Filip Pospíšil, xpospi27

VeraCrypt - bezpečné šifrování dat pro ochranu informací

https://www.veracrypt.fr/en/Home.html

Popis technologie

VeraCrypt je *open-source* nástroj pro šifrování disků v reálném čase. Nástroj vznikl jako nástupce nástroje *TrueCrypt* a je dostupný zdarma pro *Windows, macOS i Linux* Jedná se o software pro transparentní šifrování disků, který umožňuje šifrovat celé pevné disky nebo jednotlivé diskové oddíly. Dále umí vytvořit virtuální šifrovaný disk (souborový kontejner), který se po připojení chová jako běžný diskový svazek. VeraCrypt podporuje silné šifrovací algoritmy (např. *AES, Serpent, Twofis*h, …) , navíc lze případně více algoritmů kaskádovat pro vyšší bezpečnost. Podporována je i tvorba skrytých šifrovaných svazků pro popiratelné šifrování (*plausible deniability*)[1].

Cena technologie a náklady na nasazení:

VeraCrypt je k dispozici zcela zdarma (jedná se o freeware s open-source licencí *Apache 2.0* a *TrueCrypt 3.0*). S nasazením nejsou spojené žádné licenční poplatky. Náklady na nasazení spočívají především v čase správce nebo uživatele, který provede instalaci a základní konfiguraci. Pro osobní použití jsou finanční nároky minimální – pouze čas na nastavení. Pro firemní použití může být nákladem integrace do firemních procesů, avšak samotný software zůstává bezplatný. Vzhledem k dostupnosti na více platformách nejsou nutné ani dodatečné náklady na různé verze pro různá prostředí. Hardwarové nároky *VeraCryptu* jsou nízké – moderní procesory s podporou *AES-NI* akcelerace zvládají šifrování dat s minimálním dopadem na výkon systému.

Účel technologie

Proti jakým hrozbám VeraCrypt chrání:

VeraCrypt slouží k ochraně důvěrnosti dat uložených na pevných discích či přenosných úložištích před neoprávněným přístupem.

- **Ztráta nebo krádež zařízení:** Pokud je notebook nebo externí disk se senzitivními daty ztracen nebo odcizen, útočník nemůže číst uložená data bez znalosti hesla či klíče. Šifrování dat je snadný a efektivní způsob ochrany, který předchází zneužití dat i v případě fyzického získání úložiště neoprávněnou osobou. *VeraCrypt* tak brání úniku citlivých informací při krádeži hardware.

[1] Technika, která umožňuje uživateli věrohodně popřít existenci chráněných dat, protože bez správného hesla nebo klíče není možné prokázat, že zašifrovaná data obsahují skrytý obsah.

- **Neoprávněný přístup k uloženým datům:** I pokud má potenciální útočník krátkodobý přístup k disku, narazí pouze na šifrovaná data vypadající jako náhodný šum a bez správného hesla je neinterpretuje. Tím technologie chrání citlivé soubory před přečtením či kopií nepovolanou osobou.
- **Sdílení počítače více uživateli bez oddělení dat:** V případě, že je zařízení používáno více osobami (např. v domácnosti, škole nebo malé firmě) a nejsou nastavena dostatečná oprávnění jednotlivých uživatelů, může dojít k nechtěnému přístupu k citlivým souborům jiného uživatele. Šifrování dat pomocí *VeraCrypt* zajistí, že osobní či důvěrné soubory zůstanou chráněné a přístupné pouze po zadání správného hesla bez ohledu na to, kdo je aktuálně přihlášený do systému.
- **Malware zaměřený na sběr uložených dat:** V situaci, kdy je zařízení kompromitováno škodlivým softwarem (např. *keyloggerem*, *trojským koněm* nebo *spywarem*), může útočník získat volně uložené soubory nebo přihlašovací údaje. Pokud jsou citlivá data uložena ve šifrovaném svazku *VeraCrypt*, bez jeho připojení a znalosti hesla jsou pro malware neviditelná a nečitelná, čímž se minimalizuje riziko jejich odcizení.
- **Ochrana šifrovaných dat proti ransomwaru**: Když je zařízení napadeno ransomwarem tak hrozí zašifrování a následné zpřístupnění všech dostupných souborů na discích. Pokud jsou citlivá data uložena ve VeraCrypt svazku a ten není není v danou chvíli připojen, ransomware k nim nemá přístup a nedokáže je zašifrovat ani poškodit, čímž je výrazně snížené riziko ztráty důležitých dat

Paragrafy z vyhlášky č. 82/2018 Sb., které nasazení splňuje:
§ 12 odst. 2 písm. e) – Bezpečné používání mobilních zařízení: Vyhláška požaduje zavádět bezpečnostní opatření pro bezpečné používání mobilních zařízení a zařízení mimo správu organizace. Šifrování disků notebooků či externích médií pomocí *VeraCrypt* **naplňuje** tento požadavek, neboť chrání data na mobilních zařízeních pro případ jejich ztráty či odcizení. Tím je zajištěno, že citlivé informace nebudou dostupné neoprávněným osobám ani při kompromitaci fyzického zařízení.
§ 26 – Kryptografické prostředky: Tato vyhláška také stanovuje povinnost používat odolné kryptografické algoritmy k ochraně informací. Nasazením *VeraCrypt* organizace využívá aktuálně odolné kryptografické algoritmy a klíče dle písm. a) uvedeného paragrafu. *VeraCrypt* podporuje moderní algoritmy *(AES, Serpent, aj.)* a bezpečné hashovací funkce *(SHA-512, atd.)*, čímž **naplňuje** požadavek silné kryptografie.
§ 26 písm. c) – Bezpečné nakládání s kryptografickými prostředky:
Vyhláška požaduje, aby organizace zajistila bezpečné nakládání s kryptografickými prostředky, zejména ochranou klíčů a hesel před neoprávněným přístupem. *VeraCrypt* v praxi podporuje správu šifrovacích klíčů, umožňuje využití klíčových souborů a hardwarových tokenů a tím naplňuje tento požadavek bezpečného zacházení s klíči i hesly.
§ 17 – Fyzická bezpečnost: Vyhláška požaduje předcházet ztrátě nebo zneužití aktiv fyzickým zabezpečením. *VeraCrypt* sice nezabrání krádeži zařízení jako takové, ale šifrováním uložených dat výrazně snižuje riziko jejich následného zneužití neoprávněnou osobou po odcizení nosiče.
Příloha č. 4 – Opatření k ochraně a likvidaci informací:
Vyhláška uvádí šifrování jako jednu z metod bezpečné ochrany a likvidace citlivých dat. *VeraCrypt* umožňuje bezpečné šifrování dat, a tím naplňuje doporučené opatření k ochraně informací před jejich únikem i při likvidaci médií.

Přínosy nasazení VeraCrypt

Ochrana důvěrnosti a soulad s regulacemi: Šifrování pomocí *VeraCrypt* zásadně zvyšuje důvěrnost uložených dat. I při kompromitaci hardware zůstávají data chráněna, což pomáhá splnit legislativní požadavky na ochranu citlivých informací.

Bezplatné a dostupné řešení: *VeraCrypt* je volně dostupný, takže odpadá nutnost nákupu drahých komerčních řešení pro šifrování disků. To je přínosné zejména pro malé organizace s omezeným rozpočtem.

Snadné použití a multiplatformnost: *VeraCrypt* nabízí přívětivé uživatelské rozhraní a průvodce, které usnadňují vytvoření šifrovaného svazku i laikům. Podporuje více operačních systémů, což usnadňuje nasazení – např. uživatelé s *Windows* i *macOS* mohou sdílet šifrovaný kontejner.

Vysoká úroveň bezpečnosti: Nástroj používá prověřené šifrovací algoritmy a metody derivace klíčů (*PBKDF2 s iteracem*i, možnost nastavit *PIM – Personal Iterations Multiplier* pro zvýšení odolnosti proti *brute-force*). Oproti původnímu *TrueCrypt* byly ve *VeraCrypt* opraveny známé slabiny a posíleny některé algoritmy.

Funkce skrytého svazku (deniability): Unikátní funkcionalitou je možnost vytvořit skrytý šifrovaný svazek uvnitř jiného svazku. To přináší *popiratelnou šifrovací ochranu* – v případě nátlaku může uživatel odhalit pouze vnější „nevinný“ svazek a utajit existenci vnitřního (skrytého) svazku s nejcitlivějšími daty.

Široké možnosti použití: *VeraCrypt* lze využít k šifrování celých systémových disků s předbootovým ověřením (na *Windows*), k šifrování externích disků nebo k tvorbě šifrovaných souborových kontejnerů pro zálohy a cloudová úložiště. Tato flexibilita umožňuje chránit data v různých scénářích použití.

Případová studie nasazení

Popis prostředí: Jako modelový příklad nasazení volím notebook s *Windows 10.* Testovací prostředí tvoří fyzický počítač, aby byly simulovány reálné podmínky. Před nasazením *VeraCrypt* tento notebook uchovával data nešifrovaně na interním SSD. Hrozbou v tomto prostředí je zejména odcizení notebooku nebo kompromitace disku, což by útočníkovi umožnilo číst data. Cílem nasazení *VeraCrypt* je integrovat šifrování tak, aby byly veškeré citlivé informace na těchto úložištích chráněny.

Zapojení do infrastruktury: Notebook *Lenovo Legion 5* je osazený interním SSD diskem. Ten je rozdělený na systémový oddíl *C:* a datový oddíl *D:*, přičemž oddíl *D:* bude zašifrován *VeraCryptem*. Uživatel při startu systému zadává heslo k odemykání šifrovaného oddílu, resp. před připojením externího disku zadá heslo ve *VeraCrypt*, aby se disk připojil. V podnikovém nasazení by obdobný princip aplikovali jednotliví zaměstnanci – každý pracovní notebook by měl šifrovaný disk a společnost by definovala pravidla pro správu hesel a zálohování klíčů. *VeraCrypt* v tomto individuálním scénáři nevyužívá žádnou centrální infrastrukturu – je to klientská aplikace běžící na každém zařízení samostatně. Integrace do infrastruktury je tedy poměrně přímočará – zahrnuje instalaci softwaru na cílový stroj a nastavení šifrování na úrovni operačního systému nebo souboru.

Základní konfigurace VeraCrypt: Na testovacím notebooku jsem zvolil následující postup konfigurace pro šifrování datového oddílu *D:*. Místo šifrování celého systémového disku *C:* (které by vyžadovalo *pre-boot autentizaci*) jsem se rozhodl pro demonstraci zašifrovat oddíl *D:*, kde v praktickém nasazení budopu uložena veškerá citlivá data uživatele. Tato volba probíhá bez zásahu do boot procesů. Pomocí průvodce *VeraCrypt* jsem vytvořil nový šifrovaný svazek na oddílu *D:*. Z dostupných algoritmů jsem ponechal výchozí *AES (256-bit)* v módu *XTS*, který poskytuje vysokou rychlost díky hardwarové akceleraci a zároveň silné zabezpečení. Jako hash funkci pro *PBKDF2* jsem zvolil *SHA-512*. Nastavil jsem heslo o délce 20 znaků. *VeraCrypt* nabízí možnost definovat tzv. *PIM* (*Personal Iterations Multiplier*) – ponechal jsem implicitní hodnotu, která již sama o sobě zvyšuje počet iterací derivace klíče (na ~500k iterací pro AES-SHA512), čímž se dále znesnadňuje prolomení hesla hrubou silou.

Ověření funkčnosti: Po nasazení a nastavení *VeraCrypt* jsem otestoval, že vše funguje správně a dosahuje požadované bezpečnosti:

- **Kontrola šifrovaného oddílu:** Po dokončení šifrování oddílu *D:* se tento oddíl stal nepřístupným bez použití *VeraCrypt*. Při pokusu otevřít oddíl v Průzkumníku Windows systém nabídl jeho naformátování (protože pro něj vidí pouze nesrozumitelná data). To potvrzuje, že data jsou pro systém bez dešifrování nečitelná.
- **Připojení (mount) šifrovaných svazků:** Spustil jsem *VeraCrypt*, vybrali zašifrovaný oddíl *D:* a zadali správné heslo. Oddíl *D:* se během několika vteřin připojil jako dostupný disk (oddíl je nutné připojit pod jiným písmenem než *D:*) a byl normálně čitelný – ověřil jsem, že všechny soubory jsou v pořádku. Rychlost čtení a zápisu uvnitř těchto svazků byla prakticky shodná s nešifrovaným stavem, což jsem ověřil kopírováním většího souboru a měřením času.
- **Test vypnutí a přihlášení:** Po odpojení (unmount) šifrovaných svazků jsem počítač restartoval. Ověřil jsem, že při přihlášení do Windows není šifrovaný oddíl *D:*

přístupný, dokud uživatel znovu nespustí *VeraCrypt* a neodemkne jej heslem. To simuluje scénář, kdy zařízení je ukradeno vypnuté – útočník by po zapnutí viděl jen prázdný disk *D:* vyžadující formátování.

Shrnutí: Celkově se nasazení *VeraCrypt* v testovacím prostředí osvědčilo. Data byla úspěšně zabezpečena proti definovaným hrozbám a běžná práce uživatele (po zadání hesla) zůstala téměř neovlivněná. Tím je demonstrováno, že *VeraCrypt* je vhodný pro osobní/individuální použití k zajištění soukromí dat.

Další vlastnosti, rozšíření a možnosti použití

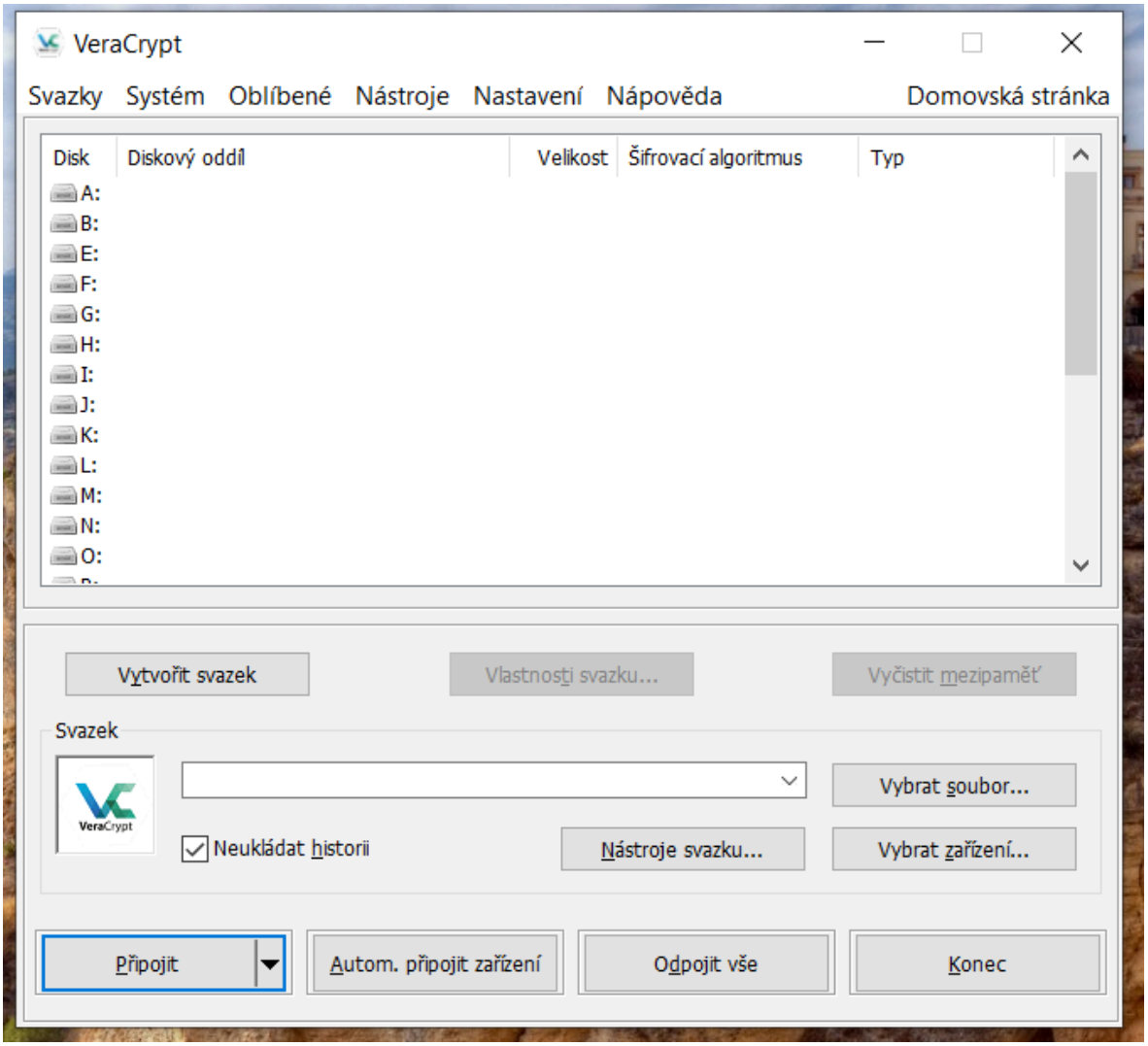
VeraCrypt nabízí i několik dalších funkcí a rozšíření, které stojí za zmínku:

- **Podpora hardwarových tokenů a akcelerace:** *VeraCrypt* umožňuje využít i externí hardwarové tokeny či čipové karty pro ukládání šifrovacích klíčů, což může zvýšit bezpečnost.
- **Možnosti skriptování a přenositelnost:** *VeraCrypt* může běžet i v *přenosném módu (portable mode)* bez instalace, což je užitečné např. při použití na cizím počítači z USB.
- **Bezpečné mazání a ukončení**: *VeraCrypt* dokáže bezpečně vymazat obsah šifrovaného svazku nebo celý svazek (tím, že přepíše klíčové oblasti pseudonáhodnými daty), což prakticky znemožní obnovu původních dat. Také obsahuje funkci „*panic hotkey*“ – možnost nastavit si klávesovou zkratku, která při nouzovém použití okamžitě odpojí všechny svazky a ukončí *VeraCrypt*.
- **Aktivní komunita a vývoj:** *VeraCrypt* je aktivně udržován. Proběhly nezávislé bezpečnostní audity (např. organizací OSTIF v roce 2016 a audit BSI v roce 2020), které nenašly zásadní chyby. Vývojáři reagují na objevené zranitelnosti a vydávají aktualizace – např. aktuální verze 1.26.20 (2025) zahrnuje podporu Windows 11 a opravy drobných chyb.

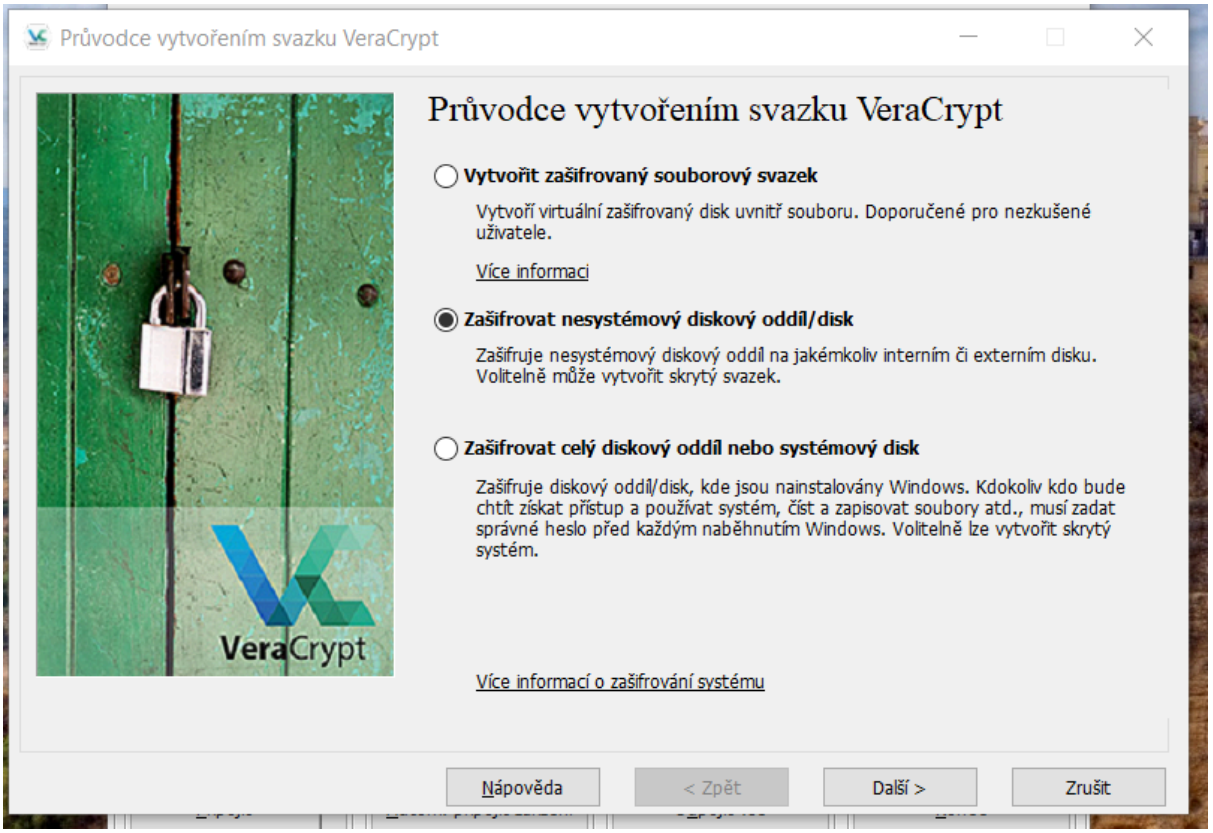
VeraCrypt je silný nástroj pro ochranu dat šifrováním, vhodný primárně pro osobní použití a malé organizace. Poskytuje vysokou úroveň zabezpečení proti celé řadě hrozeb spojených s uloženými daty. Díky nulovým nákladům a flexibilním možnostem konfigurace představuje snadno dostupné řešení, jak zvýšit bezpečnost citlivých informací.

Praktický postup:

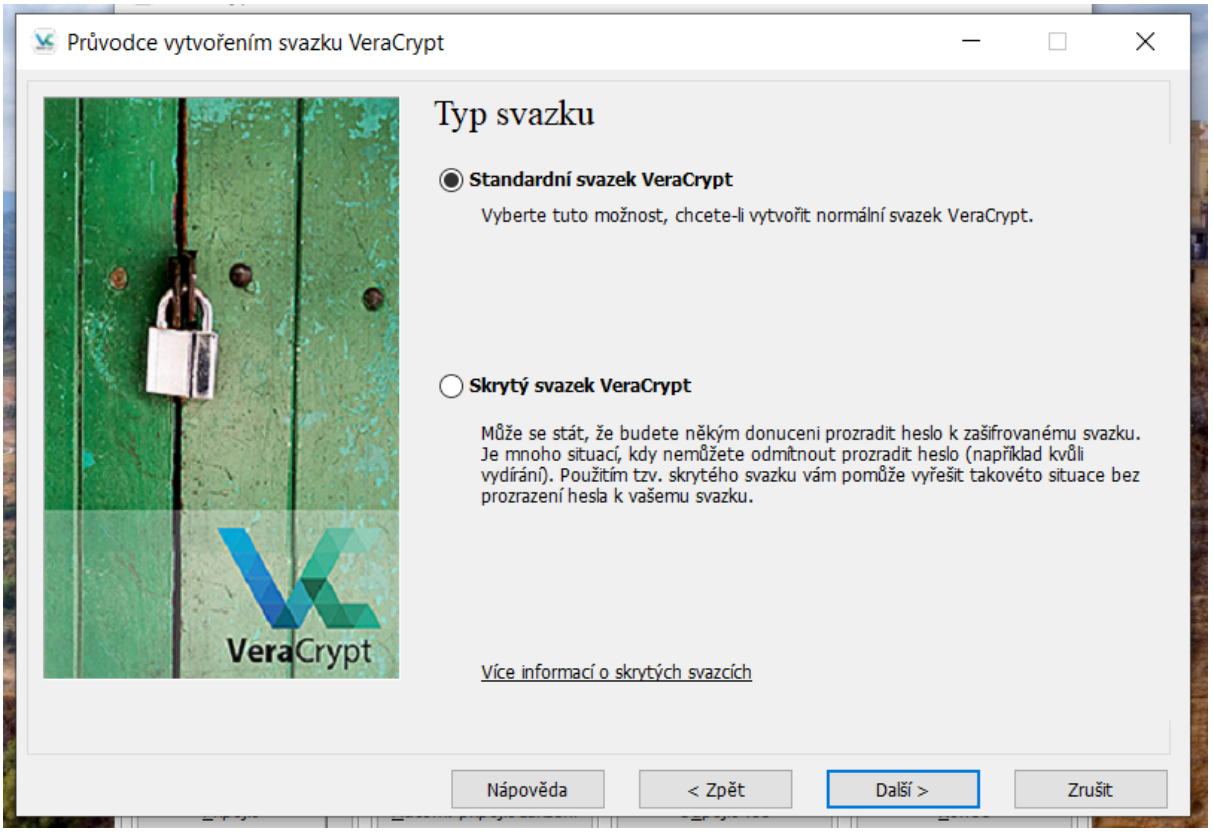
Krok 1: Nainstaluji nástroj *VeraCrypt* stažený z jeho domovské adresy.



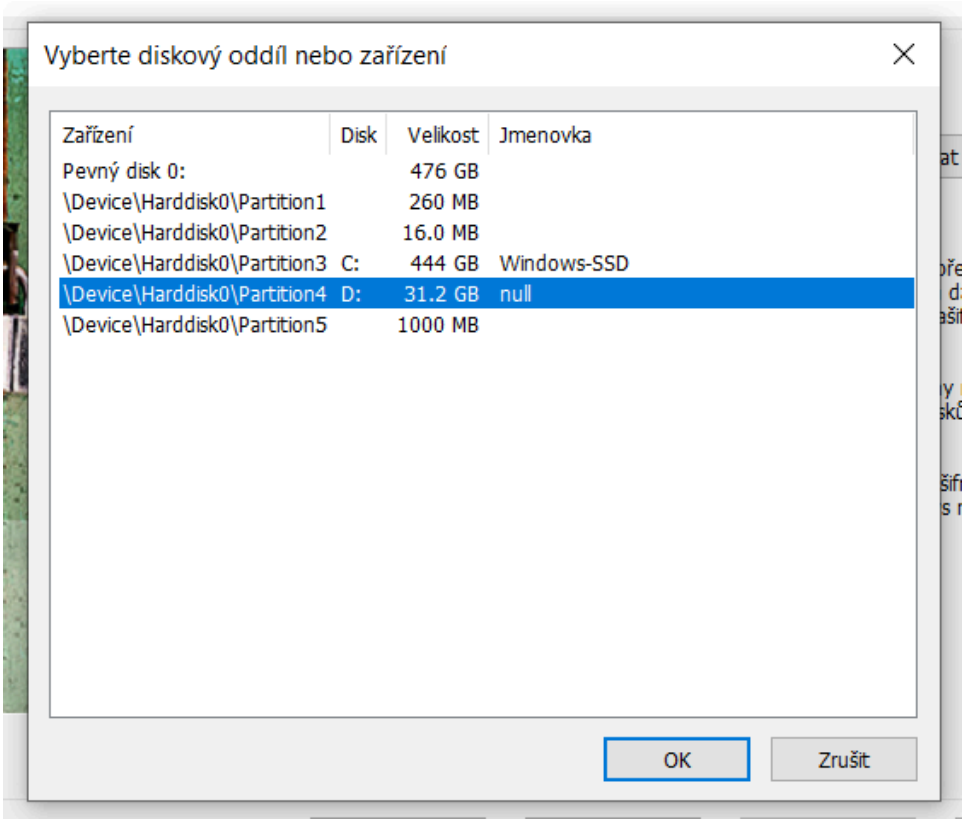
Krok 2: Po instalaci se mi nabízí seznam dostupných oddílů. K těmto oddílům mohu připojit již existující jednotky nebo virtuální jednotky *VeraCrypt*.



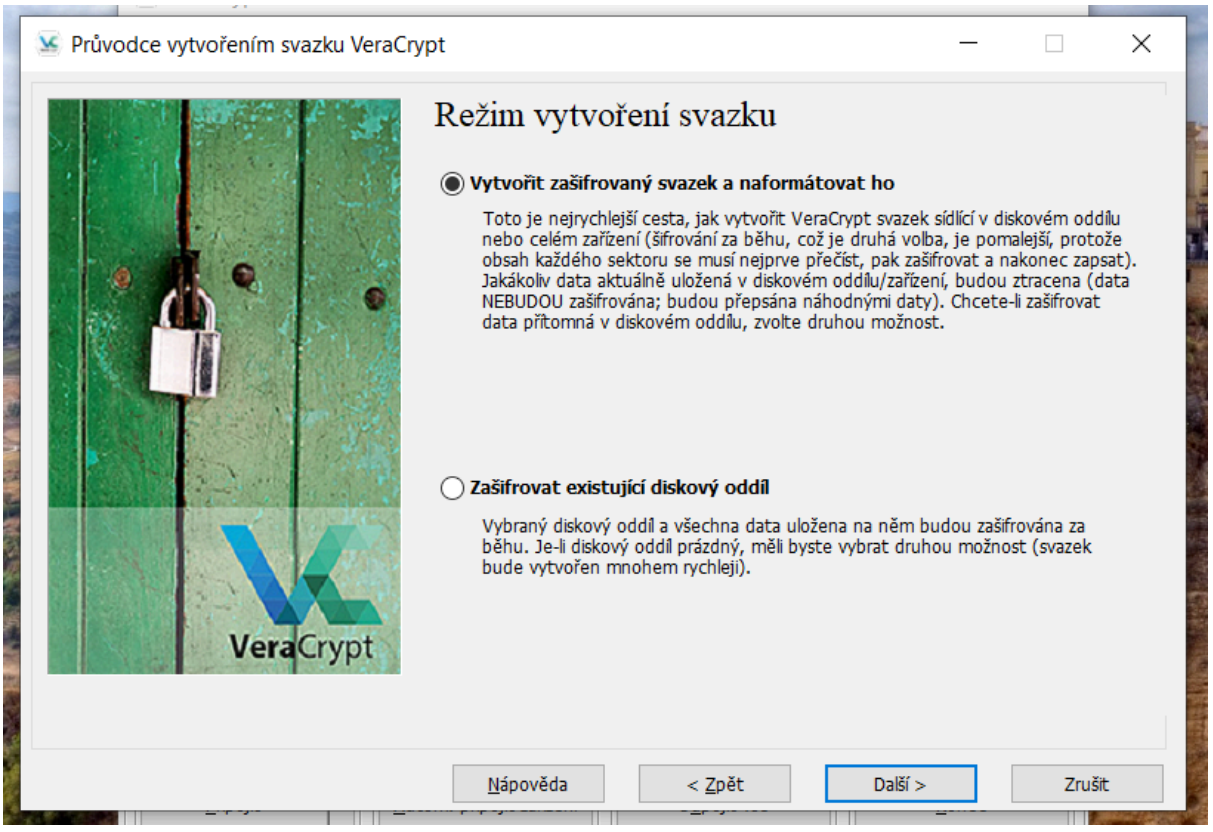
Krok 3: V průvodci volím šifrování nesystémového disku. V případě šifrování systémového disku je nutné zasahovat do bootloaderu.



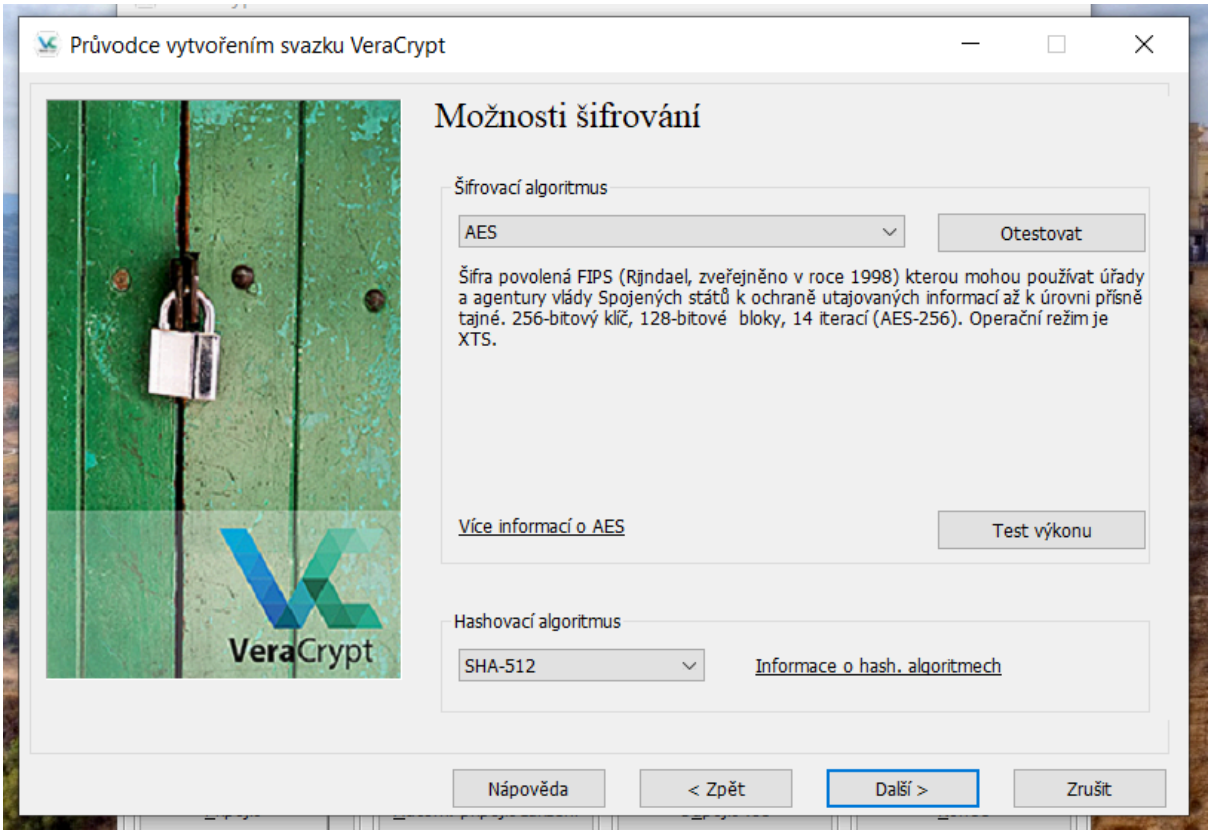
Krok 4: Volím standardní svatek *VeraCrypt*. Oddíl tedy nebude skrytý.



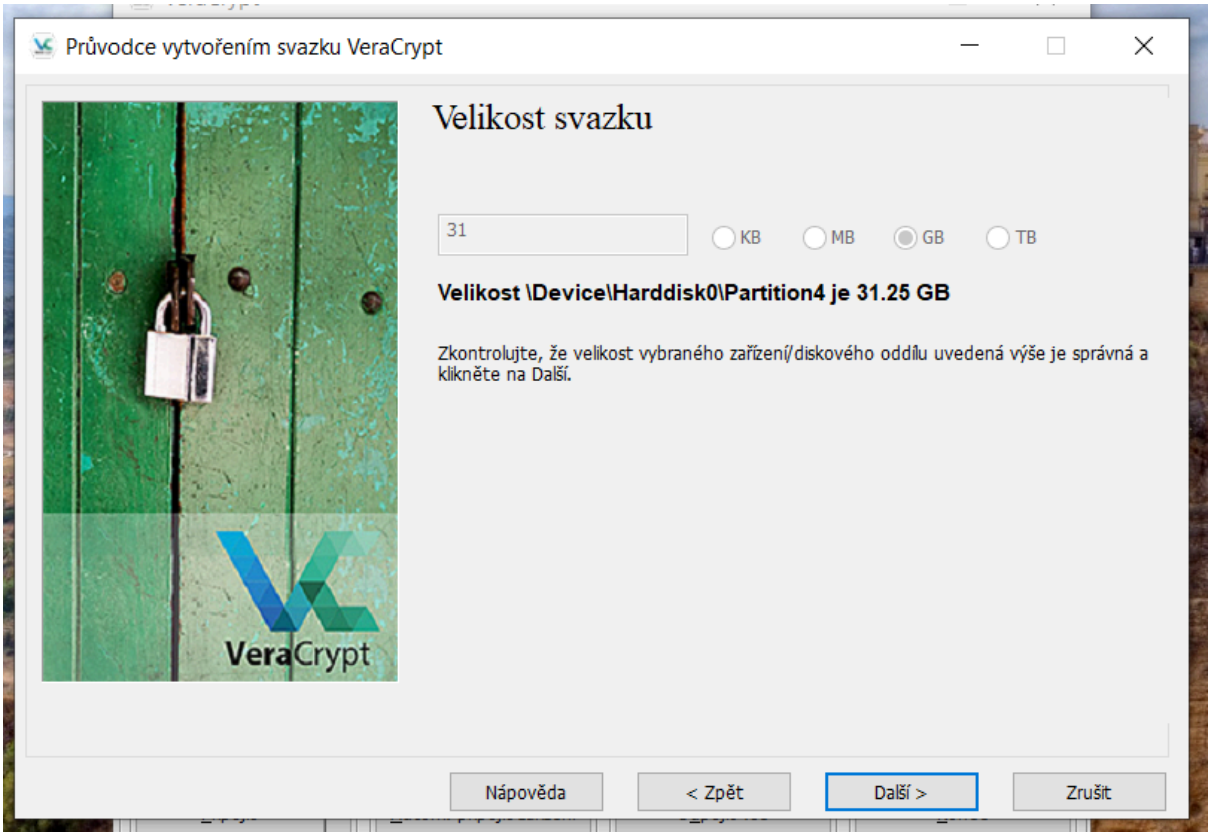
Krok 5: Volím nesystémový oddíl *D:*.



Krok 6: Na oddílu *D:* se v mém případě nenachází žádná data, disk tedy před šifrováním zformátuji.

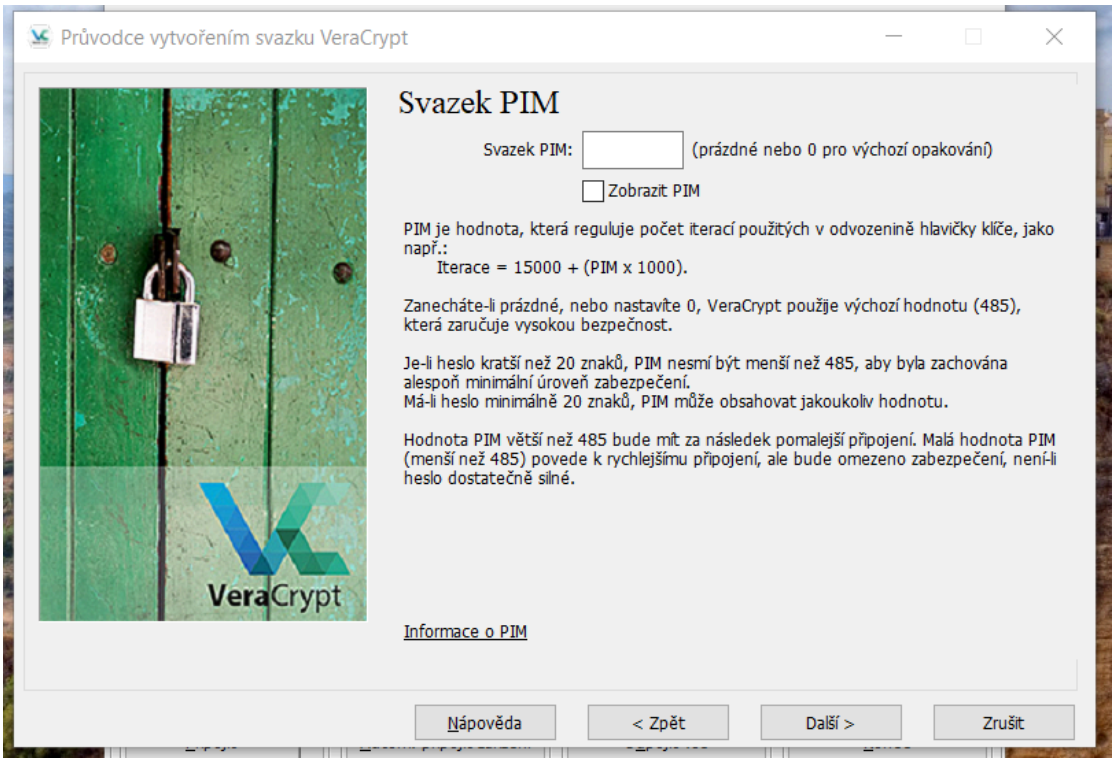


Krok 7: Volím šifrovací algoritmus *AES* v kombinaci s hashovacích algoritmem *SHA-512*.

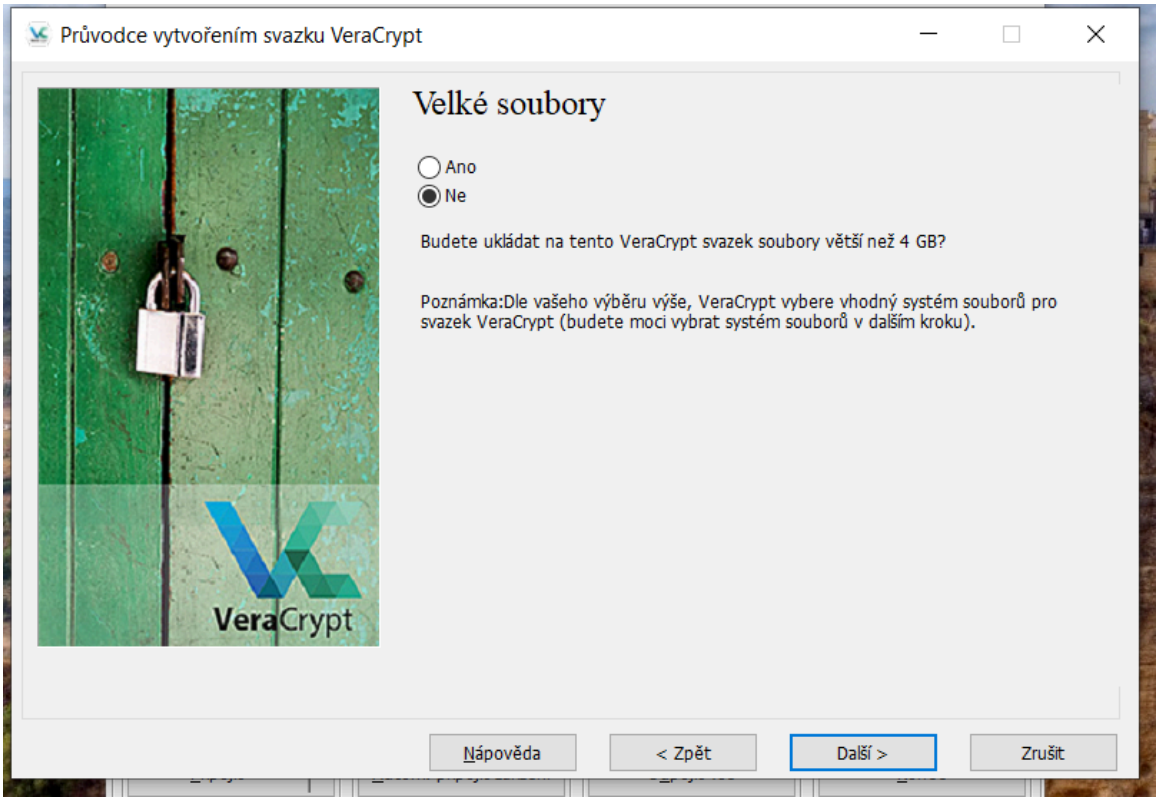


Krok 8: Velikost oddílu nechávám původní.

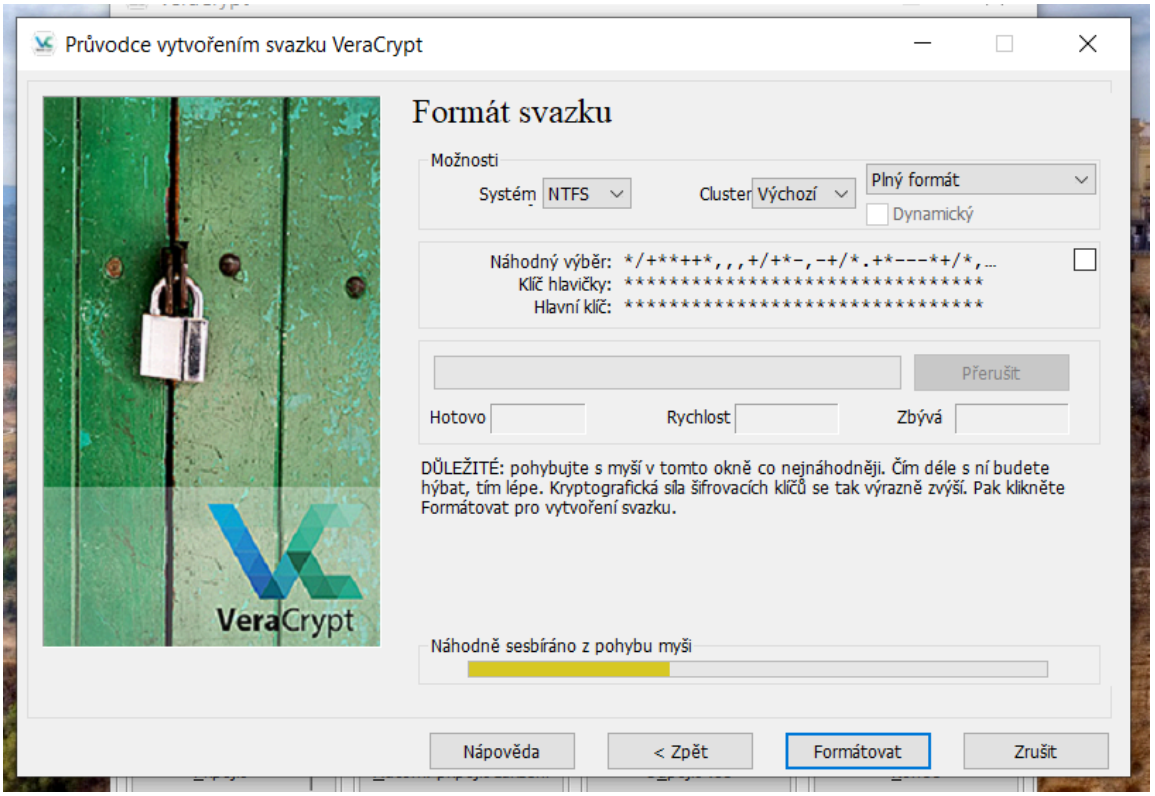
Krok 9: Volím heslo o délce 20 znaků. Pro účely prezentace je heslo triviální, pro praktické nasazení takové heslo není bezpečné.



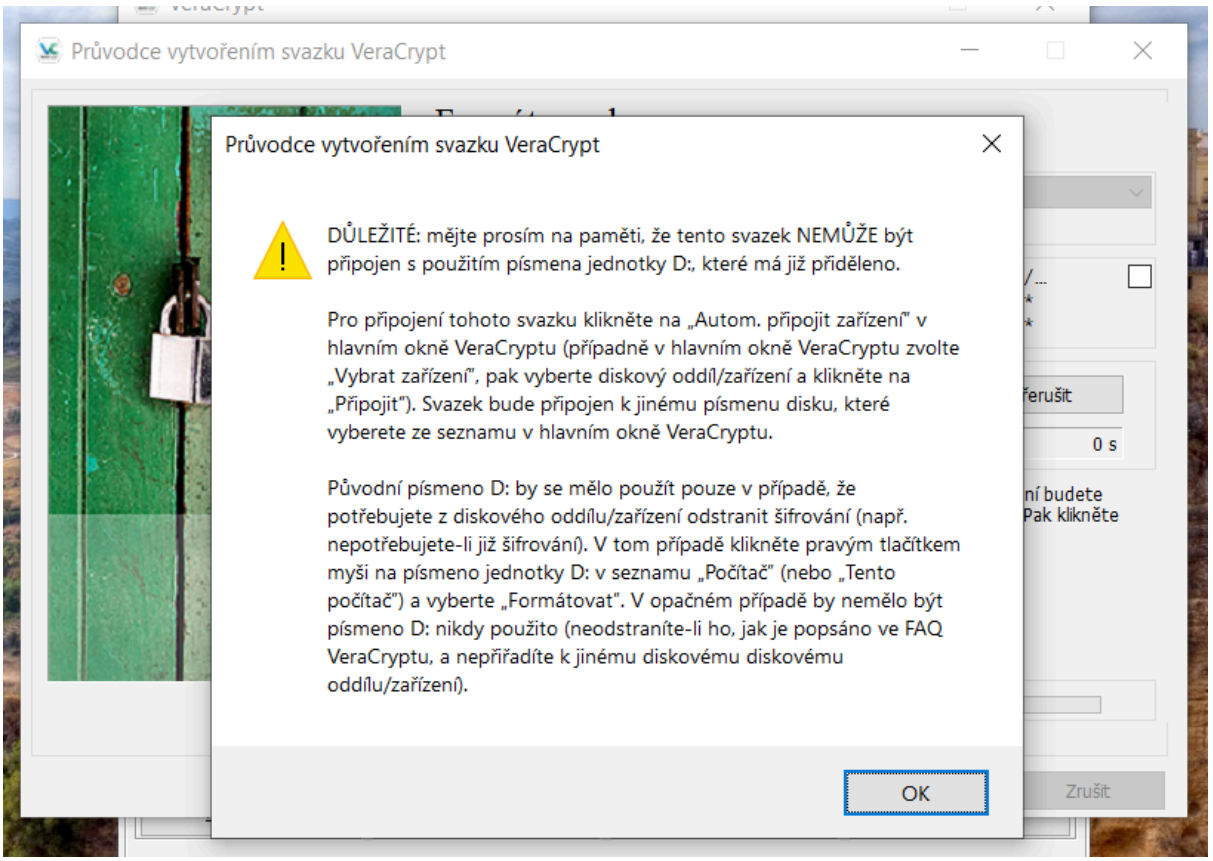
Krok 10: PIM nechávám na výchozí hodnotě.



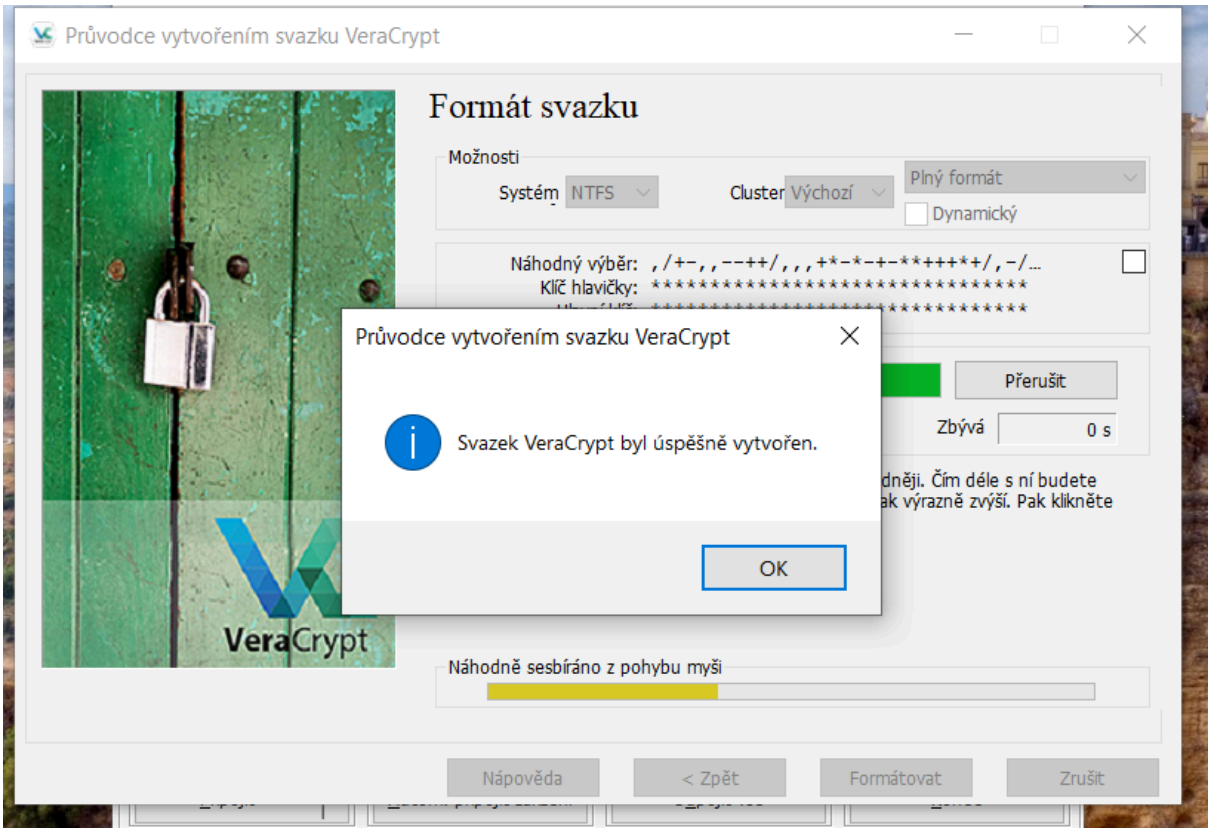
Krok 11: Neplánuji ukládat velké soubory. Tento krok ovlivňuje pouze to, jestli bude v dalším kroku defaultně vybrán souborový systém *FAT* nebo *NTFS*.



Krok 12: Vybírám specifikaci pro oddíl a jeho formátování. (Mohu změnit doporučený souborový systém *FAT* na základě předchozí kroku na *NTFS*.)

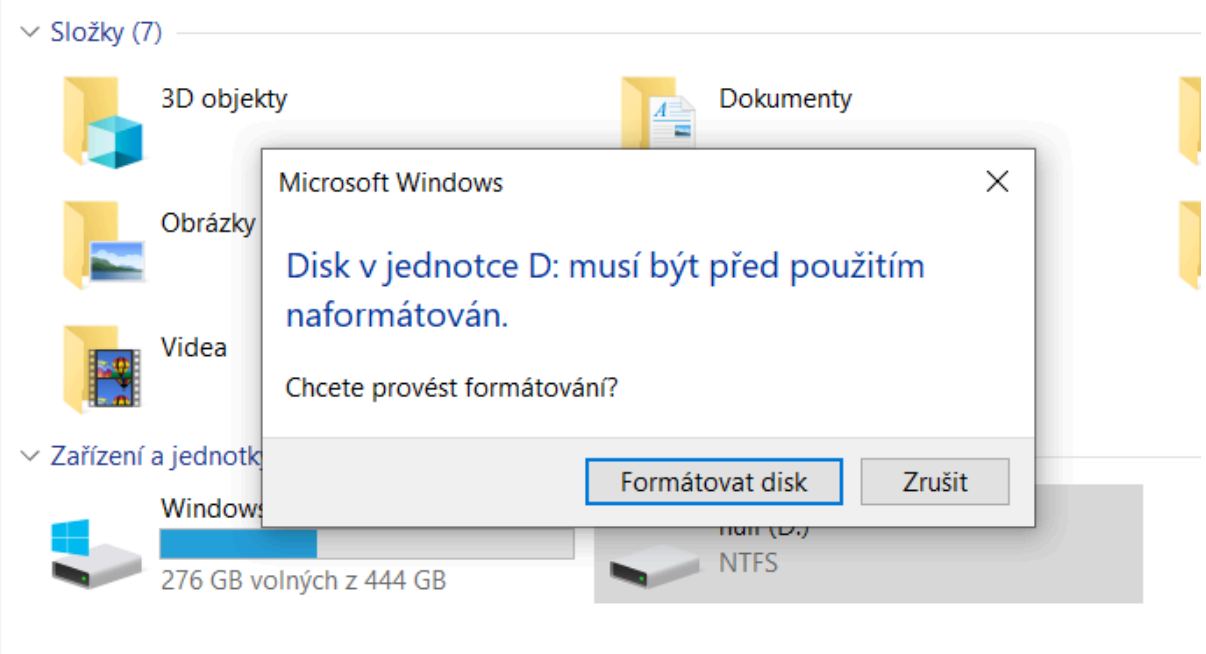


Krok 13: Upozornění ohledně formátování oddílu a následného použít.

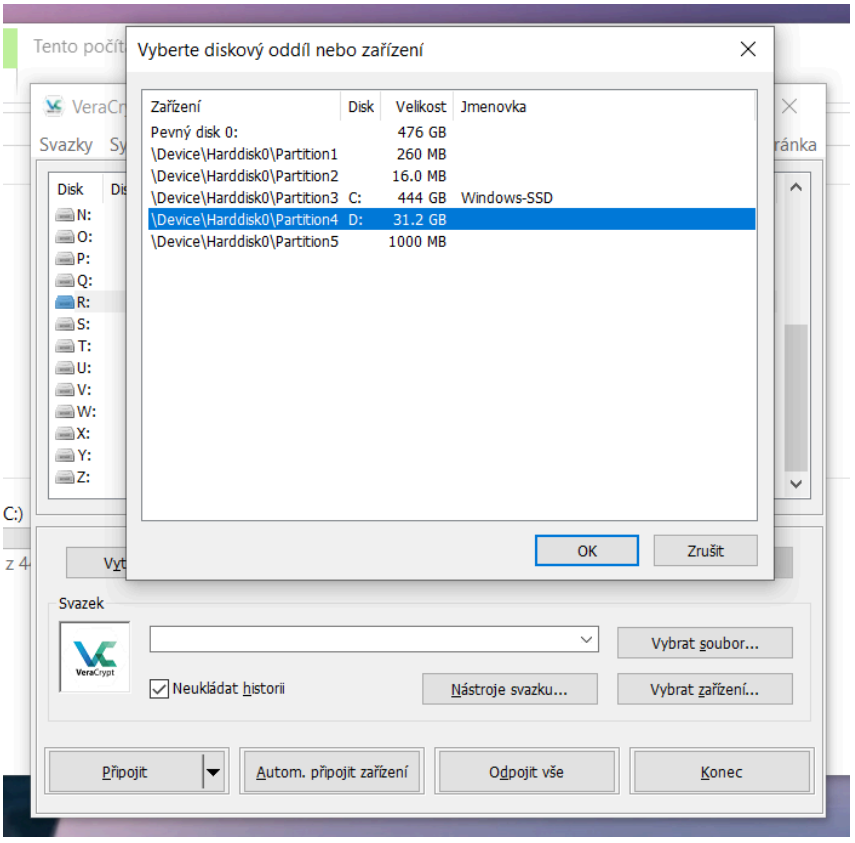


Krok 14: Šifrovaný oddíl je úspěšně vytvořen.

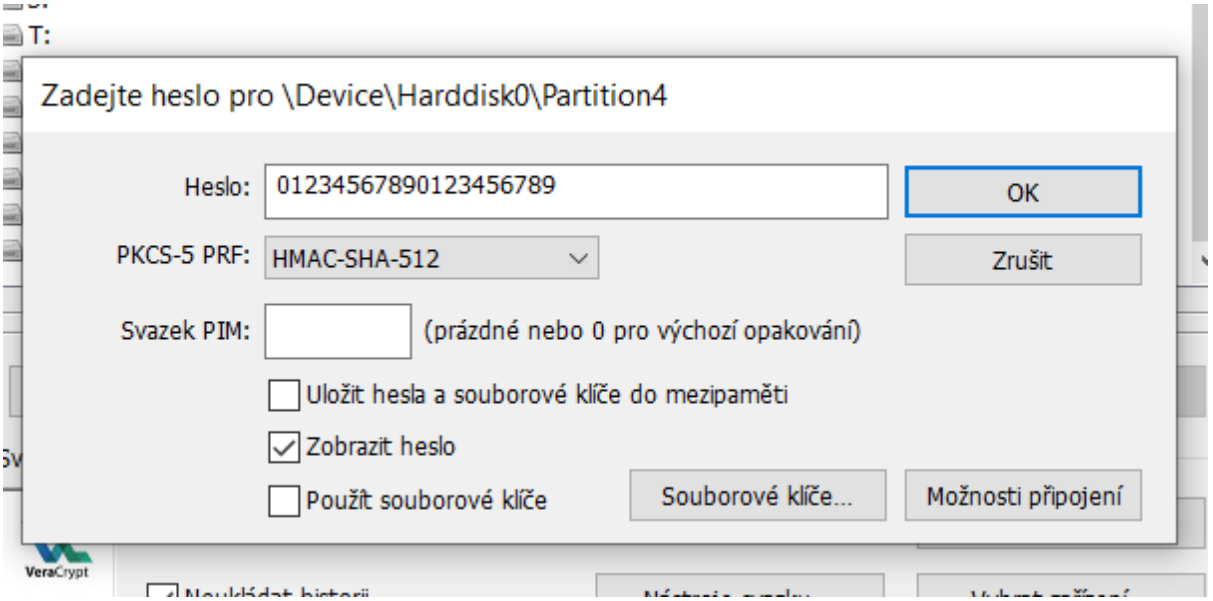
Základní ověření



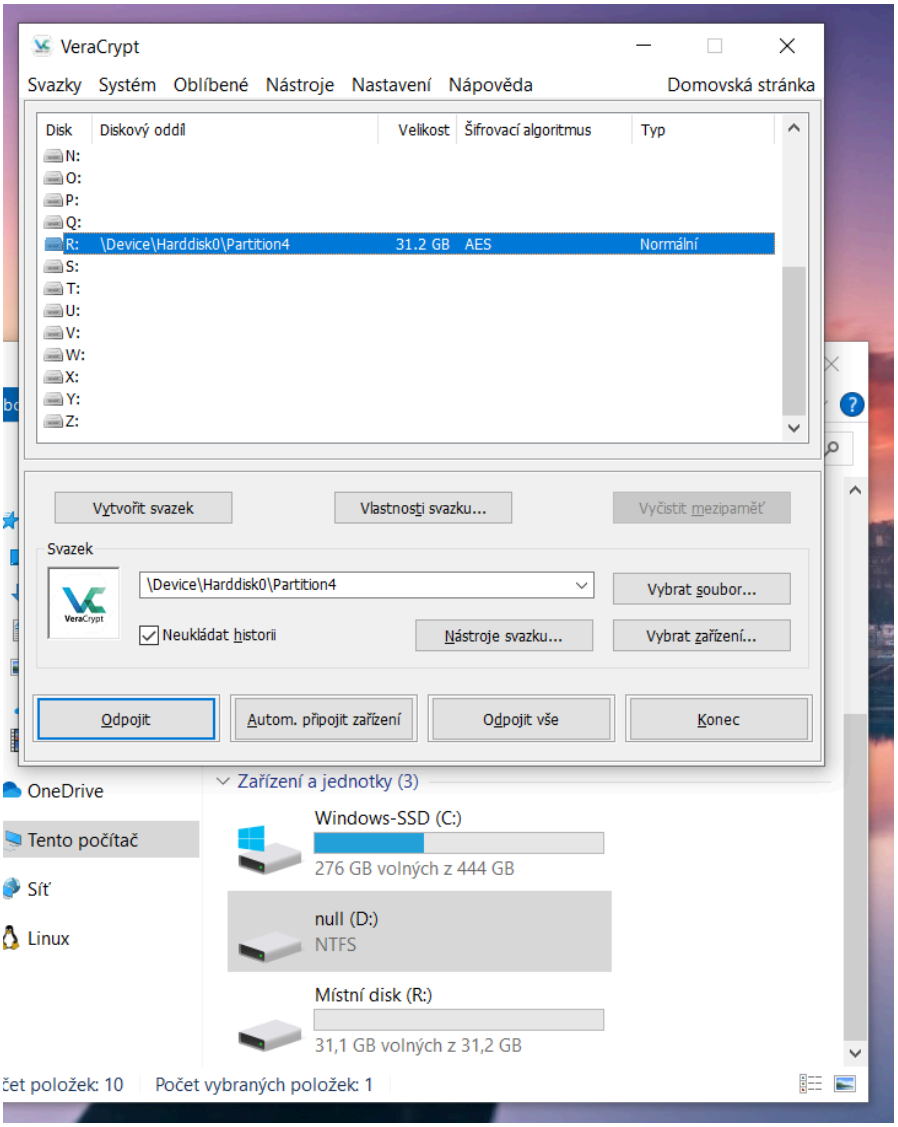
Krok 1: Oddíl není dostupný, k dispozici jsou jen nesmyslná data a *Windows* nabízí formátování.



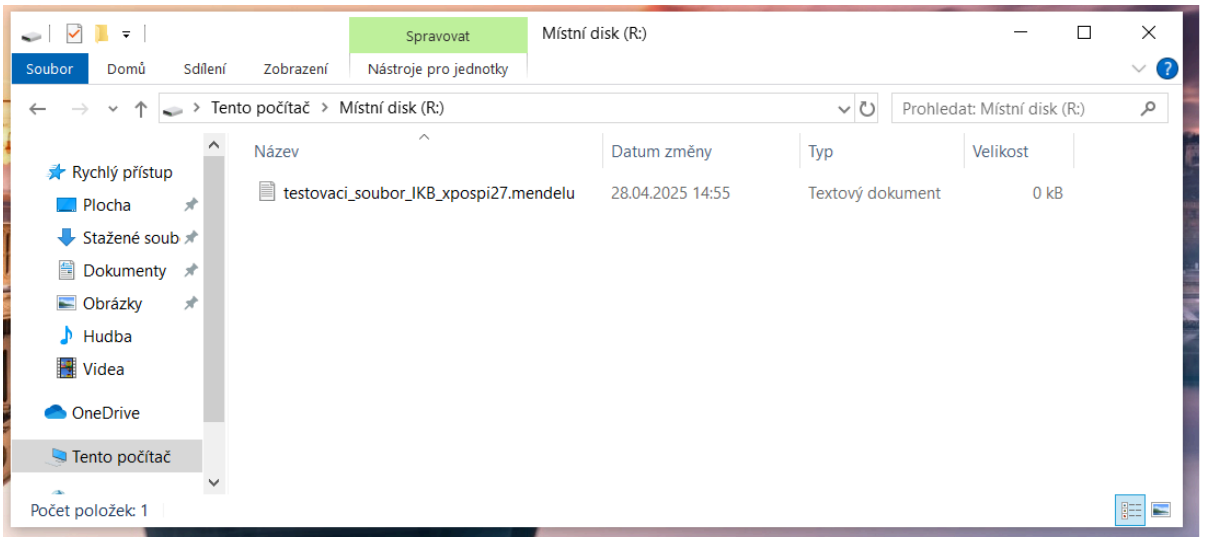
Krok 2: V seznamu oddílu *VeraCrypt* vybírám šifrovaný disk a v seznamu dostupných svazků vybírám například písmeno *R*:.



Krok 3: Zadávám potřebné informace pro dešifrování oddílu.



Krok 4: Oddíl je dešifrovaný a připojený jako oddíl *R:*.



Krok 5: Ověřuji, že se dostanu k datům uloženým na oddílu.

```
PS C:\> Get-PSDrive -PSProvide FileSystem

Name           Used (GB)     Free (GB) Provider      Root

on
----           ---------     --------- --------      ----


--
C                 168,11        276,33 FileSystem    C:\
R                   0,07         31,18 FileSystem    R:\
```

(Krok 6): Přítomnost oddílu mohu ověřit i pomocí příkazu v *PowerShellu*.

```
PS C:\> Get-PSDrive -PSProvide FileSystem

Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
C                 168,13        276,31 FileSystem    C:\
```

(Krok 7): Oddíl ve *VeraCryptu* odpojuji a ověřuji, že ani z *PowerShellu* není viditelný.