BM Software, Němčičky 84, 69107 Němčičky u Břeclavi
Vývoj, výroba, prodej a montáž docházkových a identifikačních systémů

Tel: 519 430 765, Mobil: 608 447 546
e-mail: bmsoft@seznam.cz
web: http://www.dochazka.eu

Databáze Docházky 3000 na šifrovaném disku *(pro MySQL)*

Úvodní informace:

Tento návod pomáhá zohlednit požadavky obecného nařízení o ochranně osobních údajů fyzických osob (dále jen GDPR) a také směrnice NIS2 v docházkovém systému Docházka 3000. Řešení navržené v tomto návodu využívá možnost vytvoření šifrovaného disku pomocí nástroje BitLocker, který je standardní součástí vyšších verzí operačního systému Windows.

Pokud vaše verze operačního systému nástroj BitLocker neobsahuje, musíte šifrovaný disk vytvořit jinými prostředky (viz jiné návody na internetu) a pak úvodní body tohoto návodu provedete vlastním postupem (k tomuto návodu se vrátíte až v bodě *Instalace docházky)*. Je také možné využít již existující šifrované disky síťového úložiště (NAS, SAN) a pak místo tohoto návodu použijte návod dostupní na instalačním či aktualizačním CD docházky ve složce *Prirucky* v PDF souboru *Databáze v NAS*.

Tento návod předpokládá vytvoření šifrovaného disku z jiného oddílu primárního disku, nebo druhého fyzického disku zapojeného do hlavního PC docházky (docházkového serveru). A to buď rotačního nebo SSD. Nedoporučuje se klasický USB flash disk (fleška) z důvodu nízké životnosti a vyšší náchylnosti k odpojení, mechanickému poškození či dokonce zcizení. Tento návod kvůli zjednodušení nepopisuje tvorbu šifrovaného disku z primárního systémového oddílu (disku C:), i když tato metoda je také možná (viz návody na webu), může být upřednostněna z důvodu posílení zabezpečení dalších částí systému a zkušeným správcům jí lze doporučit.

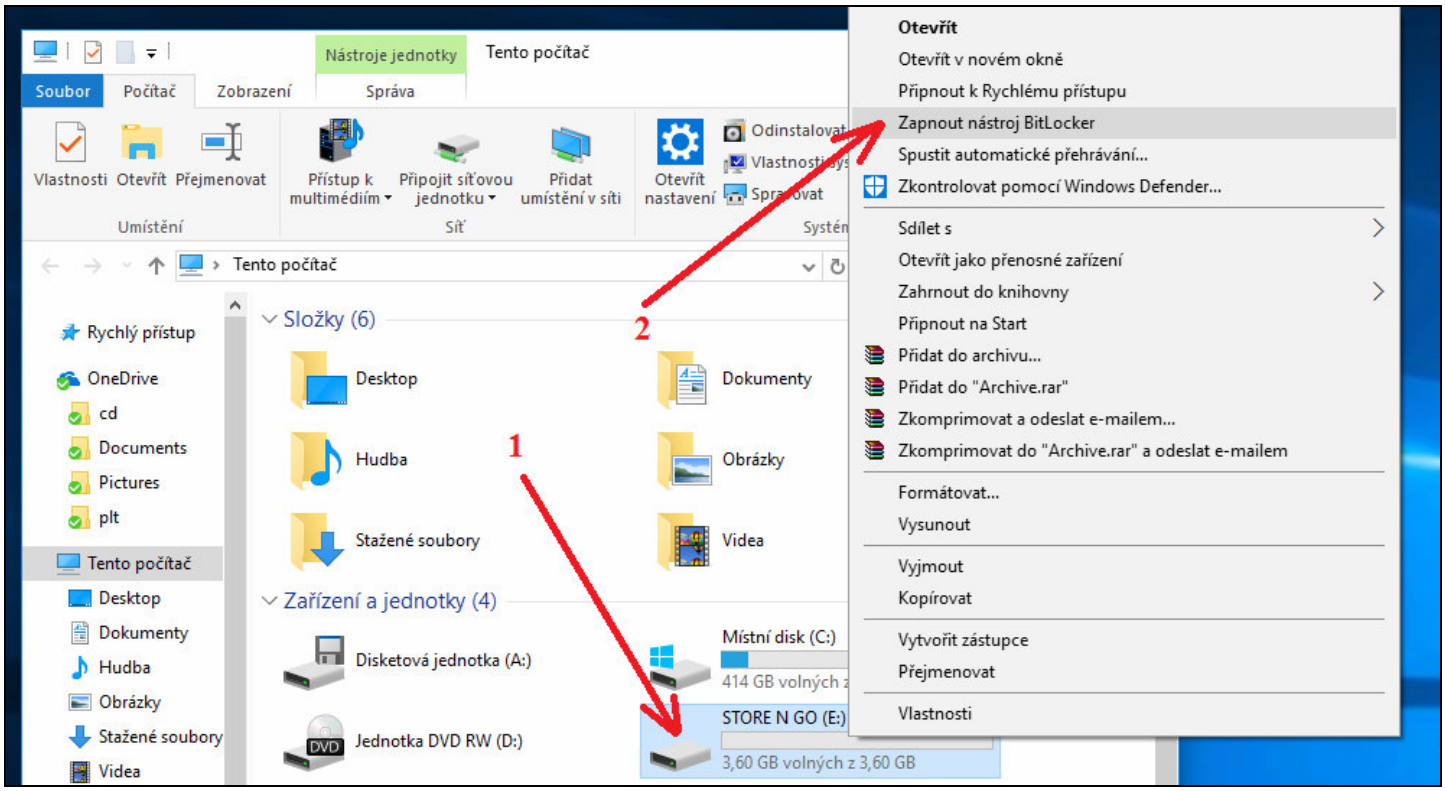
Pokud přistoupíte dle níže uvedeného návodu k přenosu databázových souborů docházky na šifrovaný disk, nezapomínejte na stále nutnou potřebu zálohování databáze a to opět na šifrované (ale jiné) médium. Záloha neslouží jen jako opatření proti ztrátě dat kvůli poškození disku docházkového serveru, ale umožňuje i obnovu stavu databáze docházky po nechtěné operaci s daty. Například když omylem vymažete zaměstnance nebo dokonce celou firmu, není databáze přesunuta na šifrovaný disk proti této operaci chráněna a obnova je možná jen ze zálohy provedené některou z metod popsaných v příručce *zaloha_databaze.pdf* (zohlednit změnu písmene označujícího diskovou jednotku – například míst C: to bude E:).

1) Vytvoření šifrované diskové jednotky

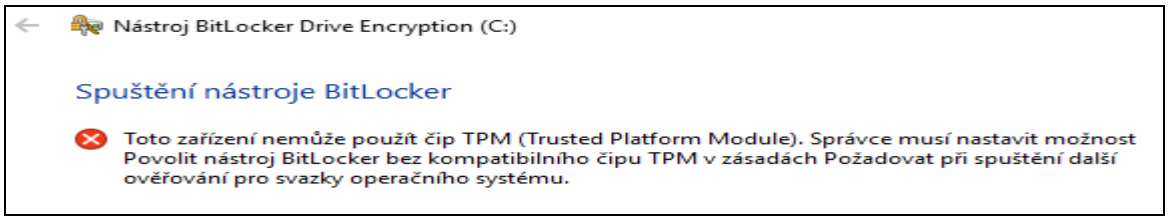
Důležitým předpokladem je, že v hlavním PC docházky (docházkovém serveru) máte buď více fyzických disků, nebo samostatný (sekundární) oddíl vytvořený na primárním disku. Jednotka C:\ tedy zůstane beze změny a budeme pracovat například s diskem E:\. Z tohoto samostatného diskového oddíl tedy vytvoříme šifrovaný disk pomocí nástroje BitLocker v operačním systému Windows 10.

Nejprve klikněte v dolní liště vlevo na ikonu žluté složky

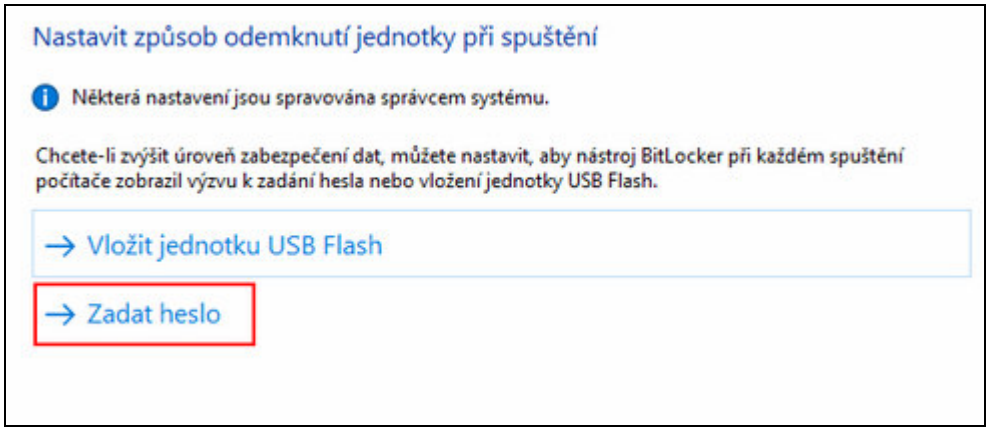
Otevře se průzkumník, vlevo přepneme na *Tento počítač*, klikneme **<u>pravým tlačítkem myši</u>** na diskovou jednotku kterou chceme zašifrovat (zde E:) a z nabídky vybereme volbu *Zapnout nástroj BitLocker.*
Pokud v nabídce tato volba není, máte verzi Windows bez BitLockeru (např. Home) – viz 2. odstavec 1. strany.



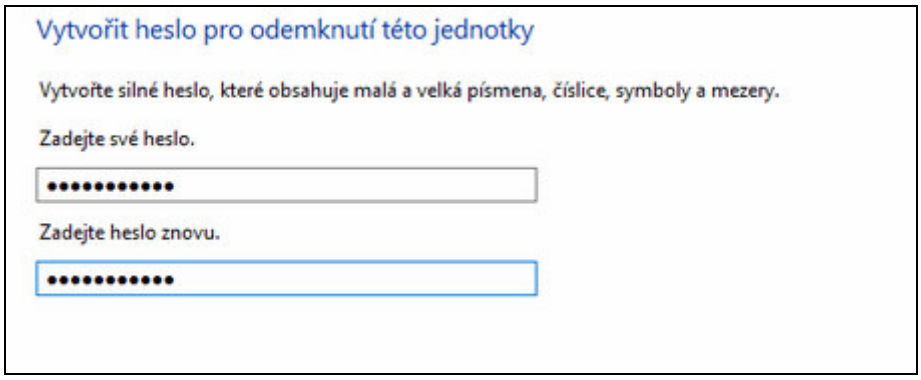
Pokud máte starší počítač, zobrazí se hlášení o nepřítomnosti čipu TPM.



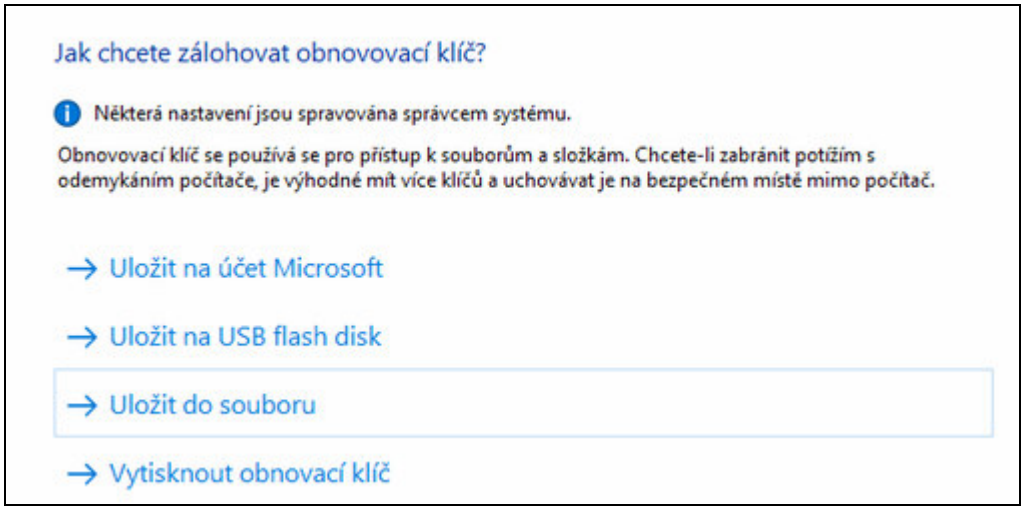
V případě této „chyby“ musíte (přes ikonu lupy na liště Windows vlevo dole) spustit program *gpedit.msc*
Otevře se Editor místních zásad skupiny. V levé části okna se ve stromové struktuře menu proklikejte na »Konfigurace počítače | Šablony pro správu | Součásti systému Windows | Šifrování jednotky nástrojem BitLocker | Jednotky operačního systému«. Zde dvojklikem otevřete nastavení »Požadovat při spuštění další ověřování«. V okně Požadovat při spuštění další ověřování zvolte »Povoleno« a zaškrtněte možnost »Povolit nástroj BitLocker bez kompatibilního čipu TPM«. Potvrďte nastavení tlačítky »Použít« a »OK«. Nyní již půjde aktivovat šifrovací nástroj Bitlocker na disku s operačním systémem bez dalších problémů. Pouze odemčení bude třeba provádět pomocí klíče na flešce nebo pomocí hesla:

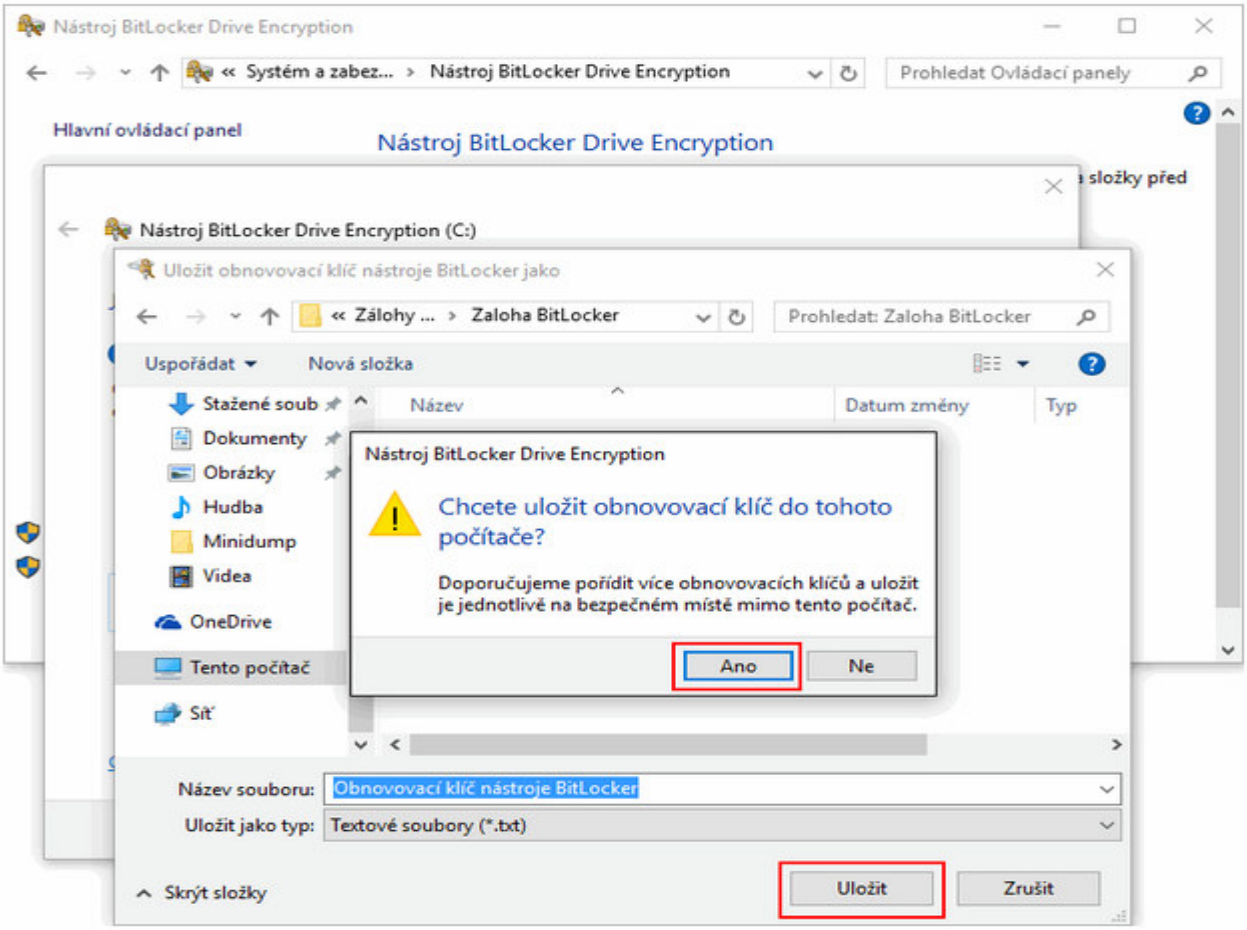


V případě použití hesla zvolte dostatečně silné heslo:



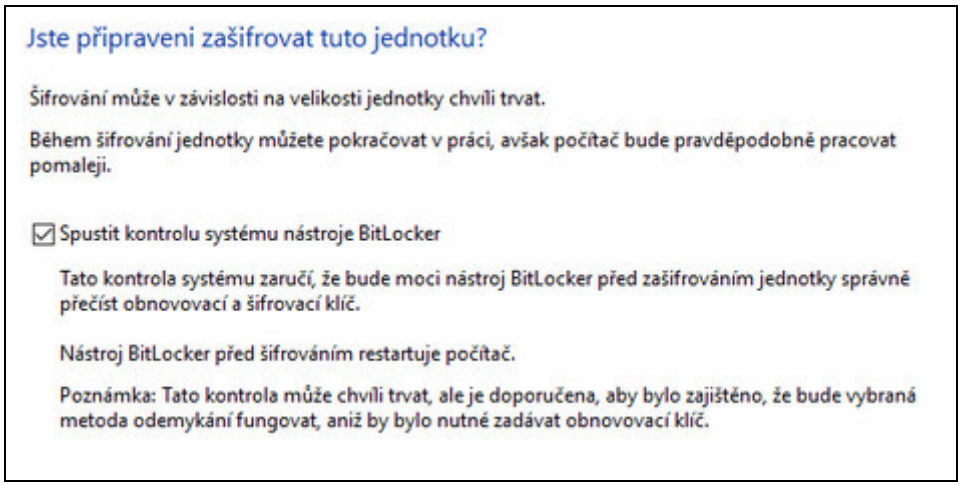
Nyní je nutné zvolit umístění zálohy obnovovacího klíče. Pokud dojde k uzamčení počítače (například z důvodu havárie hardwaru), budete k jeho odemčení potřebovat obnovovací klíč. Požadování tohoto klíče zajišťuje, že počítač může odemknout a obnovit přístup k zašifrovaným souborům pouze autorizovaná osoba. Zálohu obnovovacího klíče uložte mimo počítač na bezpečné místo. V případě jeho ztráty bude jedinou možností uvedení počítače zpět do továrního nastavení. V našem příkladu zvolíme umístění zálohy obnovovacího klíče do souboru. Po kliknutí na »Uložit do souboru«, vyberte umístění zálohy obnovovacího klíče a klikněte na tlačítko »Uložit«. Soubor nelze umístit na jednotku, kterou budete šifrovat.





Zvolte »Zašifrovat celou jednotku« a pokračujte tlačítkem »Další«. V dalším kroku zvolte »Nový režim šifrování« a pokračujte tlačítkem »Další«.

Nakonec ponechte zaškrtnutí volby »Spustit kontrolu systému nástroje BitLocker«, klikněte na tlačítko »Pokračovat« a restartujte počítač.



Po restartu počítače budete vyzváni k zadání hesla k odemknutí jednotky. Zadejte heslo, které jste zvolili v průběhu nastavování nástroje BitLocker a stiskněte klávesu [Enter]. Naběhne operační systém Windows a dojde k zahájení šifrování zvolené jednotky. V Ovládacích panelech nyní vidíte informaci o prováděném šifrování nástrojem BitLocker. Během šifrování můžete pokračovat v práci, ale počítač bude pomalejší.

Nyní bude při každém spuštění počítače vyžadováno zadání hesla k odemknutí šifrované jednotky nástrojem BitLocker Drive Encryption. Nezapomeňte si uložit obnovovací klíč na bezpečné místo mimo počítač.

Takto jsme tedy připravili zašifrovaný disk (v tomto příkladu E:) a můžeme jej použít k uložení databáze docházky. Viz další kroky.

2) Docházkový systém s databází na šifrovaném disku

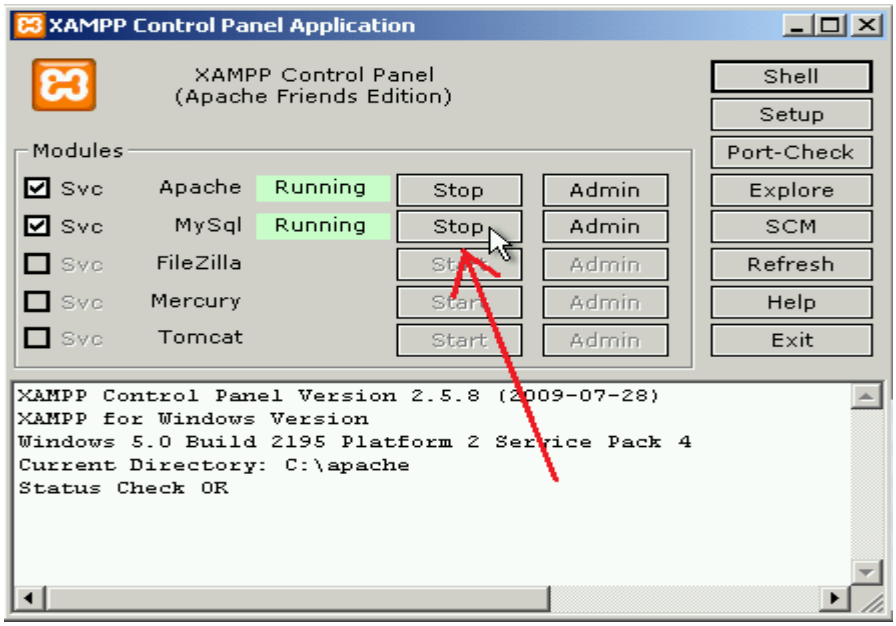
Samotnou instalaci docházkového systému provedete podle tištěného návodu, který k systému dostanete. V instalaci není žádná změna, takže můžete vše zprovoznit a nakonfigurovat kompletně podle instalační příručky na lokální disk PC. Převod na šifrovaný disk není podmíněn žádnou změnou postupu instalace.

Z toho tedy plyne, že k převodu databáze docházky na šifrovaný disk se můžete rozhodnou i kdykoli později, kdy už docházkový systém nějakou dobu používáte. Není tedy nutné docházku přeinstalovávat. Níže uvedený postup je tedy stejný i pro ty uživatele, kteří se k převodu rozhodnou po několika letech provozu Docházky 3000.

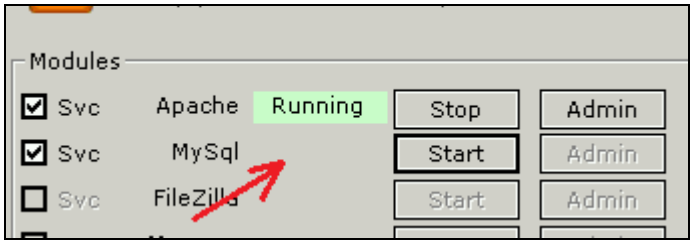
Zastavení databázového serveru docházky:

Před změnou konfigurace je nutné zastavit databázový server docházky. Proto je vhodné provádět celou operaci v době, kdy s docházkou nepracují zaměstnanci a ani není používán docházkový terminál.

Databázový server se zastaví pomocí programu *C:\apache\xampp-control.exe* který je třeba spustit jako uživatel s oprávněním administrátora na docházkovém serveru.



Jakmile se program spustí, klikněte v řádku se službou *MySQL* na tlačítko *Stop*. Po několika vteřinách by měl zmizet zelený nápis *Running* vedle tohoto tlačítka.



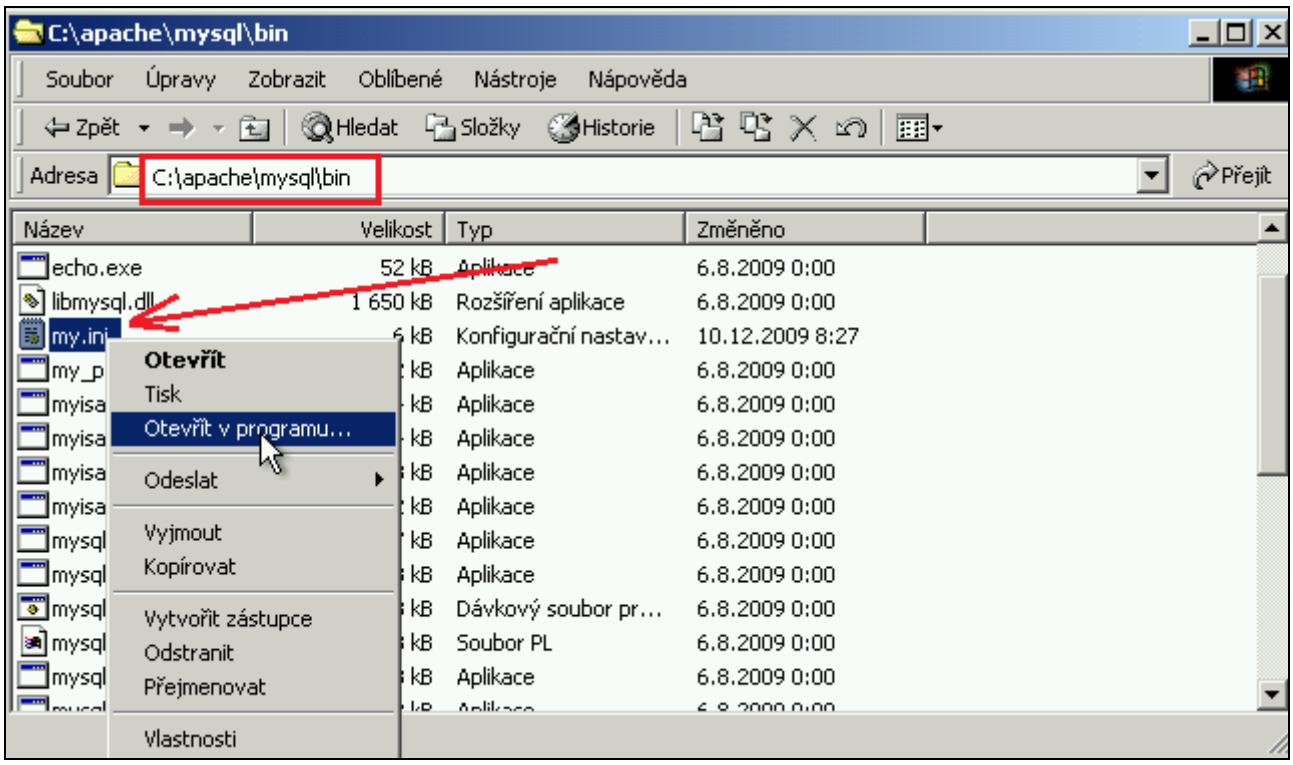
Nyní je databázový server zastaven a s docházkou není možné pracovat.

Kopírování databáze docházky do šifrovaného disku

Nyní je třeba zkopírovat obsah složky *C:\Apache\Mysql\Data* kompletně z primárního disku (oddílu) serveru docházky do zvoleného místa (např. nové složky *E:\databaze*) na šifrovaném disku. Musí se přenést vše kompletně včetně podsložek z *C:\Apache\Mysql\Data*

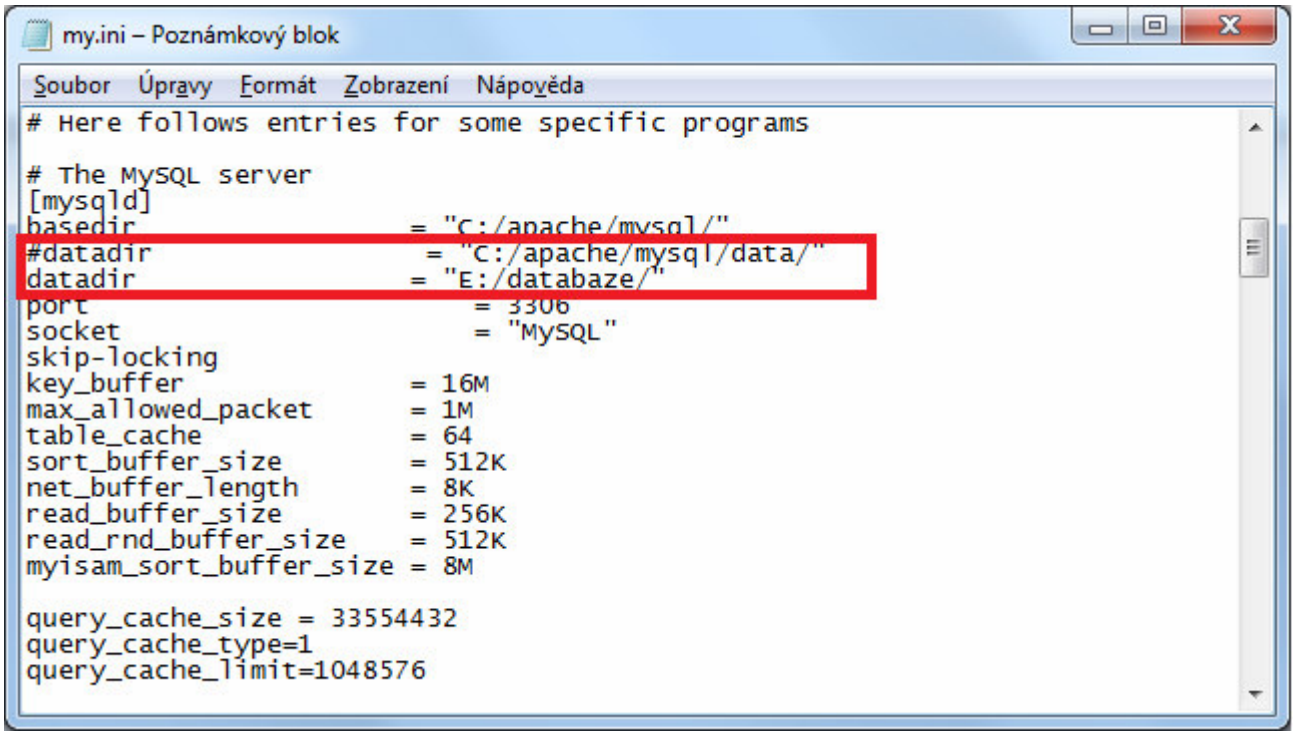
Úprava konfigurace MySQL serveru:

Jakmile je datová složka překopírovaná, je třeba na docházkovém serveru upravit konfigurační soubor *C:\Apache\Mysql\Bin\my.ini* který otevřete nejlépe pomocí programu *Poznámkový blok* (neboli *notepad)* či jiný jednoduchý textový editor.



V souboru vyhledáte v sekci *[mysqld]* řádek s textem *datadir = "C:/apache/mysql/data/"*
Tento zápis je třeba upravit na novou cestu k datové složce na šifrovaném disku. Doporučujeme stávající řádek zkopírovat a pod existující záznam vložit znovu s tím, že na začátek prvního vložíte znak #
Tím se první řádek sice zneplatní (zahešuje), ale zůstane v souboru pro případ pozdější změny úložiště opět zpět na primární disk doch. serveru.

Nakonec druhou kopii řádku upravíte tak, aby obsahovala novou cestu na složku v šifrovaném disku. V našem příkadu tedy bude zápis vypadat takto: *datadir = "E:/databaze/"*



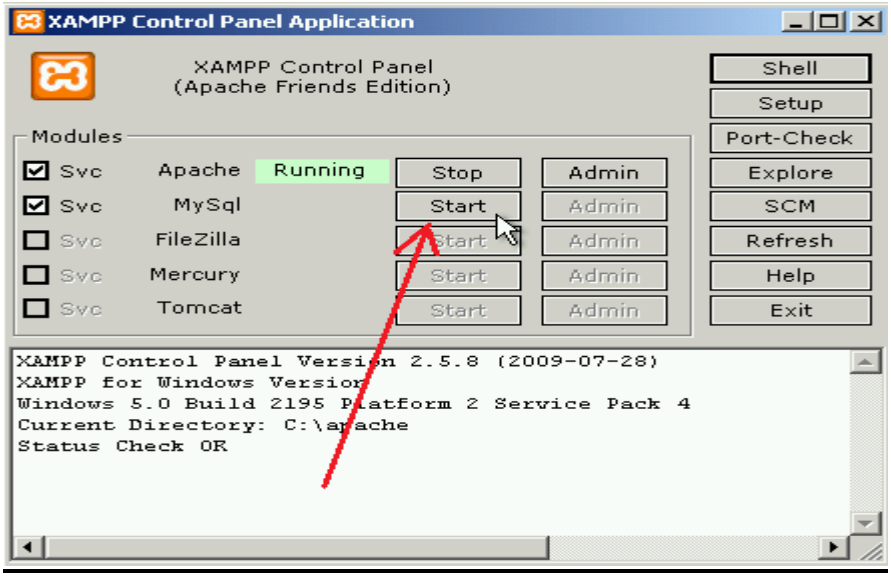
První řádek je zahešovaný (zneplatněný znakem #) a druhý řádek obsahuje nový zápis udávající cestu, na které bude nově MySQL server docházky hledat její databázi.

Upozornění: Pokud využijete šifrovaný síťový disk (například v NASu), tak cesta k datové složce docházky musí být udaná jako síťová cesta. Nefunguje to, že byste nasdíleli disk NAS serveru do operačního systému pod nějakým písmenem jednotky (např. E:) a pak cestu zadali v tomto tvaru s písmenem (např. e:\dochazka – toto nefunguje).
V průzkumníkovi sice uvidíte pod písmenem správnou složku, ale databázový server MySQL neumí s tímto tvarem cesty pracovat a nešel by v bodě 6 spustit. Cesta tedy musí být zadaná jako např: *//JmenoNasu/SdilenaSlozka/DatovaSlozka/* nebo s využitím IP adresy např: *//192.168.1.100/SdilenaSlozka/DatovaSlozka/*

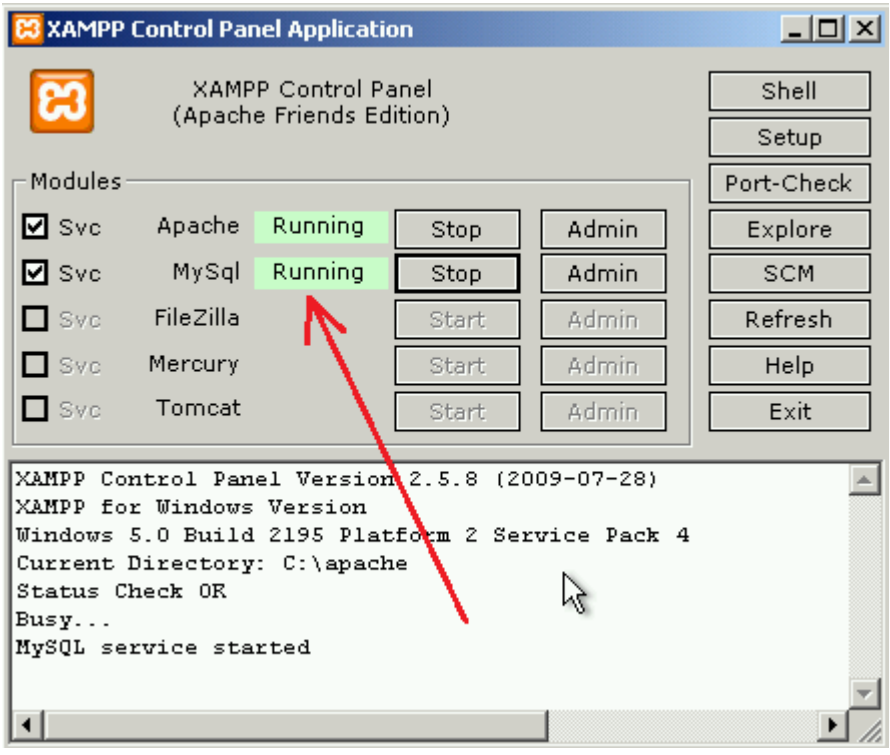
Nyní konfigurační soubor uložte (např. CTRL-S nebo *Soubor / Uložit)* a tím je konfigurace hotová.

Opětovné spuštění MySQL serveru

Obdobným postupem jako v bodě 3 je nyní třeba nastartovat databázový systém MySQL na hlavním PC docházky – docházkovém serveru. Takže spusťte programu *C:\apache\xampp-control.exe* a v jeho řádku *MySQL* klikněte na tlačítko *Start.*



Po několika vteřinách se rozsvítí zelený nápis *Running* a docházka by měla začít opět fungovat.



Pokud by se databázový systém MySQL do několika vteřin nespustil, máte špatně zadanou cestu k datové složce na sdíleném disku. Při použití šifrovaného disku v NASu musí mít docházkový server přístupová práva a právo přihlášení správně nastavena, aby mohla služba MySQL s datovým adresářem vždy plně pracovat.

Ochrana účtu databázového spojení:

Standardně se aplikační server Apache přes PHP připojuje do databáze pomocí parametrů zadaných na hlavním PC docházky (docházkovém serveru) v souboru *c:\apache\htdocs\dochazka2001\access.php*
Na 3. řádku je DNS jméno serveru s databází nebo jeho IP adresa, na 4. řádu uživatelské jméno a na 5. řádku heslo tohoto uživatele, který musí mít k databázi uvedené na 6. řádku plná práva, aby mohl vkládat, upravovat a mazat tabulky i záznamy v nich. Samotný soubor access nelze vzdáleně přes webový prohlížeč zobrazit, takže uživatelé nemají možnost ze svých pracovních PC parametry spojení docházkového serveru do databáze zjistit. Spojení přímo do databáze ani není přístupné po síti, jelikož databáze nekomunikuje se síťovým rozhraním. Je k ní tedy přístup jen lokálně z docházkového serveru a po síti je ve výchozím stavu po instalaci programu zcela nedostupná. Dostupné je jen webové rozhraní docházky, ale přímo s databází uživatelé přes síť pracovat nemohou – nepřihlásí se po síti na konzolu MySQL serveru, což je nastaveno po instalaci záměrně kvůli ochraně databáze. Museli byste to sami v konfiguraci databázového serveru povolit, což nedoporučujeme. Databáze je tedy přístupná jen pro samotný server docházky, nikoli pro stanice uživatelů. Protože přístup k serveru by si měl správce IT náležitě zabezpečit, aby se nedalo přihlásit například přes vzdálenou plochu bez znalosti silného hesla, je tímto ochráněný i přístup na konzolu databázového serveru. Apache web server se tedy přes PHP připojuje k databázi lokálním spojením dle parametrů v souboru access. Po instalaci je uveden uživatelský účet root s prázdným databázovým heslem. Pokud byste chtěli i tento lokální databázový účet chránit heslem, doplníte heslo tohoto uživatele do souboru access na 5. řádek (nic jiného v souboru neměňte, ani strukturu či pořadí řádků, jinak přestane docházka fungovat). Dále upravíte heslo tohoto uživateli i v databázi pomocí příkazu Set password for ... (viz dokumentace k databázovému serveru). Poté je třeba upravit přístup i pro případné zálohování databáze příkazem mysqldump, přístup pro opravu databáze příkazem test_db a další postupy pracující přímo s databází mimo aplikaci docházky (resp. jejího webové rozhraní). Ochrana účtu databázového spojení heslem ale není nepřekročitelná, protože pokud již uživatel získá přístup k hlavnímu PC docházky, takže na něm dokáže spouštět příkazy a zobrazovat soubory, může si ze souboru access heslo přečíst. Takže pro ochranu databáze je třeba v první řadě chránit přístup k docházkovému serveru standardními prostředky Windows. Což je v pravomoci správce IT.

Závěrem:

Po přenosu databáze na šifrované datové úložiště doporučujeme otestovat správné fungování docházky včetně přenosu dat z terminálů atd. Hlavně nezapomeňte ověřit funkčnost i po restartu hlavního PC docházky – docházkového serveru. Ten musí mít k datové složce na šifrovaném disku přístup a to i hned po naběhnutí systému po restartu, aniž by se musel přihlašovat uživatel. Jinak by nemusela služba MySQL automaticky nastartovat.

Původní nešifrovanou databázi uloženou v adresáři *C:\apache\mysql\data\db003444* je vhodné smazat (stačí soubory obsažené přímo v této složce), aby nehrozil únik nešifrovaných dat z pohledu obecného nařízení o ochraně osobních údajů (GDPR) nebo kyber-bezpečnostní směrnice NIS2. Samozřejmě za předpokladu, že se šifrovanou databází systém bezchybně funguje a je uložena na jiném disku (tedy nešifrovali jste přímo disk C:\). Původní nešifrovanou databázi před smazáním zazálohujte (např. na šifrovaný flash disk).

Při používání databáze docházky v této upravené konfiguraci na jiném než primárním (C:\ ) šifrovaném disku je třeba myslet na to, že v příručce pro zálohování databáze dojde ke změně u metody A a C. Data nejsou na primárním systémovém disku C:\, ale na samostatném šifrovaném disku či oddílu (v tomto příkladu disk E:\). Nyní se zdá tato poznámka jasná, ale pokud se třeba časem rozhodnete vyměnit hlavní počítač docházky za jiný, vyvstává riziko, že zapomenete na nové umístění databáze. Změna tedy bude i v příručce pro přeinstalaci

docházky na jiné PC - je třeba použít na novém docházkovém serveru databázi ze šifrovaného disku. Upravte firemní směrnici k zálohování / obnově dat

Rovněž podpora ze strany výrobce počítá se standardním umístěním databáze na lokálním disku C:\ docházkového serveru. A tak je třeba na upravenou konfiguraci vždy myslet a upozornit ostatní správce, pracovníky podpory, či si náležitě upravit kroky některých příruček z dokumentace (oprava databáze, záloha, přeinstalace atd.). Problematika podpory ze strany výrobce je vzhledem k nařízení GDPR a směrnici NIS2 komplikovanější (zasílá se databáze) a je řešena v návodu v programu v menu *Firma / Nařízení GDPR*

Pokud se později z nějakého důvodu rozhodnete vrátit databázi ze šifrovaného disku zpět na systémový disk C:\ docházkového serveru, musíte opět při vypnuté služby MySQL zkopírovat jak soubory datové složky databáze, tak také upravit zpět konfigurační soubor *my.ini* – stačí odhešovat (smazat #) prvnímu zápisu u položky *datadir* s lokální cestou a zahešovat spodní s cestou na šifrovaný disk. Následně uložit konfiguraci a opět spustit službu MySQL.

Řešení problémů:

Pokud při startu OS není přístup k šifrovanému disku k dispozici, nespustí se služby MySQL a docházka pak zobrazuje na úvodní obrazovce chybu navázání spojení s databází. Pak lze dodatečně po přihlášení službu MySQL nastartovat například přes příkazový řádek spuštěním příkazu: *net start mysql*
V případě problémů lze dát příkaz do dávkového souboru a spouštět například naplánovanou úlohou. Ale za normálních okolností (šifrování interního disku či oddílu, administrátorská práva, dodržený postup) by se tento problém neměl vyskytnout a vše by mělo fungovat bez problému.