

Zálohování databáze

Databáze jsou data klienta Nabyvatele uložena v paměťové struktuře Produktu Poskytovatele. Databázi je nutno zálohovat. Záloha je kopie dat v daném okamžiku pro případ nutnosti obnovení v budoucnu. Zálohování je nutno provádět pravidelně vzhledem k níže popsaným rizikům.

Nejčastějším způsobem nasazení systému SmartMEDIX je v nasazení prostředí klienta. Program přistupuje k databázi umístěné na serveru v místní nebo i vzdálené síti. Serverem může být vybraný počítač nebo dedikovaný server – počítač sestavený, nakonfigurovaný a zabezpečený pro obsluhu velkého množství požadavků.

Lze zálohovat celý server, který je možno v případě potřeby obnovit včetně všech nastavení (mailů, certifikátů, importů laboratorní výsledků apod.). Minimálním požadavkem na zálohování systému SmartMEDIX je zálohování databáze.

Prostředím pro běh systému SmartMEDIX je počítač nebo vnitřní síť počítačů s aktuálně podporovaným a aktualizovaným operačním systémem Windows společnosti Microsoft (nebo Linux pro databázový server). Komplementem operačního systému je zajištění zabezpečení systémové ochrany vhodným prostředkem, zjednodušeně antivirem s ochranou proti ransomware.

Rizika

Mezi rizika s potenciálem ztráty databáze patří:

- a) Napadení počítačovým virem nebo vyděračským ransomware programem;
- b) Přírodní katastrofa nebo živelní událost;
- c) Vykradení objektu;
- d) Technická závada vedoucí k pádu systému a ztrátě dat;
- e) Chyba databázového stroje vedoucí ke korupci dat;
- f) Lidská chyba např. nezáměrný výmaz dat;
- g) Další rizika.

Základní doporučení pro zálohování databáze

- 1) Zálohujte pravidelně, optimálně denně, nejpozději jednou týdně.
V kritickém provozu je nutno zvážit zálohu i vícekrát za den nebo průběžnou zálohu za chodu;
- 2) Zálohujte více způsoby do několika cílových umístění, např. jedna záloha on-line v cloudu a záloha či zálohy off-line na externím médiu;
- 3) Udržujte minimálně jednu zálohu off-line, tj. odpojenou od sítě a počítače;
- 4) Pro externí zálohy používejte více cílových médií – tj. minimálně dva rotované externí disky;
- 5) Testujte obnovitelnost záloh pravidelně, aby se zajistilo, že proces obnovy funguje správně a data jsou kompletní;
- 6) Simulujte scénáře pro případ obnovení systému po útoku nebo havárii.

Souhrn výše uvedeného: zálohy provádějte minimálně ve smyslu **strategie 3–2–1**, což znamená, že si vždy uděláte minimálně tři kopie svých dat, z nichž dvě budou místní, ale na rozdílných zařízeních, a minimálně jedna kopie bude umístěna geograficky odděleně.

Vytvoření zálohy databáze

Databáze představuje strukturovaný soubor. SmartMEDIX podporuje databázové stroje Firebird a Microsoft SQL Server. SmartMEDIX má vždy hlavní databázi. Volitelně existuje možnost ukládat vybrané datové objekty jako obrázky a PDF v separátní databázi – repozitóri a zmenšit tak velikost hlavní databáze obsahující základní strukturovaná data. Je potřeba zajistit zálohování všech používaných databází.

Databázový soubor nelze přímo kopírovat. Pro zálohování dat slouží záloha – soubor se snímkem databáze v čase zálohy. Zálohu lze vytvořit buď ze systému SmartMEDIX programem SmartBackup, nebo specializovaným programem či naplánovanou úlohou systému Windows.

Rozšířená doporučení

- 1) Optimálně zajistěte, aby byl zálohován celý kritický systém včetně související infrastruktury. Udržujte zálohy softwarových licencí, certifikátů, přístupových klíčů a dalších kritických dokumentů.
- 2) Zvažte využití externích specializovaných služeb technické podpory pro vaši výpočetní infrastrukturu, která bude zajišťovat a starat se o pravidelné zálohy kritických systémů v souladu s aktuálními bezpečnostními doporučeními.
- 3) Používejte ověřené zálohovací systémy s možností obnovy na rozdílný hardware jako např.:
 - <https://www.acronis.com/>
 - <https://www.veeam.com/>
 - <https://www.macrium.com/>
 - <https://www.easeus.com/>
 - <https://www.aomeitech.com/>

Replikace

Replikace databáze zajišťuje redundanci dat na více uzlech a určitým způsobem tak vytváří on-line zálohu. V každém případě je nutné vyvářet místní zálohu aspoň základního uzlu v duchu strategie 3–2–1.

Závěr

Data jsou vždy v určitém ohrožení. Všechny platformy mají své incidenty s úniky či ztrátami dat a neexistuje univerzálně nenapadnutelný systém. Vyděrači mají velmi propracované strategie sledování chodu napadené firmy či platformy a následného útoku. Otázka zabezpečení systému a zálohování vyžaduje náležitou pozornost.

Funkční záloha = funkční zdravotnické zařízení či firma i v případě nechtěného incidentu.