

## Jak ochránit data v programu Stravné 5

### Uložení dat v programu Stravné 5

Program nepotřebuje mít fyzicky přístupné soubory s daty na disku, k datům přistupuje vždy přes SQL server. Toto platí jak na lokálním počítači, tak při práci na počítačové síti.

Uvnitř SQL serveru jsou data uložena v samostatné databázi. Pro přístup k datům je nutné mít přístup k SQL serveru a povolení pro danou databázi.

V rámci databáze data nejsou šifrována. Zašifrovaná jsou pouze klíčová data, jako jsou hesla.

### Ochrana přímo v programu Stravné 5

V programu Stravné 5 se při spuštění zadává jméno a heslo, které slouží jak pro přístup do programu, tak i pro přístup k datům na SQL serveru. Přihlašování do programu lze nastavit tak, že se přebírá přihlášení z Windows - pak je potřeba chránit přístup do Windows, protože po přihlášení do Windows je již program přístupný bez dalšího přihlášení.

Je třeba si uvědomit, že popsaná ochrana funguje pouze pro spuštění programu Stravné 5. Při znalosti jména a hesla pro SQL server je možné se dostat na data i mimo program VIS.

### Ochrana na počítači

Toto je základní způsob ochrany dat programu Stravné 5.

Ochrana může být:

- fyzická: zabránit fyzickému přístupu k počítači (zamknutí kanceláře apod.)
- ve Windows: nastavit přihlašování a přístupová práva ve Windows tak, aby k programu VIS a k souborům SQL serveru měli přístup jen oprávnění uživatelé

### Ochrana na počítačové síti

Na počítačové síti jsou data uložena na serveru. Ochrana pak spočívá v ochraně tohoto serveru (jako klasického počítače v předchozí kapitole) a v ochraně při přístupu na server přes síť, která se realizuje nastavením přístupových práv. Data SQL serveru nesmí být přes síť přímo přístupná a i samotný SQL server by měl být maximálně chráněn před přístupem po síti.

Speciální případ tvoří přístup na SQL server po internetu. SQL server by neměl být nikdy přímo přístupný přes internet - k přístupu je potřeba používat VPN (virtuální privátní síť), která přidává další stupeň ochrany.

### Ochrana zálohy dat

Záloha dat obsahuje data z programu VIS pro případ ztráty nebo poškození dat v programu. Data jsou v záloze čitelná, proto je nutné zálohu dat chránit stejně jako data v programu:

- zálohy vytvářené na lokálním počítači chránit pomocí ochrany počítače
- zálohy vytvářené na počítačové síti chránit pomocí ochrany počítačové sítě
- zálohy vytvářené na externí disky a na flashdisky chránit fyzicky - chránit tyto disky před odcizením