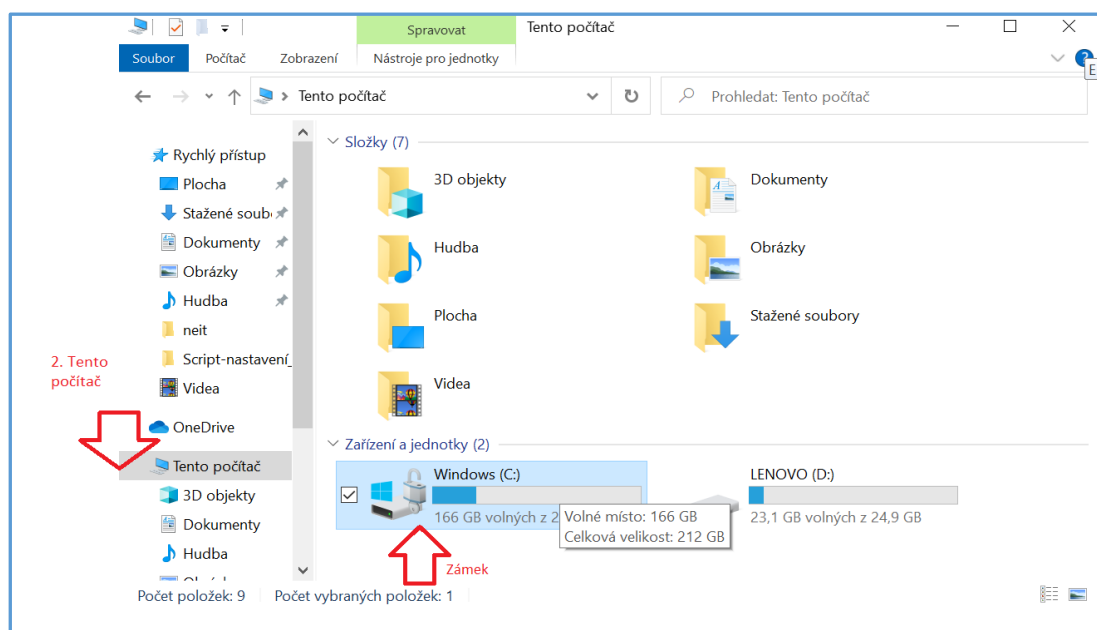


Návod na zjištění stavu zabezpečení disků nástrojem BitLocker a provedení zálohy obnovovacích klíčů.

Zjištění stavu disků na počítači:

1. Spustit průzkumníka
2. Vybrat „Tento počítač“

Zde již vidíme, zda je disk **šifrovaný (označený zámekem, jako u disku C:)** nebo ne (bez zámku, jako u disku D: viz obr.)



Pokud nástroj BitLocker zatím není použit, přejděte rovnou k návodu na jeho **zapnutí na straně 4**.

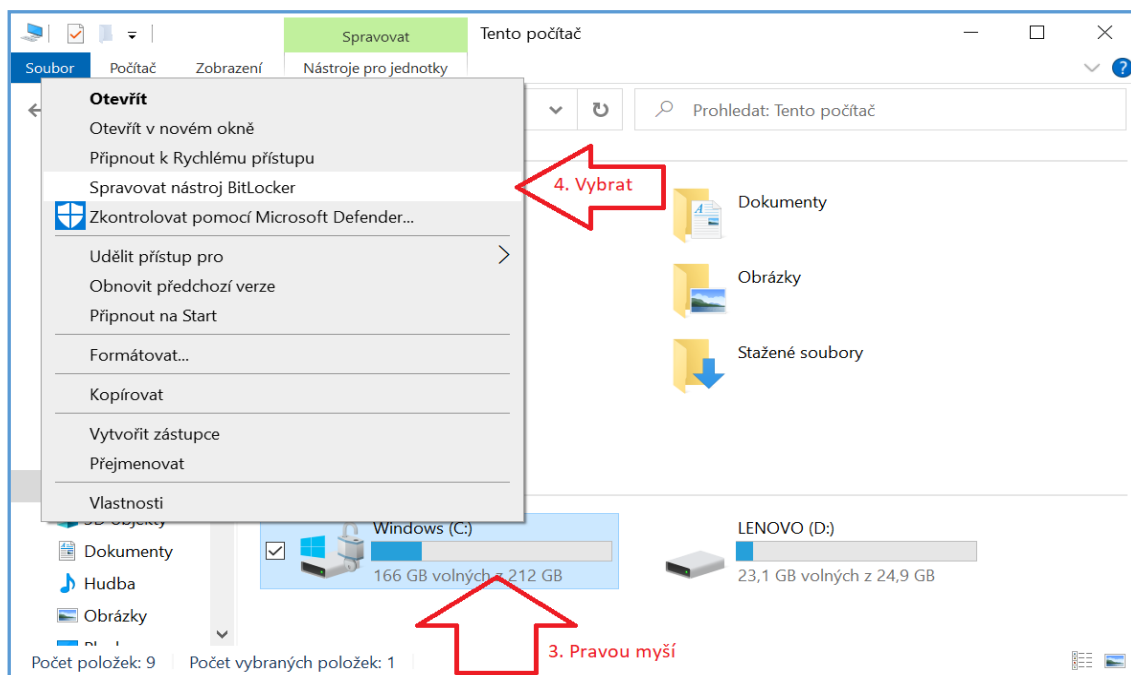
Pokud je disk již zašifrovaný a nevíte, kde máte uložené klíče, je možné provést zálohu klíčů dodatečně, a to několika způsoby - viz bod 3. a dále. Pro umístění zálohy klíče není vhodné použít disk přímo v počítači a už vůbec ne ten šifrovaný, ke kterému klíč patří! Dobrá volba je zvolit USB flash disk nebo klíče vytisknout na papír, ještě lépe pak obojí, protože ani flash disk není příliš spolehlivé médium. Zálohy si pak uložte na bezpečné místo.

V současné době byla také změněna bezpečnostní politika (GPO) naší domény tak, aby záloha klíčů disku C byla vždy před zahájením šifrování primárně uložena v databázi AD. Z tohoto důvodu **nyní již nepůjde provést aktivaci BitLockeru a zašifrování disku, bez toho aniž by daný počítač byl v daný moment připojený (přihlášený) k doméně ad.neit.cz (NEIT)**. Způsob lokální zálohy klíčů zůstává nezměněn a je i nadále v moci běžného uživatele.

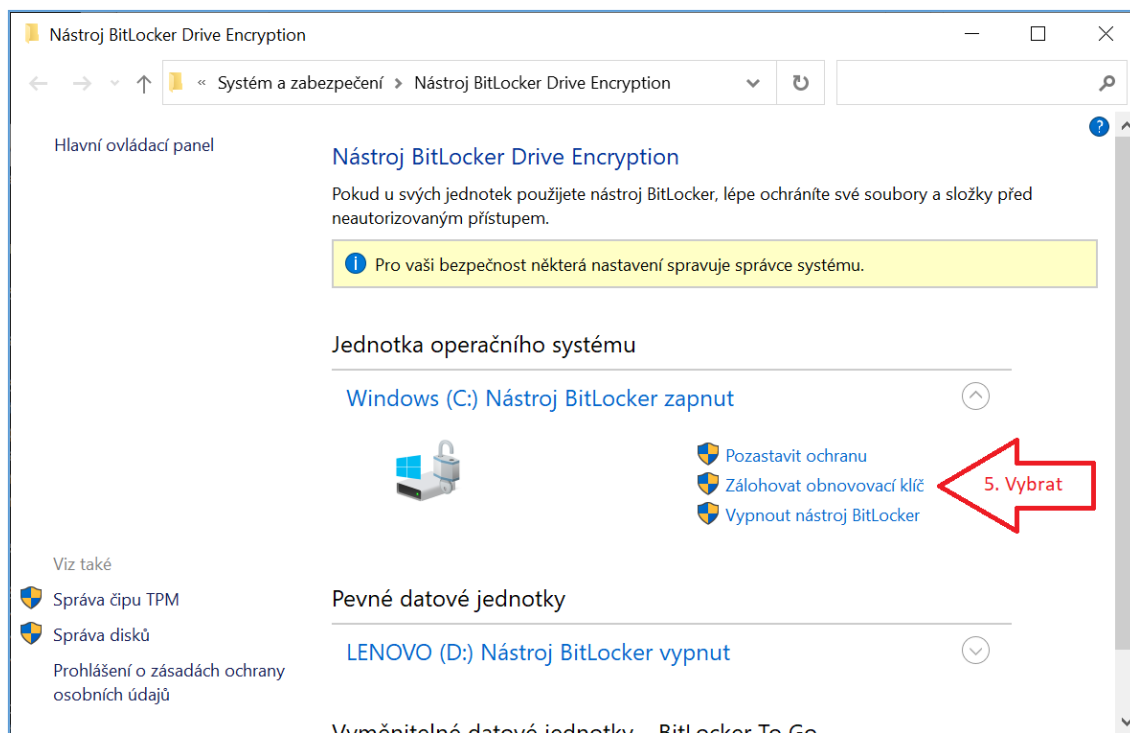
U počítačů, které již mají aktivovaný BitLocker a zašifrovaný disk z dřívější doby, dojde k uložení klíčů do databáze AD buď automaticky po načtení změněné GPO nebo budou dotyční uživatelé postupně informováni některým ze správců infrastruktury, který zároveň poradí, jak klíče do AD načíst dodatečně.

Nyní už záloha klíčů na lokální médium:

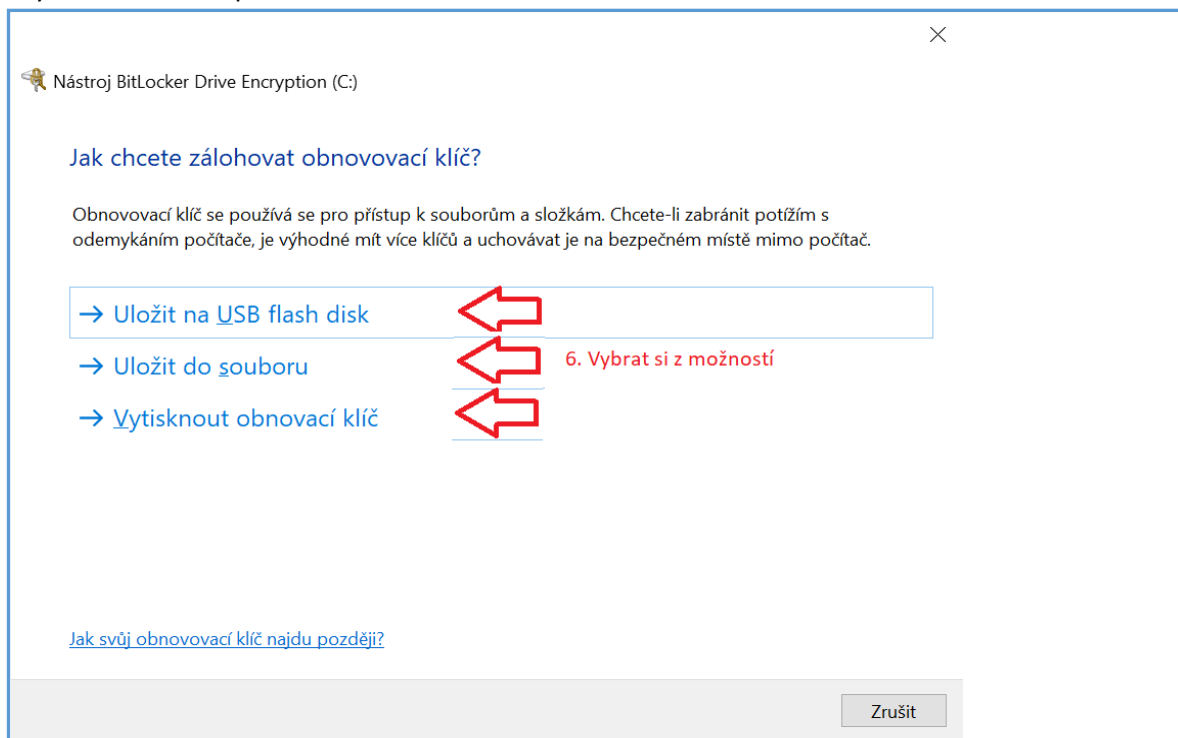
3. Pravým tlačítkem myši kliknout na zašifrovaný disk (označený zámečkem)
4. Vybrat „Spravovat nástroj BitLocker“



5. Vybrat „Zálohovat obnovovací klíč“



6. Vybrat si médium pro zálohu klíče a dát uložit.



7. Zálohu uložit na bezpečné místo.

Návod na zapnutí nástroje bitlocker a zašifrování disků:

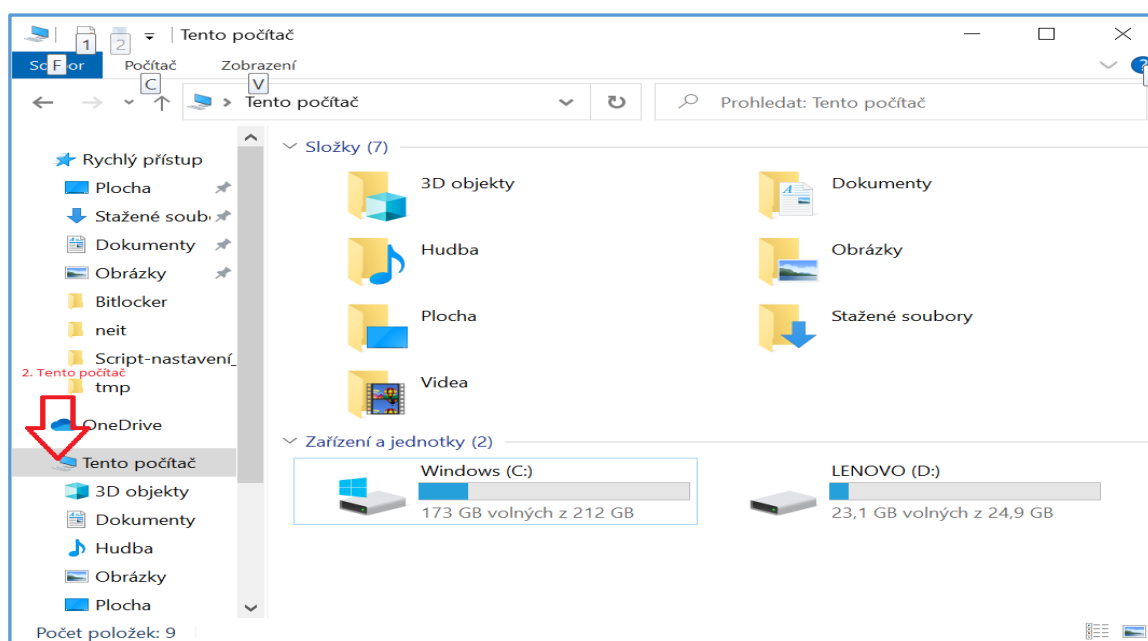
Pokud máte disk rozdělen na více oddílů, např. C a D, zašifrujte podle následujícího návodu nejdříve disk C. Postup u dalších disků je trochu odlišný, viz **str. 8**. Pro disk C je totiž klíč uložen v čipu TPM (mimo disk) a odtud je pak přenesen do centrální databáze AD. To se u ostatních disků již neděje, proto následuje důležité upozornění:

Zašifrování je NUTNÉ nejprve provést na jednotce C a až poté na jednotce D, v opačném případě hrozí, že se do systému již nepřihlásíte a může dojít ke ztrátě dat!

Pokud chcete zašifrování disku vypnout, je nutné nejprve vypnout nástroj bitlocker na jednotce D a až poté na jednotce C!

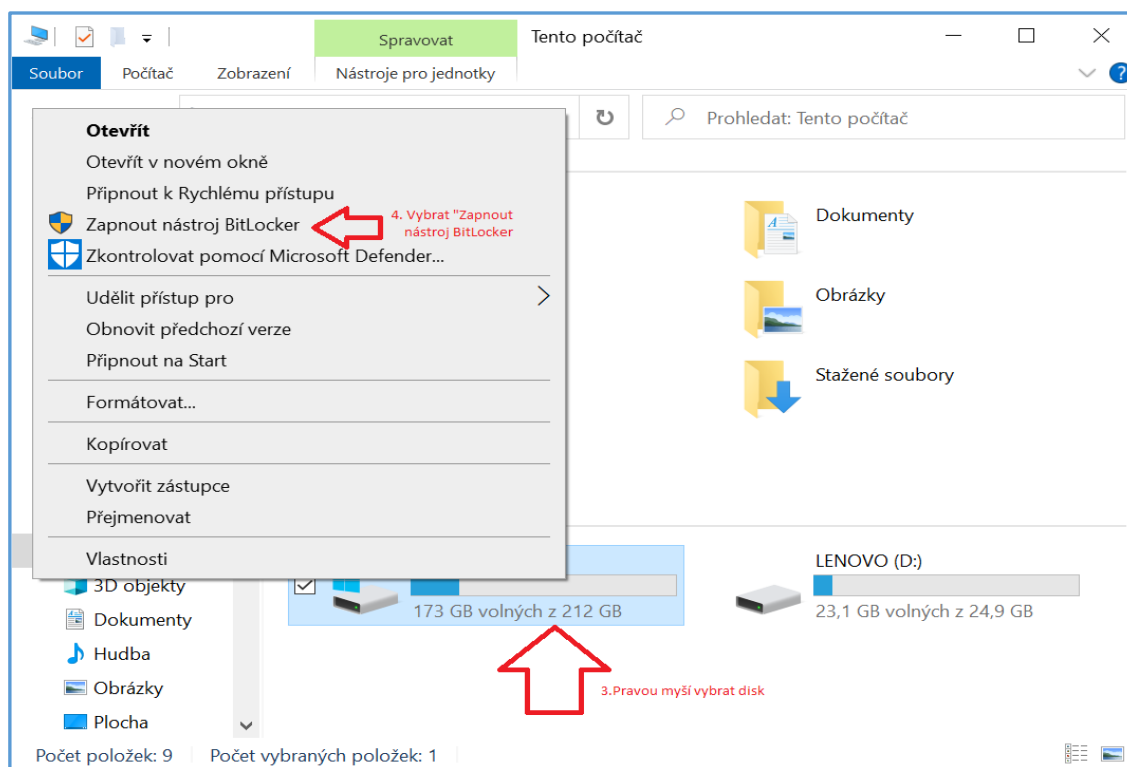
A nyní již postup při šifrování jednotky C:

1. Ideální varianta je připojit počítač přímo v kanceláři k LAN přes kabel RJ45 a přihlásit se k firemní doméně (**doménovým účtem**).
2. Následně vybrat „Tento počítač“.

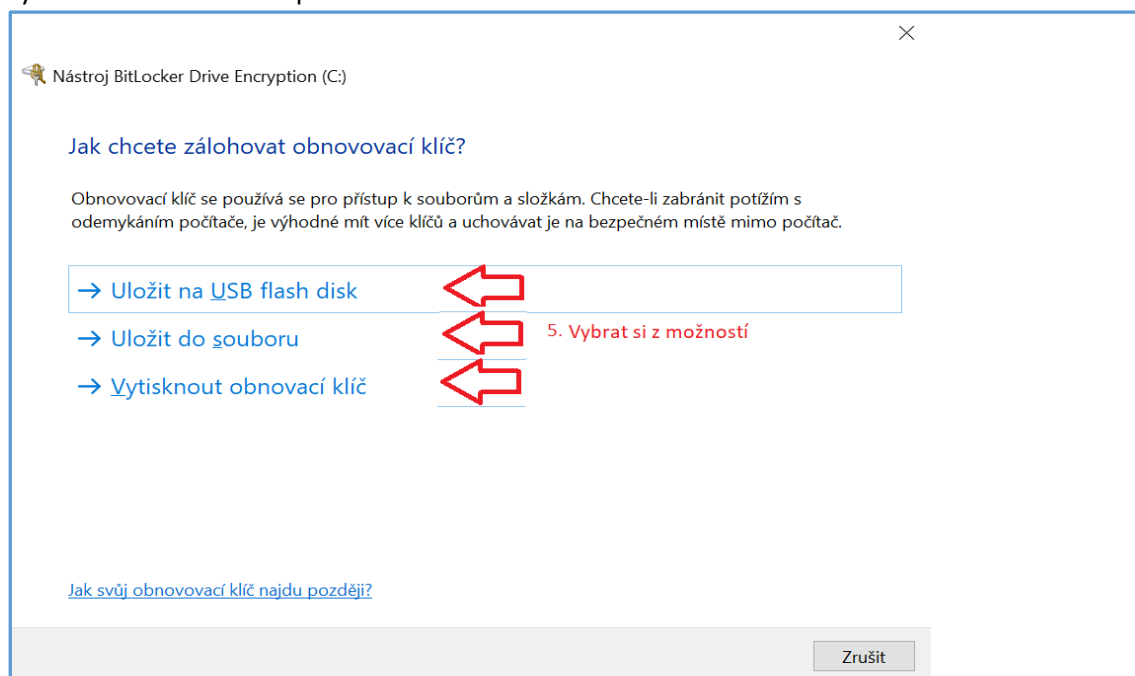


(Pozn.: Obdobně je možné postup realizovat i v ovládacích panelech, tím se však zabývat nebudu.)

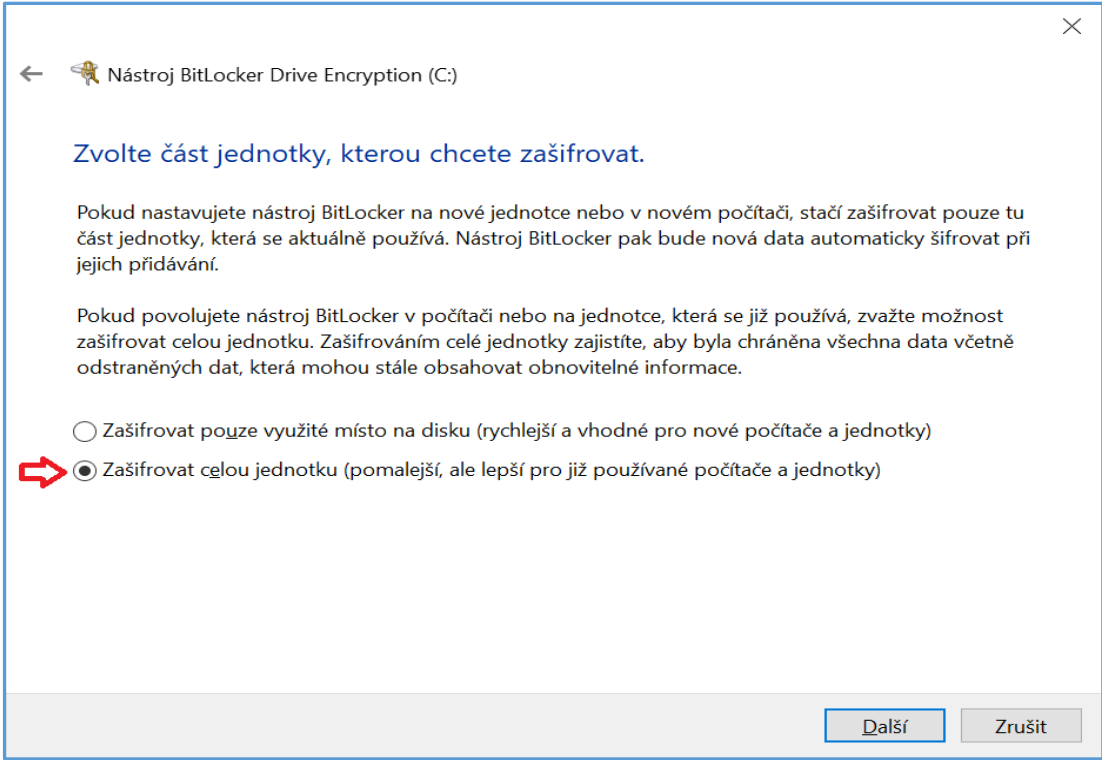
3. Pravým tlačítkem myši kliknout na požadovaný nezašifrovaný disk C: (bez označení zámečkem)
4. Vybrat „Zapnout nástroj BitLocker“



5. Vybrat si cílové médium pro zálohu klíče.



6. Vybrat „Zašifrovat celou jednotku...“



←  Nástroj BitLocker Drive Encryption (C:)

Zvolte část jednotky, kterou chcete zašifrovat.

Pokud nastavujete nástroj BitLocker na nové jednotce nebo v novém počítači, stačí zašifrovat pouze tu část jednotky, která se aktuálně používá. Nástroj BitLocker pak bude nová data automaticky šifrovat při jejich přidávání.

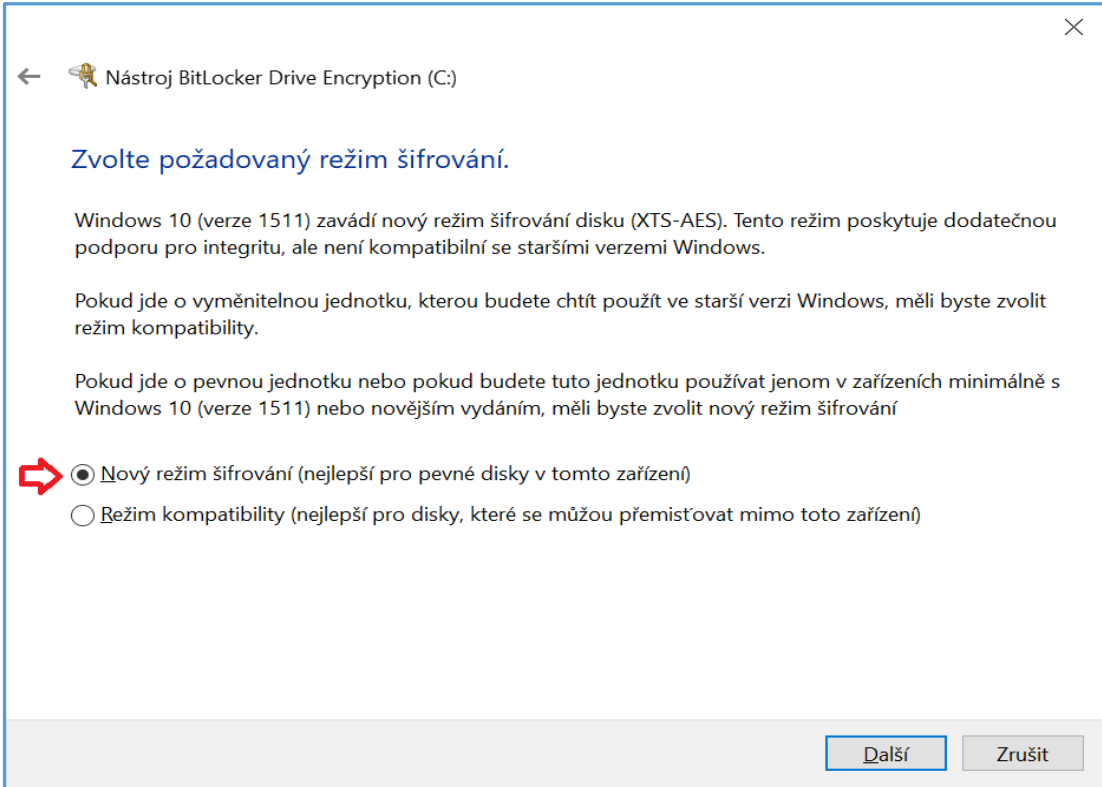
Pokud povolujete nástroj BitLocker v počítači nebo na jednotce, která se již používá, zvažte možnost zašifrovat celou jednotku. Zašifrováním celé jednotky zajistíte, aby byla chráněna všechna data včetně odstraněných dat, která mohou stále obsahovat obnovitelné informace.

☐ Zašifrovat pouze využitě místo na disku (rychlejší a vhodné pro nové počítače a jednotky)

 ☒ Zašifrovat celou jednotku (pomalejší, ale lepší pro již používané počítače a jednotky)

Další **Zrušit**

7. Vybrat „Nový režim šifrování...“



←  Nástroj BitLocker Drive Encryption (C:)

Zvolte požadovaný režim šifrování.

Windows 10 (verze 1511) zavádí nový režim šifrování disku (XTS-AES). Tento režim poskytuje dodatečnou podporu pro integritu, ale není kompatibilní se staršími verzemi Windows.

Pokud jde o vyměnitelnou jednotku, kterou budete chtít použít ve starší verzi Windows, měli byste zvolit režim kompatibility.

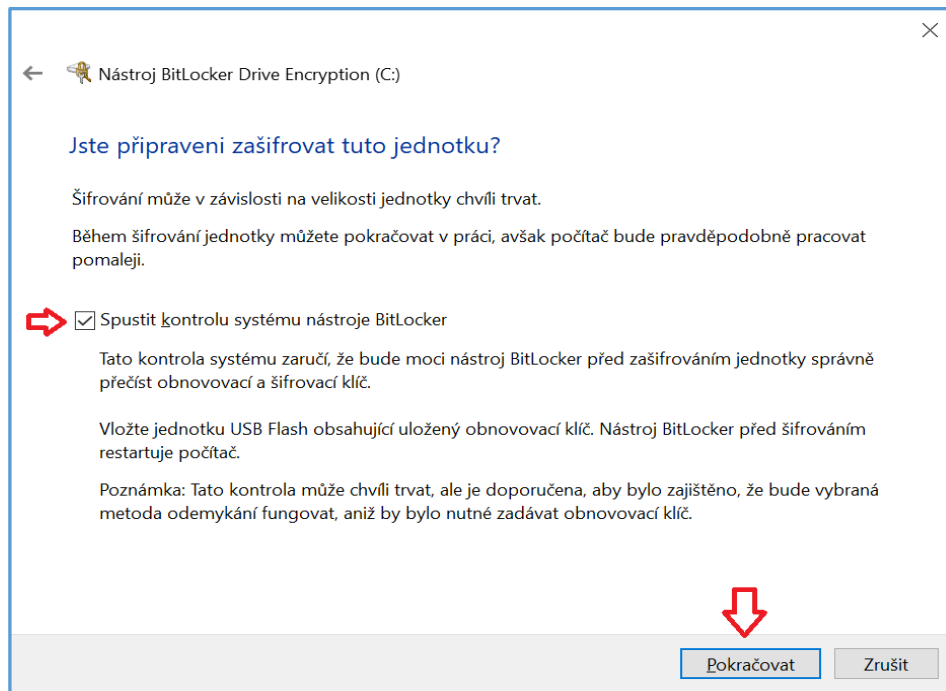
Pokud jde o pevnou jednotku nebo pokud budete tuto jednotku používat jenom v zařízeních minimálně s Windows 10 (verze 1511) nebo novějším vydáním, měli byste zvolit nový režim šifrování

 ☒ Nový režim šifrování (nejlepší pro pevné disky v tomto zařízení)

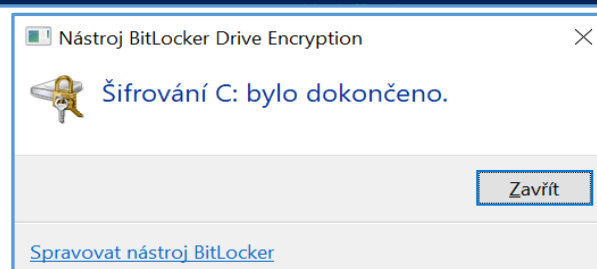
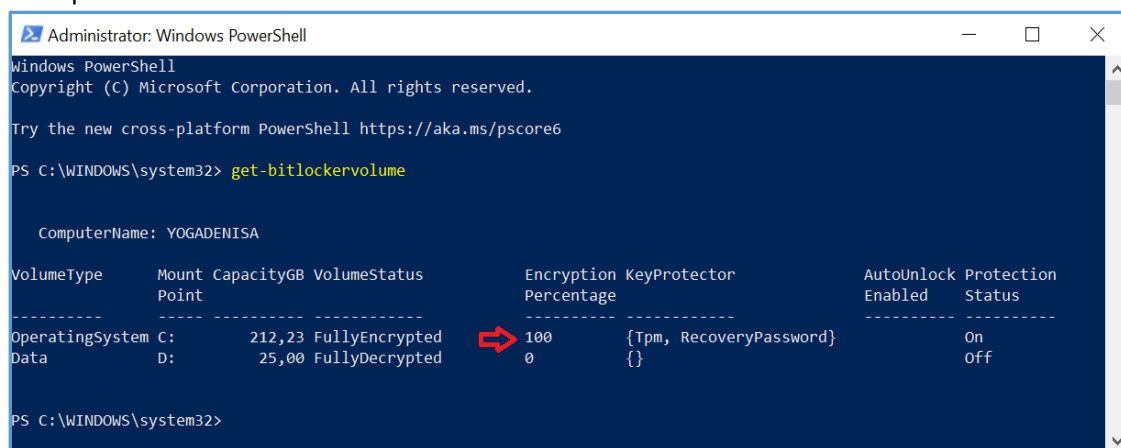
☐ Režim kompatibility (nejlepší pro disky, které se můžou přemísťovat mimo toto zařízení)

Další **Zrušit**

8. Doporučené je zaškrtnout „Spustit kontrolu systému...“. (Přeskočit kontrolu je možné jen v případě, že BitLocker byl na počítači použit již někdy v minulosti.) Následně pak stisknout tlačítko „Pokračovat“

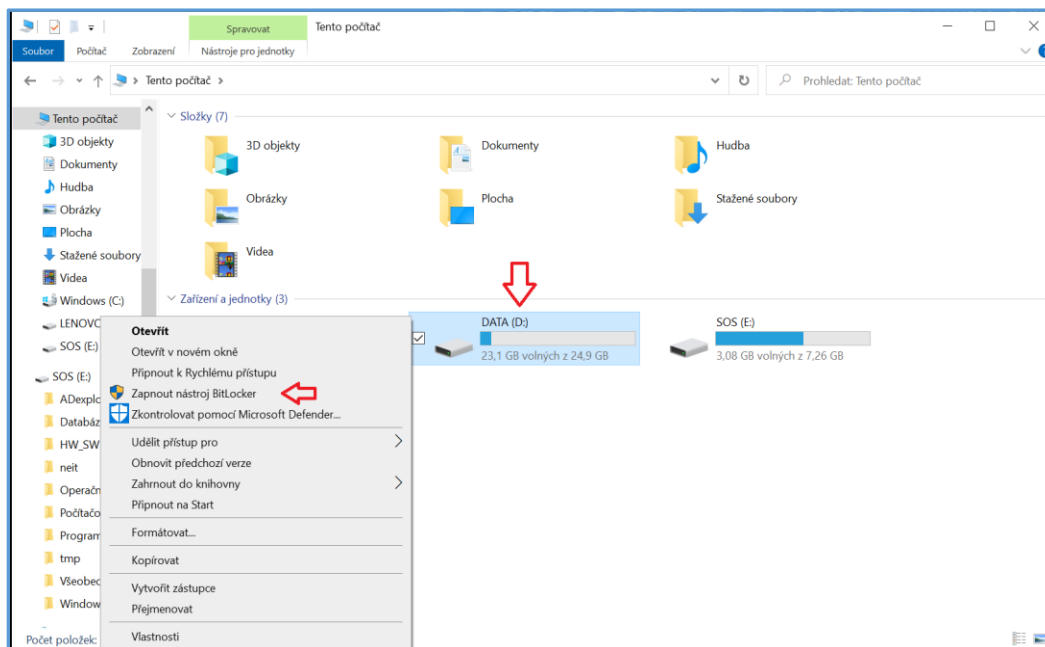


9. Nyní počkáme, až se po kontrole počítač zrestartuje. Po té je již možno během šifrování pokračovat v běžné práci. Doba šifrování záleží na velikosti a rychlosti disku. Pokud se chceme přesvědčit, že již bylo dokončeno, můžeme v konzoli PoweShellu spuštěné „jako administrátor“ použít cmdlet „Get-BitlockerVolume“, který nám ukáže průběh operace v procentech:

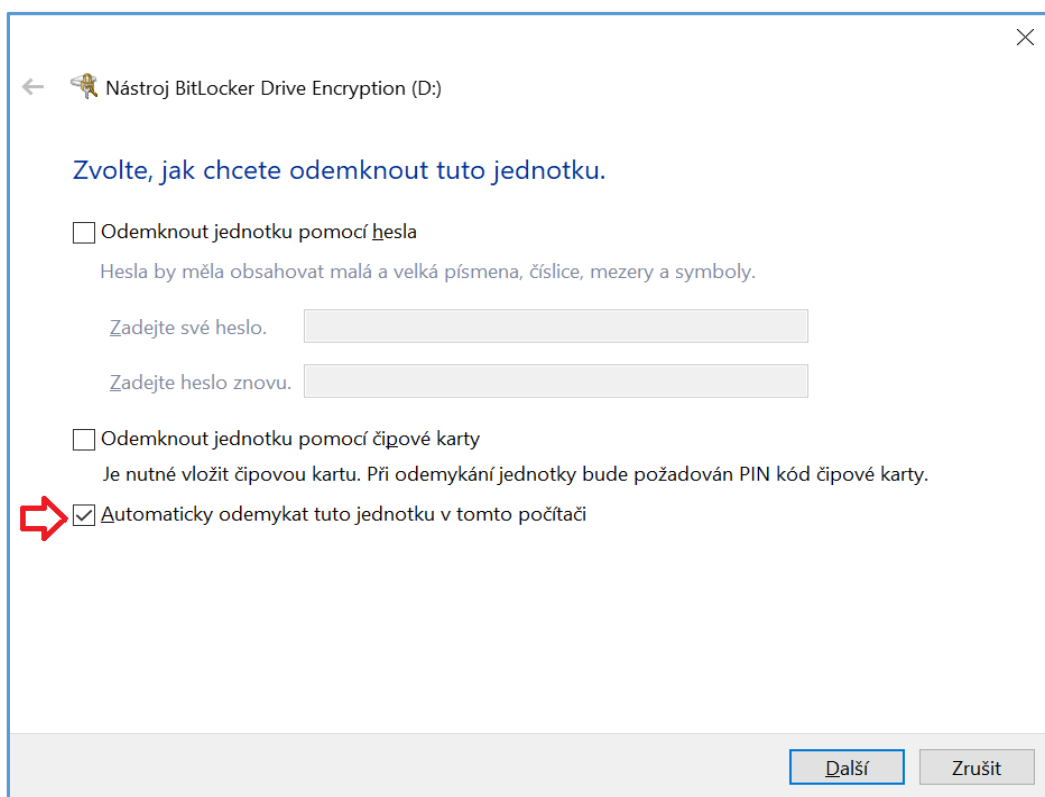


Pokud máte disk rozdělen na více oddílů, např. C a D pokračujte zašifrováním disku D:

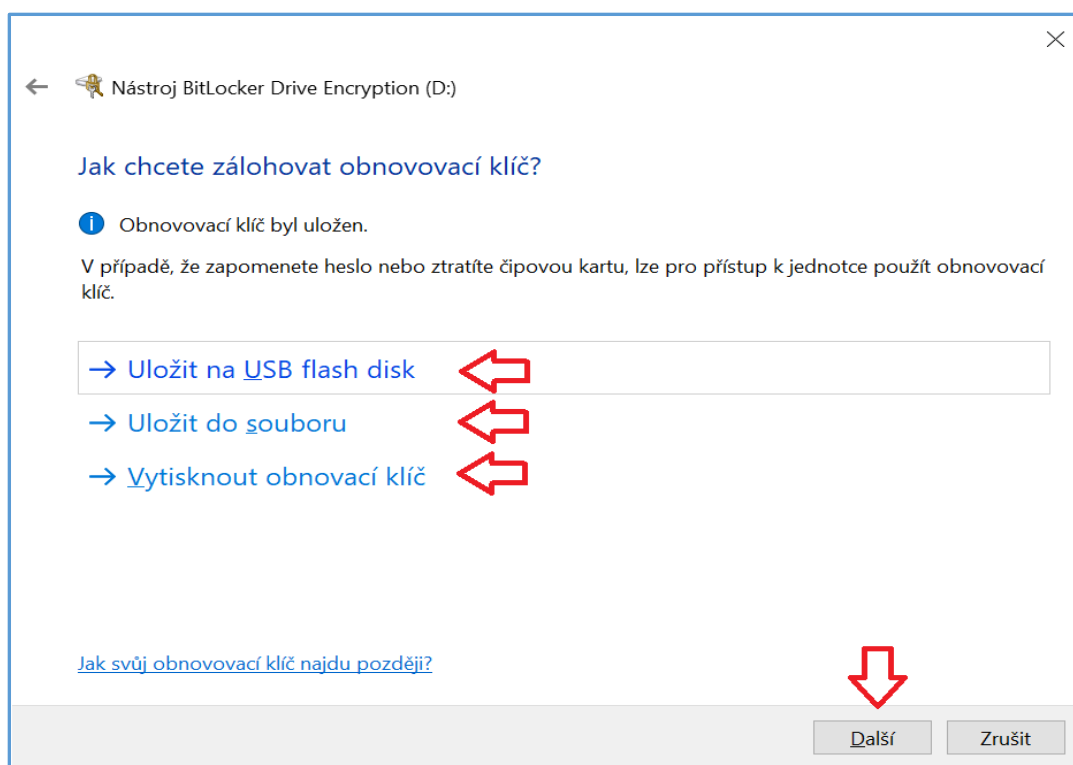
1. Obdobně jako u disku C:



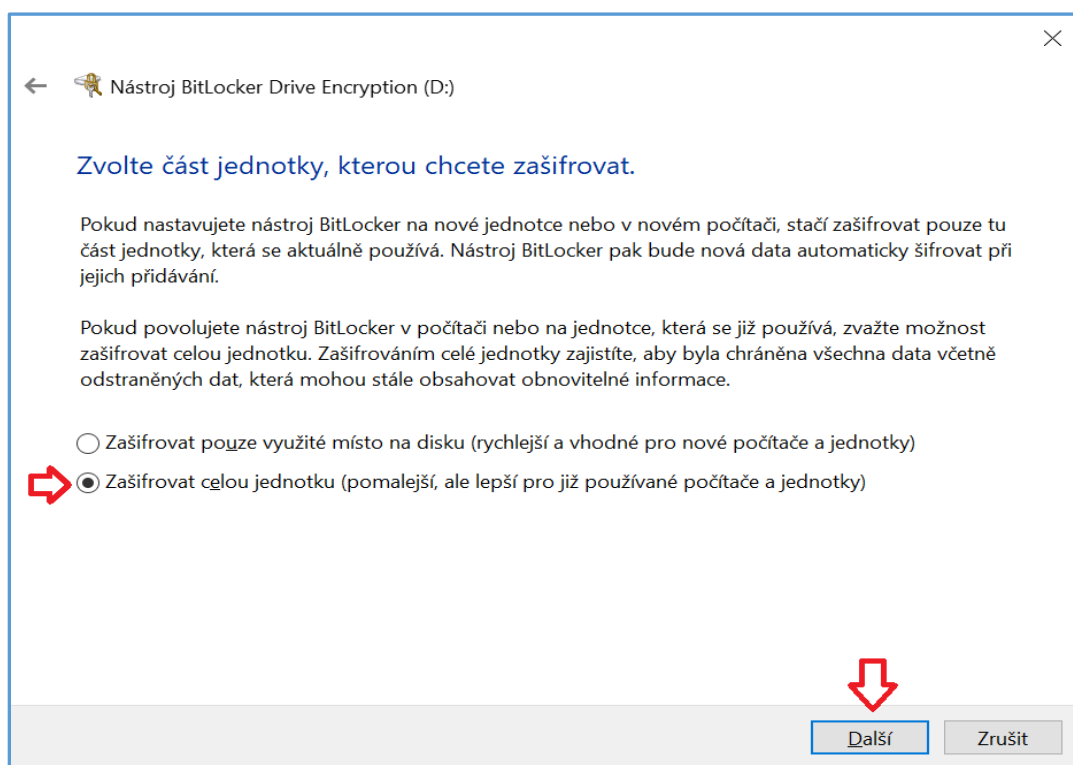
2. Pozor, zde je změna:



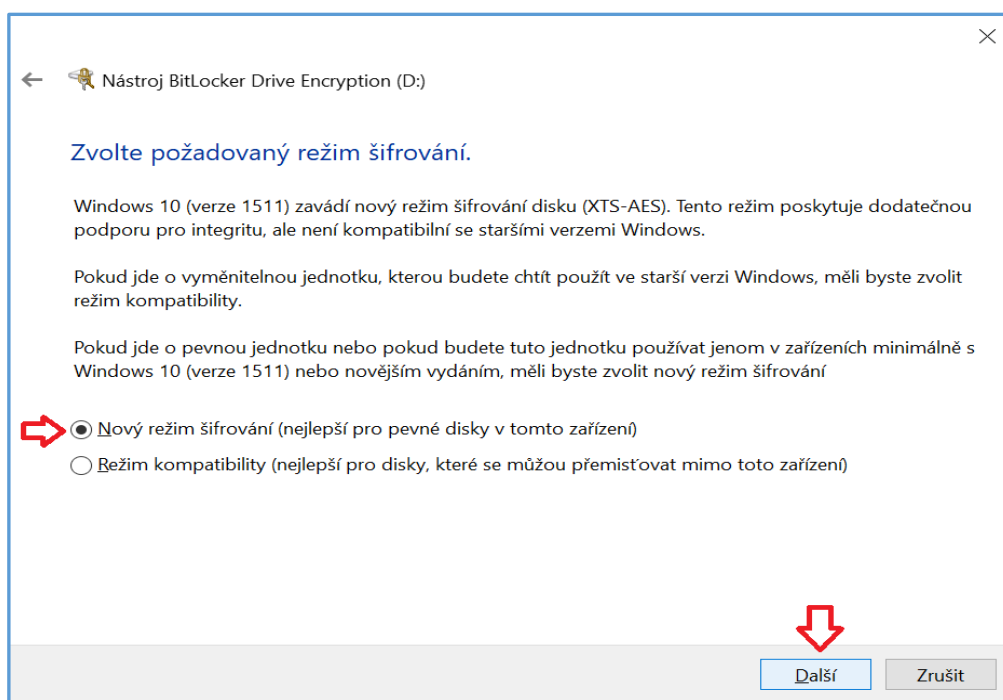
3. Obdobně jako u disku C vybrat, kam se uloží záloha klíče:



4. Doporučené je zvolit opět celou jednotku. U klasického velkého a zároveň poloprázdného HDD bych ale zvolil „Zašifrovat pouze využité místo“, neboť v takovém případě může být operace o několik hodin kratší.



5. Obdobně jako u disku C:



6. Obdobně jako u disku C, ale již bez kontroly:

