. CESNET OwnCloud, CESNET FileSender apod.
EXTERNÍ ÚLOŽIŠTĚ	Datová úložiště provozovaná externími subjekty, tj. mimo MUNI a CESNET.
SE SMLOUVOU S MUNI	
MUNI MICROSOFT O365	Cloudová datová úložiště poskytovaná v rámci služby Microsoft Office 365 pro Masarykovu univerzitu. Zejména se jedná o osobní úložiště OneDrive a dokumentové knihovny služby SharePoint a Skupin O365. Patří sem ale také další data uložená v MUNI O365 cloudu, jako např. elektronická pošta v MUNI O365 Outlook, soubory sdílené v sociální síti MUNI Yammer apod.
MUNI GOOGLE G SUITE FOR EDUCATION	Cloudová datová úložiště poskytovaná v rámci služby Google G Suite for Education pro Masarykovu univerzitu. Zejména se jedná o datové kapacity MUNI Google Drive, patří sem ale i další data uložená v MUNI G Suite for Education cloudu, např. elektronická pošta v MUNI Google Mail, poznámky v MUNI Google Keep, kalendářová data v MUNI Google Calendar apod.
BEZ SMLOUVY S MUNI	
VEŘEJNÁ GOOGLE/MICROSOFT/DROPBOX/… ÚLOŽIŠTĚ	Do této kategorie spadají zejména veřejné cloudové služby (zřízené typicky zdarma soukromým koncovým uživatelem jen proti elektronické registraci přes web) jako Google Drive, Microsoft OneDrive, Dropbox, Amazon úložiště, repositáře na GitHub apod. Zásadním rozdílem a „poznávacím znamením“ této kategorie cloudových úložišť oproti cloudovým službám uvedeným výše je, že MUNI nemá žádný (právní) vztah s provozovateli těchto externích služeb, a proto není schopna garantovat jakékoliv záruky ohledně bezpečnosti/důvěrnosti uložených dat nebo politiky nakládání s nimi.

5 Doporučení pro použití datových úložišť na MUNI

5.1 Souhrnné přehledové schéma

TYP ÚLOŽIŠTĚ	POUŽITÍ			
	ZELENÁ: VEŘEJNÁ DATA	MODRÁ: INTERNÍ DATA	ORANŽOVÁ: DISKRÉTNÍ DATA	ČERVENÁ: CITLIVÁ DATA
PŘENOSNÁ MÉDIA (FLASH DISKY, EXTERNÍ HDD, CD, DVD, …)	Vhodné	Možné doporučeno použití šifrování	Nevhodné možné při použití šifrování	Nevhodné
LOKÁLNÍ ÚLOŽIŠTĚ				
V POČÍTAČÍCH (STOLNÍ, NOTEBOOKY)	Vhodné	Vhodné	Vhodné doporučeno použití šifrování	Nevhodné možné v dobře odůvodněných případech, při provedení individuální analýzy, použití šifrování a aplikaci dalších bezpečnostních opatření, která z analýzy vyplynou
V MOBILNÍCH ZAŘÍZENÍCH (MOBILNÍ TELEFONY, TABLETY, …)	Vhodné	Vhodné nutný zámek obrazovky (vzor, čtečka otisků prstů, PIN, heslo)	Možné nutné použití šifrování nutný silný zámek obrazovky (čtečka otisků prstů, PIN, heslo)	Nevhodné možné v dobře odůvodněných případech, při provedení individuální analýzy, použití šifrování a aplikaci dalších bezpečnostních opatření, která z analýzy vyplynou
SÍŤOVÁ A CLOUDOVÁ ÚLOŽIŠTĚ ÚVT (TZV. STANDARDNÍ A STŘEDNÍ SÍŤOVÉ ÚLOŽITĚ, VIZ KATALOG IT, ÚLOŽIŠTĚ CERIT-SC)	Vhodné	Vhodné	Vhodné	Vhodné, doporučeno provedení individuální analýzy, použití šifrování a aplikaci dalších bezpečnostních opatření, která z analýzy vyplynou

TYP ÚLOŽIŠTĚ	POUŽITÍ			
	ZELENÁ: VEŘEJNÁ DATA	MODRÁ: INTERNÍ DATA	ORANŽOVÁ: DISKRÉTNÍ DATA	ČERVENÁ: CITLIVÁ DATA
ÚLOŽIŠTĚ IS MUNI (NAPŘ. DOKUMENTOVÝ SERVER, ÚSCHOVNA APOD.)	Vhodné	Vhodné	Vhodné	Vhodné, doporučeno provedení individuální analýzy, použití šifrování a aplikaci dalších bezpečnostních opatření, která z analýzy vyplynou
ÚLOŽIŠTĚ CESNET (NAPŘ. CESNET ARCHIVNÍ ÚLOŽIŠTĚ, OWNCLOUD, FILESENDER, …, VIZ ODDĚLENÍ DATOVÝCH ÚLOŽIŠŤ CESNET)	Vhodné	Vhodné	Vhodné	Vhodné, doporučeno provedení individuální analýzy, použití šifrování a aplikaci dalších bezpečnostních opatření, která z analýzy vyplynou
EXTERNÍ ÚLOŽIŠTĚ				
SE SMLOUVOU S MUNI				
MUNI MICROSOFT O365 (MUNI O365 ONEDRIVE, SHAREPOINT, …, VIZ MUNI O365)	Vhodné	Vhodné	Vhodné doporučeno použití šifrování	Možné výhradně s adekvátním procesním pokrytí dané situace na základě individuální analýzy a aplikaci bezpečnostních opatření, která z analýzy vyplynou
MUNI GOOGLE G SUITE FOR EDUCATION (VIZ MUNI GOOGLE APPS)	Vhodné	Vhodné	Nevhodné možné při použití šifrování	Nevhodné
GRAMMARLY	Vhodné	Vhodné	Nevhodné	Nevhodné
BEZ SMLOUVY S MUNI				
VEŘEJNÁ GOOGLE/MICROSOFT/DROPBOX/… ÚLOŽIŠTĚ	Vhodné	Nevhodné	Nevhodné	Nevhodné

5.2 Přenosná média

Co zde ukládat
Veřejná data, interní data.

V případě interních dat je doporučeno použití šifrování.

Tato úložiště jsou vhodná pro data, která je nutné přenést do počítače s omezeným nebo žádným připojením k internetu nebo interní datové síti, případně se jedná o „cizí“ počítač, na kterém se uživatel z bezpečnostních důvodů nechce přihlašovat svým heslem ke svým účtům. Používány mohou být také pro (off-line) uložení záložních kopií dat primárně uložených jinde.

Co zde neukládat
Citlivá data.

Ukládání diskrétních dat není doporučeno, možné je při použití šifrování.

Proč (ne)používat právě takto
Přenosná média jsou typicky přenášena z místa na místo. Snadno mohou být ponechána bez dozoru / ztracena na veřejných místech, kde hrozí jejich krádež a následné zneužití/zveřejnění uložených dat. U těchto médií je také velmi obtížné zjistit, zda nedošlo k neautorizovanému přístupu k datům (např. kolega si z flash disku zkopíruje nejen prezentaci z konference, kvůli které jsme mu flash disk půjčili, ale také ostatní soubory, které jsou na disku uložené).

Tato média také z praktických a ekonomických důvodů neobsahují prakticky žádné ochranné mechanismy proti ztrátě dat (vícenásobné uložení, automatické kontroly uložených dat apod.), takže z důvodu selhání média mohou být data na nich uložená snadno bez varování ztracena. Ke ztrátě dat může snadno dojít také prostou ztrátou/krádeží zařízení samotného. Tato média proto nejsou vhodná jako jediné primární úložiště dat, ale jen pro uložení druhé nebo další kopie.

Poznámka: Přenosná média jsou velmi vhodná pro uložení druhé nebo třetí kopie dat jako off-line zálohy. V kombinaci s odpovídajícím fyzickým (uložení v uzamčené skříni, trezoru apod.) / logickým (šifrování dat apod.) zabezpečením mohou být po odpovídající analýze případně používána i pro zálohování citlivých dat.

5.3 Lokální úložiště

Je důležité pamatovat na to, že na lokální úložiště zařízení se skrze používané aplikace často ukládají/synchronizují (automaticky a/nebo dočasně) také data primárně uložená v síťovém / cloudovém úložišti – pokud tedy na zařízení pracujete s daty ze sítě/cloudu, je třeba zabezpečení zařízení přizpůsobil kategorii těchto dat, i když jsou jinak data primárně uložena mimo zařízení na síťovém úložišti / v cloudu (např. Google Drive, Microsoft OneDrive, OwnCloud, pošta, kalendáře, …).

5.3.1 V počítačích

Co zde ukládat
Veřejná data, interní data, diskrétní data.

V případě diskrétních dat je vhodné použití šifrování.

Tato úložiště jsou vhodná pro data, ke kterým je nutný rychlý lokální přístup přímo na daném počítači a není nutné je sdílet s jinými osobami nebo je zpracovávat na více různých zařízeních.

Co zde neukládat
Citlivá data. Jejich uložení je možné jen ve speciálních odůvodněných případech po provedení individuální analýzy konkrétního případu a zavedení odpovídajících opatření, která budou typicky obsahovat použití šifrování dat, zvláštní režim zabezpečení počítače (omezení fyzického a síťového přístupu, zvláštní režim instalace a konfigurace používaného software apod.).

Proč (ne)používat právě takto
Lokální úložiště v počítačích typicky neobsahují prakticky žádné ochranné mechanismy proti ztrátě dat (vícenásobné uložení, automatické kontroly uložených dat apod.), takže z důvodu selhání úložiště mohou být data na nich uložená snadno bez varování ztracena. Lokálně uložená data, která potřebujeme dlouhodobě zachovat, je proto nutné chránit před ztrátou zálohováním (např. na přenosné médium, na síťové úložiště, do cloudu apod.).

Aby se zabránilo neautorizovanému přístupu k datům, je třeba důsledně dbát na omezení přístupu k uživatelskému/administrátorskému účtu (přihlašovací hesla apod.), na správné nastavení přístupových práv k datům na úložišti a dodržovat zásady fyzické bezpečnosti, zejména nenechávat bez dozoru běžící počítač bez „uzamčení obrazovky“ (kde je to možné, zamykat kancelář v nepřítomnosti uživatele počítače) apod.

Obzvláštní pozornost je třeba věnovat přenosným počítačům – typicky jsou přenášené z místa na místo. Snadno mohou být ponechány bez dozoru / ztraceny na veřejných místech, čímž hrozí zvýšené riziko jejich krádeže a následné ztráty/zneužití uložených dat. Z hlediska ztráty dat je u přenosných počítačů riziko o to vyšší, že notebooky jsou při transportu a používání na cestách vystaveny vyšší zátěži (vibrace, prach, nárazy, velké změny teplot, …), což zvyšuje pravděpodobnost selhání interního úložiště dat. Přesto v principu pro interní úložiště pro notebooku platí stejná pravidla jako pro úložiště ve stolních (desktop) počítačích.

5.3.2 V mobilních zařízeních

Co zde ukládat
Veřejná data, interní data, diskrétní data.

V případě uložení interních dat je nutno používat na zařízení zámek obrazovky, tj. ochranu přístupu k funkcím zařízení „vzorem“, PINem, heslem či otiskem prstu, který zabrání tomu, aby mohl se zařízením a daty v něm volně pracovat každý, kdo se k zařízení náhodně dostane.

V případě uložení diskrétních dat je nutné používat silný zámek obrazovky – tj. nestačí již použití vzoru, ale je třeba použití silného PINu či hesla, respektive čtečky otisků prstů.[1]

V případě diskrétních dat je také nutné použití šifrování. Mobilní zařízení je také typicky možné nakonfigurovat tak, aby jej bylo možné na žádost jeho oprávněného uživatele vzdáleně uzamknout/vymazat, pokud je ztraceno/odcizeno.

Co zde neukládat
Citlivá data. Jejich uložení je možné jen ve výjimečných odůvodněných případech po provedení individuální analýzy konkrétního případu a zavedení odpovídajících opatření, která budou typicky obsahovat použití šifrování dat, použití specifického modelu mobilního zařízení se specifickým software, konfigurací, zabezpečením a režimem používání.

[1] Otisk prstu je zpravidla méně bezpečný než použití silného PINu či hesla, ale má mnohem menší negativní vliv na pohodlí používání zařízení.

Proč (ne)používat právě takto

Mobilní zařízení, jako např. chytrý mobilní telefon, jsou uživateli často využívány jako společné zařízení pro pracovní i osobní účely. Je třeba proto dbát zvýšené opatrnosti, aby „pracovní“ data nebyla omylem uložena na osobní cloudové úložiště. Zvýšenou pozornost je nutné věnovat také instalaci aplikací – krom instalace výhradně z oficiální zdrojů aplikací (Google Play, Apple App Store apod.), čímž se pomáhá předcházet instalaci podvodné nebo „zavirované“ aplikace, je třeba věnovat zvýšenou pozornost oprávnění aplikací – nesmyslně rozsáhlé požadavky na přístupová práva aplikace mohou ukazovat na škodlivou aplikaci. I legitimní aplikace, např. počítačová hra instalovaná pro osobní zábavu, pak může získat přístup k „pracovním“ datům, čemuž by se mělo také předcházet.

Velkým problémem bezpečnosti mobilních zařízení je péče o jejich zabezpečení ze strany jejich výrobců. Pokud výrobce neposkytuje včasné softwarové opravy bezpečnostních problémů operačního systému apod., nemusí být koncový uživatel přes veškerou svou snahu schopen dané zařízení dostatečně zabezpečit. Tímto problém nejvíce trpí ekosystém kolem systému Google Android, jenž v různé míře modifikace používá pod vlastní značnou velké množství různých výrobců a zejména méně známé značky a levnější modely často bývají ponechány bez patřičné softwarové podpory. S výběrem Android zařízení s vyšší úrovní bezpečnosti může pomoci doporučení na stránce Android Enterprise Recommended.

Aby se předešlo ztrátě dat při ztrátě/krádeži/poruše zařízení, je vhodné maximum dat ze zařízení synchronizovat do cloudu nebo na síťová úložiště, což bývá typická situace u soudobých mobilních zařízení.

5.4 Síťová a cloudová úložiště ÚVT

Co zde ukládat

Veřejná data, interní data, diskrétní data, citlivá data.

V případě ukládání citlivých dat je nutné provedení individuální analýzy konkrétního případu a zavedení odpovídajících opatření, která mohou obsahovat použití šifrování dat a další požadavky na způsob práce s daty.

Úložiště jsou obzvláště vhodná pro data, která je nutné sdílet s jinými osobami nebo je zpracovávat na více různých zařízeních.

Co zde neukládat

Citlivá data bez provedení patřičné analýzy a zavedení potřebných opatření.

Proč (ne)používat právě takto

Uložení dat v datacentrech na zálohovaných serverech poskytuje zvýšenou ochranu dat proti jejich poškození nebo ztrátě, zálohování dat probíhá automaticky péčí správce úložiště, přesná politika zálohování je k dispozici v popisu parametrů úložiště. Centrální serverové uložení dat umožňuje lepší sledování přístupu k datům a zlepšuje tak možnosti zjištění neautorizovaného přístupu.

Aby se zabránilo neautorizovanému přístupu k datům, je třeba důsledně dbát na správné nastavení přístupových práv k datům na úložišti.

5.5 Úložiště IS MUNI

Co zde ukládat

Veřejná data, interní data, diskrétní data, citlivá data.

Úložiště jsou úzce integrovaná s funkcemi IS MUNI, jsou tedy velmi vhodná zejména pro data náležející do tohoto systému. V případě ukládání citlivých dat je nutné provedení

individuální analýzy konkrétního případu a zavedení odpovídajících opatření, která budou typicky obsahovat použití šifrování dat a další požadavky na způsob práce s daty. IS MUNI je primárně určen pro ukládání studijních údajů a souvisejících dat, nikoliv pro ukládání citlivých uživatelských pracovních/výzkumných dat.

Součástí IS MUNI je rovněž Úřadovna a dokumentový server, kam lze ukládat všechny dokumenty související s provozem univerzity.

Co zde neukládat
Citlivá data bez provedení patřičné analýzy a zavedení potřebných opatření.

Proč (ne)používat právě takto
Uložení dat v na zálohovaných serverech IS MUNI poskytuje zvýšenou ochranu dat proti jejich poškození nebo ztrátě. Centrální serverové uložení dat umožňuje lepší sledování přístupu k datům a zlepšuje tak možnosti zjištění neautorizovaného přístupu.

Aby se zabránilo neautorizovanému přístupu k datům, je třeba důsledně dbát na správné nastavení přístupových práv k datům na úložišti.

5.6 Úložiště CESNET

Co zde ukládat
Veřejná data, interní data, diskrétní data, citlivá data.

V případě ukládání citlivých dat je nutné provedení individuální analýzy konkrétního případu a zavedení odpovídajících opatření, která mohou obsahovat použití šifrování dat a další požadavky na způsob práce s daty.

Obecně jsou tato úložiště obzvláště vhodná pro dlouhodobější uložení / sdílení velkého množství dat s možností geografické distribuce fyzického uložení v rámci ČR a vytvářením vícenásobných geograficky distribuovaných kopií (záloh).

Co zde neukládat
Citlivá data bez provedení patřičné analýzy a zavedení potřebných opatření.

Proč (ne)používat právě takto
Použití CESNET úložišť se řídí *Pravidly využití služeb datových úložišť CESNET*. Úložiště jsou provozována českou organizací, která je spoluvlastněná akademickými institucemi v ČR a MUNI je členem jejího statutárního orgánu. CESNET je držitelem certifikace ISO 27001, provozovatel úložiště vynakládá veškeré možné úsilí, aby data ochránil před ztrátou nebo zpřístupnění nepovolaným osobám, individuálně je možné dohodnout nákup *Service Level Agreement*, kdy jsou poskytovány vyšší záruky na zabezpečení a dostupnost dat.

5.7 Externí úložiště

5.7.1 Se smlouvou s MUNI

5.7.1.1 MUNI Microsoft O365

Co zde ukládat
Veřejná data, interní data, diskrétní data, citlivá data.

V případě diskrétních dat je vhodné použití šifrování. Ukládání citlivých dat (zvláštních kategorií osobních údajů, zejm. medicínských dat) je možné výhradně s adekvátním procesním pokrytí dané situace na základě individuální analýzy a aplikaci bezpečnostních opatření, která z analýzy vyplynou.

Úložiště je obzvláště vhodné pro ukládání dat, která je nutno sdílet s více osobami, respektive pro zálohování/synchronizaci dat z osobních počítačů s Windows do cloudu.

Co zde neukládat
Citlivá data (zvláštní kategorie osobních údajů, zejm. medicínská data) bez provedení patřičné analýzy a procesního pokrytí konkrétního případu odpovídajícími opatřeními.

Proč (ne)používat právě takto
Nakládání s daty v rámci této cloudové služby je zajištěno smlouvou uzavřenou mezi Masarykovou univerzitou a společností Microsoft. Součástí smlouvy jsou i „standardní smluvní doložky" vydané Evropskou komisí a zaručující, že zpracování dat je v souladu s právem EU. Data uživatelů z EU jsou primárně uložena v datacentrech na území EU. Bezpečnostní politika Microsoftu je v souladu s ISO 27001, 27002 a 27018. Služby Office 365 splňují i požadavky GDPR.

Několikanásobné uložení v technicky pokročilých datových centrech a speciální funkce úložiště (víceúrovňové mazání „do koše", ze kterého je možné data obnovit v případě zasažení klienta malware[2] apod.) poskytuje vysokou ochranu dat proti jejich poškození nebo ztrátě. Cloudové uložení dat také umožňuje lepší sledování přístupu k datům a zlepšuje tak možnosti zjištění neautorizovaného přístupu.

5.7.1.2 MUNI Google G Suite for Education

Co zde ukládat
Veřejná data, interní data.

Úložiště je obzvláště vhodné pro ukládání dat, která je nutno sdílet a v reálném čase ve webovém prohlížeči upravovat s více osobami, respektive pro zálohování/synchronizaci dat z osobních počítačů a mobilních zařízení všech platforem.

Co zde neukládat
Citlivá data.

Ukládání diskrétních dat není doporučeno, možné je při použití šifrování.

Proč (ne)používat právě takto
V současné době je uzavřena smlouva včetně Dodatku o zpracování dat mezi MUNI a Google. Při ukládání dat není garantováno uložení na území EU.

Několikanásobné uložení v technicky pokročilých datových centrech poskytuje vysokou ochranu dat proti jejich poškození nebo ztrátě.

5.7.1.3 Grammarly

Co zde ukládat
Veřejná data, interní data.

Z principu fungování služby je třeba službě zpřístupnit data v otevřeném tvaru (bez šifrování), aby mohla proběhnout jejich obsahová analýza.

Co zde neukládat
Diskrétní data, citlivá data.

Data není možno chránit šifrováním a dochází k jejich obsahové analýze třetí stranou.

Proč (ne)používat právě takto
Služba Grammarly zpracovává data mimo EU, data nemohou být chráněna šifrováním, neboť z principu fungování služby je třeba přístup k datům pro jejich obsahovou analýzu. Dle

[2] Pozor však na to, že ani tyto funkce neposkytují absolutní ochranu: https://csirt.muni.cz/about-us/news/cloud-ransomware

dokumentace služby může docházet k předávání dat i lidským editorům. Na druhou stranu služba Grammarly deklaruje zasmluvnění svých zaměstnanců a dodavatelů v souladu s požadavky GDPR, poskytuje informace o způsobu zpracování a zabezpečení dat a zavazuje se uživatelská data používat jen pro potřeby poskytované služby – použití Grammarly pro veřejná a interní data tedy je možné.

Uživatelé by si výše uvedeného měli být vědomi při poskytování dat Grammarly a striktně kontrolovat, jaké kategorie dat do služby poskytnou. Pro optimální kontrolu je vhodné používat jen Grammarly webový editor (kdy má služba přístup jen k datům uživatelem explicitně vloženým do tohoto dedikovaného textového editoru), respektive vstupní klávesnici pro Android či iOS (kdy má služba přístup jen k textům, které uživatel vloží pomocí této softwarové klávesnice; pro jiné texty je možno používat jinou softwarovou klávesnici, která data neodesílá mimo zařízení), nikoliv rozšíření pro webový prohlížeč či MS Office, kde nemusí být zřejmé, ke kterým datům má Grammarly přístup.

5.7.1.4 Další externí služby se smlouvou s MUNI

Univerzita, resp. její součásti mají či mohou mít uzavřenu smlouvu s poskytovateli dalších externích cloudových služeb – příkladem je např. Grammarly. V takových případech je třeba udělat alespoň základní právní analýzu podmínek poskytování služby, nicméně lze očekávat, že v současné době již většina takových smluvních vztahů (zejména jsou-li uzavřeny s organizacemi působícími v prostředí EU) obsahuje i záruky ochrany dat ve smyslu zachovaného vlastnictví a požadavků GDPR. Přesto ukládání diskrétních dat by vždy mělo podléhat předchozí analýze, zejména s ohledem na kompatibilitu s požadavky GDPR. Smlouvy s mimoevropskými organizacemi by měly být právní analýze podrobeny vždy.

5.7.2 Bez smlouvy s MUNI

5.7.2.1 Ostatní cloudové služby

Tj. veřejná (a typicky bezplatná) Google/Microsoft/Dropbox/GitHub/… úložiště, služby typu Draw.io, Overleaf atd.

Co zde ukládat
Veřejná data.

Co zde neukládat
Interní data, diskrétní data, citlivá data.

Proč (ne)používat právě takto
MUNI nemá žádný vztah ani kontrolu nad těmito úložišti, není proto schopná garantovat jakékoliv záruky ohledně bezpečnosti dat a politiky nakládání s nimi. Málokterá služba je skutečně bezplatná – u služeb zdarma typicky „platíte“ službě svěřenými daty, která dáváte provozovateli služby k dispozici, často k neomezenému využití. U pracovních dat toto ve většině případů nesmíte dovolit.

Vzhledem k atraktivitě a širokému použití těchto úložišť nelze očekávat ukončení použití; je však třeba mít na vědomí potenciálně vysoké riziko zneužití dat. Veřejné cloudové a podobné služby bez explicitního smluvního ošetření by neměly být nabízeny v rámci žádných služeb MUNI a tam, kde je jejich použití vhodné nebo nezbytné, je třeba použití pro studenty a zaměstnance MUNI řádně smluvně ošetřit.

6 Šifrování dat

Šifrování dat může být efektní způsob ochrany uložených dat před jejich zpřístupněním neoprávněným osobám. Je však nutné zvážit rizika spojená se ztrátou (de)šifrovacího klíče – nástroje pro šifrování dat mohou od koncového uživatele vyžadovat, aby se vlastními silami

postaral o zálohování šifrovacích klíčů / hesel pro případ jejich ztráty, což může být proces vyžadující nadstandardní technické znalosti. **Bez dešifrovacích klíčů / hesel přitom nebude možné data jakkoliv obnovit!** Zároveň však zpřístupnění dešifrovacích klíčů / hesel (např. jejich zálohy) neautorizované osobě ohrožuje účinnost šifrování jako prostředku ochrany dat.

Z důvodu komplikovanosti správy hesel / šifrovacích klíčů, doporučujeme pro ukládání dat využívat ta úložiště, která pro danou kategorii dat šifrování nevyžadují. Pokud potřebujte pomoci se zabezpečením svých dat, obraťte se na pracovníky ÚVT MUNI na e-mailové adrese sprava-dat@ics.muni.cz.

6.1 Lokální úložiště počítačů

V operačním systému Windows je možné využít integrovaných funkcí NTFS Encrypting File, respektive BitLocker; v operačním systému Apple MacOS funkce FileVault; v operačních systémech GNU/Linux technologií dm-crypt/LUKS/EncFS apod. Případně je možné využít důvěryhodných externích multiplatformních nástrojů jako např. VeraCrypt.

6.2 Lokální úložiště mobilních zařízení

Možnosti šifrování dat na lokálním úložišti mobilních zařízení se liší dle výrobce a modelu daného zařízení. V některých případech je šifrování standardně zapnuto a není ani možné jej uživatelsky vypnout. Bezpečnost dat pak primárně závisí na síle použitého zámku obrazovky.

V jiných případech je třeba šifrování zapnout uživatelsky v nastavení daného zařízení. U velmi starých a/nebo levnějších zařízení nemusí být šifrování dostupné vůbec.

Komplikované/nemožné může být šifrování dat na externí paměťové kartě, pokud její použití zařízení podporuje.

6.3 Síťová úložiště / cloud

Je možné využít např. technologií EncFS apod. v unixových operačních systémech či použít důvěryhodných externích multiplatformních nástrojů jako např. VeraCrypt. Pro individuální šifrování jednotlivých souborů je také možné využít technologií specifických pro daný datový formát, např. integrované šifrování MS Office dokumentů (tj. ochrana heslem Word/Excel/PowerPoint dokumentů), šifrování/heslo u ZIP archivů apod. Zde je však třeba dbát zvýšené pozornosti při výběru konkrétní technologie – např. pro šifrování ZIP archivů historicky existuje několik standardů, přičemž některé z nich poskytují jen slabou ochranu dat a v dnešní době může být taková ochrana snadno překonána bez znalosti uživatelem použitého hesla.

7 Na co si dát pozor

7.1 Bezpečnost svých přihlašovacích údajů

I pokud je zabezpečení dat na síťových / cloudových úložištích na úrovni fyzických serverů / serverového software atd. na vysoké úrovni, nejslabším článkem může být koncový uživatel, respektive způsob jeho autentizace: Pokud pro přístup používáte slabé heslo / heslo sdílené s jinými službami apod., a zároveň je heslo jediným prvkem autentizace, pak může vyzrazení hesla nepovolané osobě vést ke kompromitaci zabezpečení všech dat a služeb, ke kterým má daný uživatel přístup. Přístupové údaje k pracovním datům byste nikdy neměli zadávat do cizích počítačů (v kavárně, u kamaráda apod.), u kterých nemáte žádné povědomí ani záruky o jejich zabezpečení, používejte svoje notebooky, telefony apod.

Abyste zvládli používat silná hesla unikátní pro každou službu, může být užitečné používat kvalitní správce hesel, např. KeePass.

7.2 Soukromé počítače využívané pro pracovní účely

Je nutné si uvědomit, že na domácí apod. počítače používané pro přístup k pracovním datům by měly být kladeny minimálně stejné požadavky na zabezpečení, jako na pracovní stanice. Málo kdo má doma kamerový systém a vrátnici s nepřetržitým dohledem, jako je tomu v prostorách pracovišť MUNI, proto věnujte zvýšenou pozornost fyzickému zabezpečení v době vaší nepřítomnosti (např. když jste na pracovišti), kvalitní bezpečnostní zámky a kování vstupních dveří by mělo být nutným minimem, bezpečnostní dveře dobrým vylepšením.

Nezapomínejte na své ratolesti, které nejen mohou zapomenout zamknout při odchodu z domácnosti, ale často budou domácí počítač využívat spolu s vámi – striktní oddělení uživatelských účtů na počítači pro pracovní a osobní účely a nedostupnost administrátorských oprávnění dětem na sdíleném počítači by mělo být elementárním bezpečnostním minimem, stejně jako instalace kvalitního antivirového a antimalware software a firewallu. Zabraňte instalaci her a podezřelého software na počítač, který používáte k práci. Pracovní stanice na MUNI obsahují jen vybraný software v odůvodněné konfiguraci. Na domácím počítači používaném pro pracovní účely by měla platit stejná pravidla – instalujte jen důvěryhodný software, u které jste ověřili jeho autenticitu, zamyslete se nad konfigurací software (např. antivirové programy často automaticky odesílají soubory, které se jim zdají podezřelé, svému výrobci – takto mohou být z vašeho počítače bez vašeho vědomí odeslána data, která by se do rukou třetí strany dostat neměla, zvažte vypnutí podobných funkcí u vámi využívaného software). Bezpečnost vašeho počítače je dána nejen bezpečností vašeho chování, ale také instalovaným software a jeho konfigurací.

Pamatujte, že data, která na domácím počítači nemáte, tam nemusíte chránit – ponechávejte pracovní data na síťových / cloudových úložištích MUNI a na domácí počítač stahujete jen minimum dat a jen na nezbytně nutnou dobu. Pamatujte na bezpečnost svých přihlašovacích údajů zadávaných do svého soukromého počítače – za jeho bezpečnost odpovídáte vy sami.