Kategorizace úložišť

1. Přenosná média

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 různými zařízeními nebo pro dočasné uložení dat.

Na co si dát pozor...
Přenosná média jsou typicky přenášena z místa na místo. Snadno mohou být ponechána bez dozoru či 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 úložiště 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 a bez varování ztracena. Proto nejsou vhodná jako jediné primární úložiště dat, ale jen pro uložení druhé nebo další kopie.

2. Lokální disky

a) v počítačích a notebocích

Disky pevně zabudovaná ve stolních počítačích/noteboocích (typicky interní HDD/SSD apod.)
v prostorách univerzity, v kancelářích zaměstnanců, ve studovnách apod., každé zařízení musím mít definovaného správce (administrátorský účet), zařízení musí být řádně zabezpečeno (aktualizace, antivir,…).

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. Lze je využívat také v případě omezeného nebo žádného připojení k internetu (tzv. práce off-line).

Na co si dát pozor...
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.
Tato úložiště 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 a bez varování ztracena. Lokálně uložená data, která potřebujeme dlouhodobě zachovat, je proto nutné chránit před ztrátou zálohováním (např. na přenosné médium, na síťové nebo cloudové úložiště apod.).

b) v jiných 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.

Na co si dát pozor...
Mobilní zařízení jsou uživateli často využívána jako společné zařízení pro pracovní i osobní účely. Je třeba proto dbát zvýšené opatrnosti, aby pracovní data nebyla omylem uložena na osobní cloudové úložiště.

Dle charakteru uložených 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.

Zvýšenou pozornost je třeba věnovat také instalaci podvodných nebo „zavirovaných“ aplikací. I zdánlivě neškodná aplikace, např. počítačová hra instalovaná pro osobní zábavu, může získat přístup k pracovním datům. Na potenciálně

škodlivou aplikaci mohou ukazovat například nesmyslně rozsáhlé požadavky na přístupová práva aplikace. Proto je doporučeno využívat výhradně aplikace z oficiálních zdrojů (Google Play, Apple App Store apod.).

Velkým problémem bezpečnosti mobilních zařízení je péče o jejich zabezpečení ze strany 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.
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 (viz dále).

3. Síťová a cloudová úložiště provozovaná na infrastruktuře UK

Datová úložiště v majetku UK zpřístupněná koncovým uživatelům přes počítačovou síť. Tato úložiště jsou obzvláště vhodná pro data, která je nutné sdílet s jinými osobami nebo je zpracovávat na více různých zařízeních.

Poznámka...
Zabezpečení a dostupnost uložených dat na síťových a cloudových úložištích není dána jen zvoleným technickým řešením, ale především odbornou správou a nastavením procesů ukládaní a zálohování dat..

a) úložiště typu „NAS“ (Network Attached Storage)

Uložení dat na datových úložištích připojených do LAN může v případě řádné správy splnit požadavky na zabezpečení a dostupnost vědeckých dat, je však doporučeníhodné využít mechanismy chránící před fyzickým selháním jednoho nebo více disků (RAID apod.). Třebaže NAS lze v případě kvalitní správy doporučit jako primární úložiště dat, je i zde nezbytné řešit zálohování.

Na co si dát pozor...
Tento typ méně nákladných a intuitivně spravovatelných úložišť často svádí k poloprofesionální správě přímo uživateli/vlastníky dat. Při nevhodné konfigurace bez absence zálohovacích mechanismů však může být tato varianta uložení dat poměrně riziková (např. při poruše více disků bez jejich průběžné výměny jsou data ohrožena srovnatelně jako na lokálních discích) ***. Dejte přednost profesionálním řešením ve správě IT odborníků.***

b) profesionální datová úložiště fakult a součástí (disková pole, SAN, …)

Uložení dat v serverovnách fakult a součástí prostřednictvím profesionálních úložných řešení (často redundantní disková pole, SAN) poskytuje zvýšenou ochranu dat proti jejich poškození nebo ztrátě, zálohování dat probíhá automaticky péčí správce úložiště, přesná politika zálohování bývá k dispozici v popisu parametrů úložiště. Centrální serverové uložení dat umožňuje lepší sledování přístupu k datům a zlepšuje tak možnosti zjištění neautorizovaného přístupu.

Na co si dát pozor... *Aby se zabránilo neautorizovanému přístupu k datům, je třeba důsledně dbát na správné nastavení přístupových práv k datům. Často je problémem kapacita těchto úložných prostor, neboť při nákupu nebývají dimenzována jako úložiště poskytující kapacitu pro rozsáhlá vědecká data, ale pouze na běžný provoz fakulty/součásti.*

4. Síťová a cloudová úložiště provozovaná externími subjekty mimo UK infrastrukturu

Technicky se jedná o pokročilá datová centra s několikanásobným uložením dat a speciálními funkcemi úložišť poskytující 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. S ohledem na to, že tato úložiště bývají navrhována za účelem často komerčního poskytování služeb široké skupině uživatelů, nebývá problém dohodnout pro jednotlivé vědecké projekty i nadstandardní kapacity.

a) úložiště CESNET

Datová úložiště provozována Oddělením datových úložišť sdružení CESNET mohou využívat akademičtí pracovníci, studenti a pracovníci výzkumných organizací v ČR pro vzdělávací a výzkumné účely, a to jak v režimu bez sdílení dat (tzv. VO Storage), tak v režimu tzv. virtuální organizace umožňující sdílení dat mezi uživateli v rámci federaci identit eduID.cz . Do této kategorie spadají i služby typu CESNET OwnCloud a CESNET FileSender . Použití těchto úložišť se řídí Pravidly využití služeb datových úložišť CESNET . Úložiště jsou provozována českou organizací, která je spoluvlastněná akademickými institucemi v ČR, a UK je členem jejího statutárního orgánu. Datová úložiště jsou **certifikována podle normy pro systém managementu bezpečnosti informací ČSN EN ISO/IEC 27001:2014**.,

provozovatel úložiště vynakládá veškeré možné úsilí, aby data ochránil před ztrátou nebo zpřístupnění nepovolaným osobám. **Služby je možné doporučit i k ukládání diskrétních dat** (např. v případě nutnosti zajištění vysokých záruk za zabezpečení a dostupnost dat (např. **u citlivých dat)** je možné doporučit sjednání individuálního Service Level Agreement kontraktu.

b) úložiště poskytovaná na základě centrálně uzavřených smluv s UK

Cloudová datová úložiště poskytovaná v rámci služby Microsoft Office 365 pro Univerzitu Karlovu. Zejména se jedná o osobní úložiště OneDrive a dokumentové knihovny služby SharePoint a Skupin O365. Patří sem ale také další data uložená v O365 cloudu, jako např. elektronická pošta v O365 Outlook. Nakládání s daty v rámci této cloudové služby je zajištěno smlouvou uzavřenou mezi UK 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 uložena v datacentrech na území EU (konkrétně v Holandsku a Irsku). Bezpečnostní politika Microsoftu je v souladu s ISO 27001, 27002 a 27018. Služby Office 365 splňují i požadavky GDPR.

c) úložiště poskytovaná na základě individuálních smluv s UK

Doporučeníhodnou variantou je využití standardních komerčně nabízených služeb, vždy je nutno dbát řádného smluvního zajištění kvality služeb (definice SLA parametrů) i zajištění, aby zpracovávání dat bylo plně v souladu s právem EU (plně odpovídalo požadavkům GDPR).

Na co si dát pozor...
Využití profesionálních komerčních služeb je často spojené s relativně vysokou cenou těchto služeb, při jejich sjednávání smluv se zamyslete i nad udržitelností zvoleného řešení v dlouhodobém horizontu (např. po ukončení financování projektu). Skutečně jste ověřili možnost využití služeb CESNET, z. s. p. o.?

Bezpečnostní upozornění…
Do této kategorie patří např. i cloudová datová úložiště poskytovaná v rámci služby ***Google G Suite for Education*** *na základě individuálních smluv s vybranými fakultami/součástmi UK. Zejména se jedná o datové kapacity Google Drive, patří sem ale i další data uložená v G Suite for Education cloudu, např. elektronická pošta v Google Mail, poznámky v Google Keep, kalendářová data v Google Calendar apod. Přes veškeré snahy dosud stále nedošlo ve smluvních vztazích k ujednání, jež by zaručila, že ukládání dat a jejich zpracování je v souladu s právem EU. Z tohoto důvodu služby* ***není možné bez dalších opatření doporučit k ukládání diskrétních a citlivých dat*** *.*

d) úložiště bez smlouvy s UK – síťová a cloudová úložiště pro veřejnost

Do této kategorie spadají zejména veřejné cloudové služby (zřízené typicky zdarma koncovým uživatelem jen proti elektronické registraci přes web) jako Microsoft OneDrive, Google Drive, Dropbox, Úschovna, Uložto, Amazon úložiště, repositáře na GitHub apod.

Zásadním rozdílem a „poznávacím znamením" této kategorie cloudových úložišť oproti cloudovým službám uvedeným výše je, že UK 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.

Na co si dát pozor...
Je třeba si uvědomit, že žádná z těchto služeb není skutečně bezplatná – ve skutečnosti „platíte" svěřenými daty, která dáváte provozovateli služby plně k dispozici, často k neomezenému využití. Proto je nutné mít na vědomí potenciálně vysoké riziko zneužití takto uložených dat.