VeraCrypt

Filip Pospíšil

Co je VeraCrypt a k čemu slouží

- **Bezplatný open-source** nástroj pro **šifrování dat za běhu** (on-the-fly encryption).
- Multiplatformní řešení: dostupný pro Windows, macOS i Linux.
- Umožňuje šifrovat celé disky, oddíly i vytvářet šifrované soubory - kontejnery.
- Chrání citlivá data před neoprávněným přístupem (např. při ztrátě zařízení).

Hlavní vlastnosti a výhody VeraCrypt

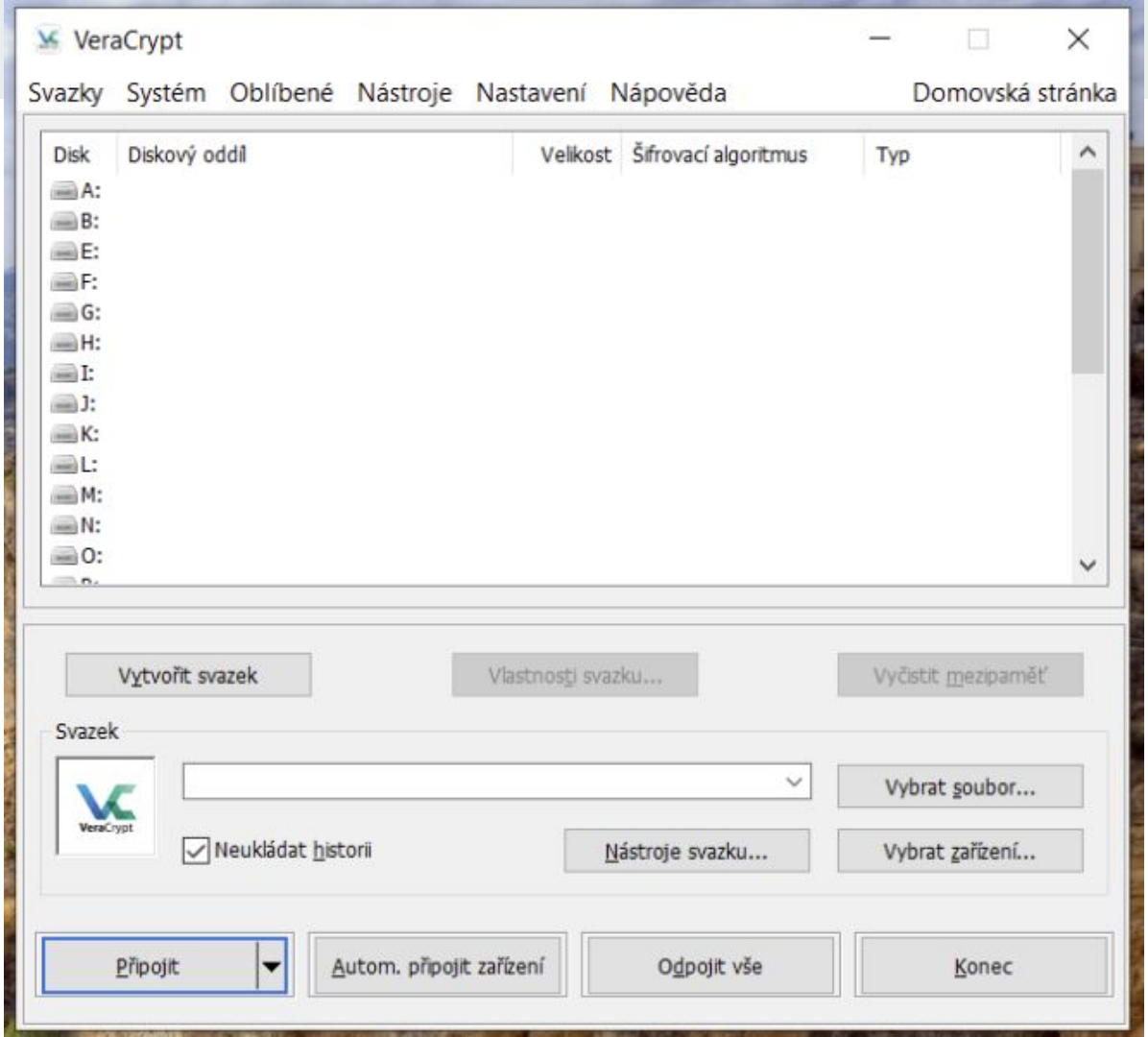
- **Silné šifrování:** Podpora algoritmů AES, Serpent, Twofish aj. (možnost kaskádování více šifer).
- **Odolnost proti prolomení:** PBKDF2 s vysokým počtem iterací (+ volitelný PIM) pro ochranu hesla hrubou silou.
- **Open-source a zdarma:** Otevřený, auditovatelný kód, žádné licenční poplatky.
- **Multiplatformní a přívětivý:** Jednotné GUI pro Windows/Linux/macOS, použití snadné díky průvodci.
- **Skryté svazky:** Možnost vytvořit skrytý šifrovaný svazek v jiném (plausible deniability).

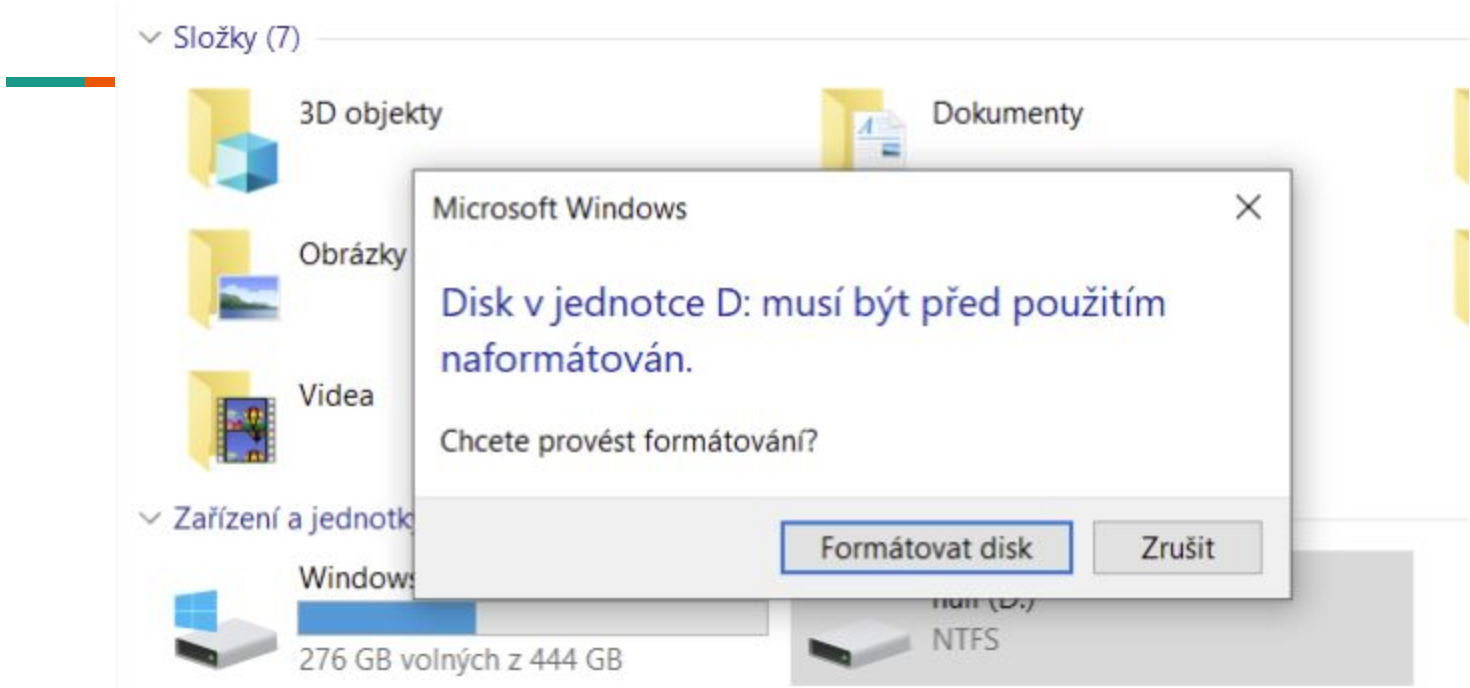
Scénáře použití a ochrana před hrozbami

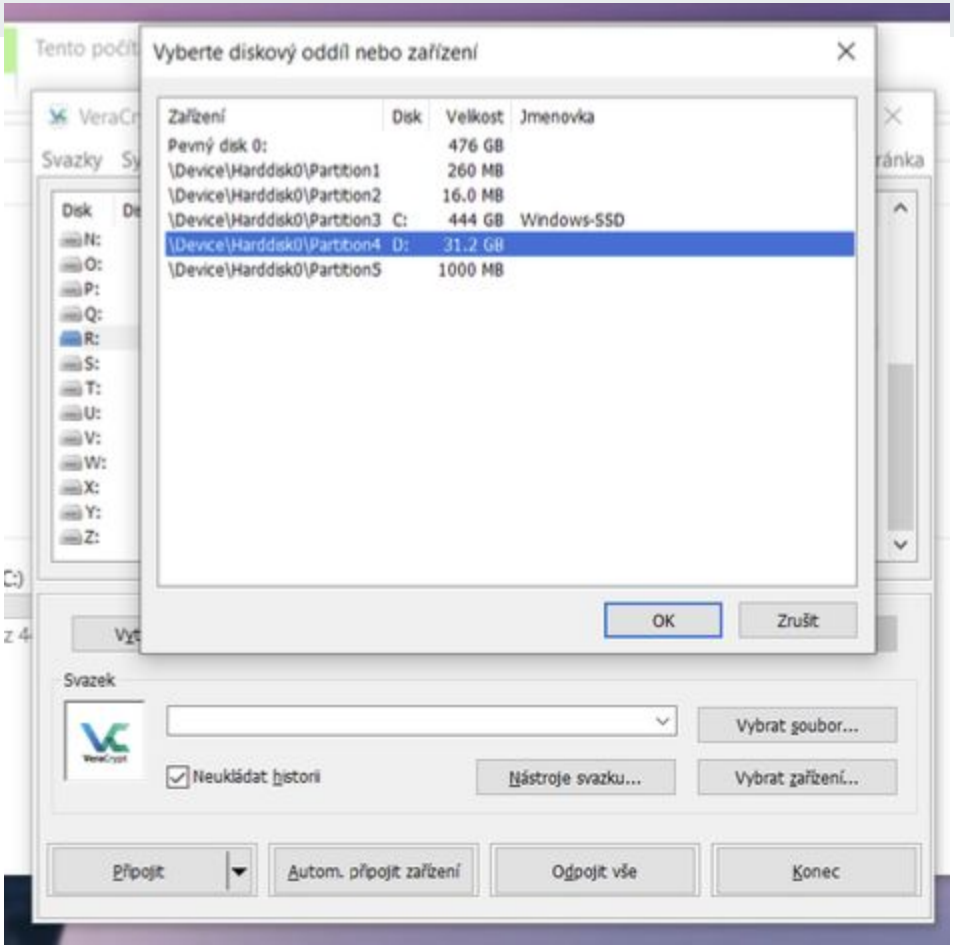
- **Ztráta nebo krádež zařízení:** Šifrování celého disku ochrání data ztraceného notebooku či flash disku.
- **Sdílený počítač:** Šifrovaný svazek uchová soukromá data nepřístupná ostatním uživatelům PC.
- **Zálohy a cloud:** Šifrované kontejnery ochrání zálohy na externích discích i v cloud úložištích.
- **Malware:** Šifrování chrání data v klidovém stavu, ale nebrání malwaru útočit na odemčená data.
- **Likvidace disku:** Při vyřazení/prodeji disku zůstávají data díky šifrování nečitelná.

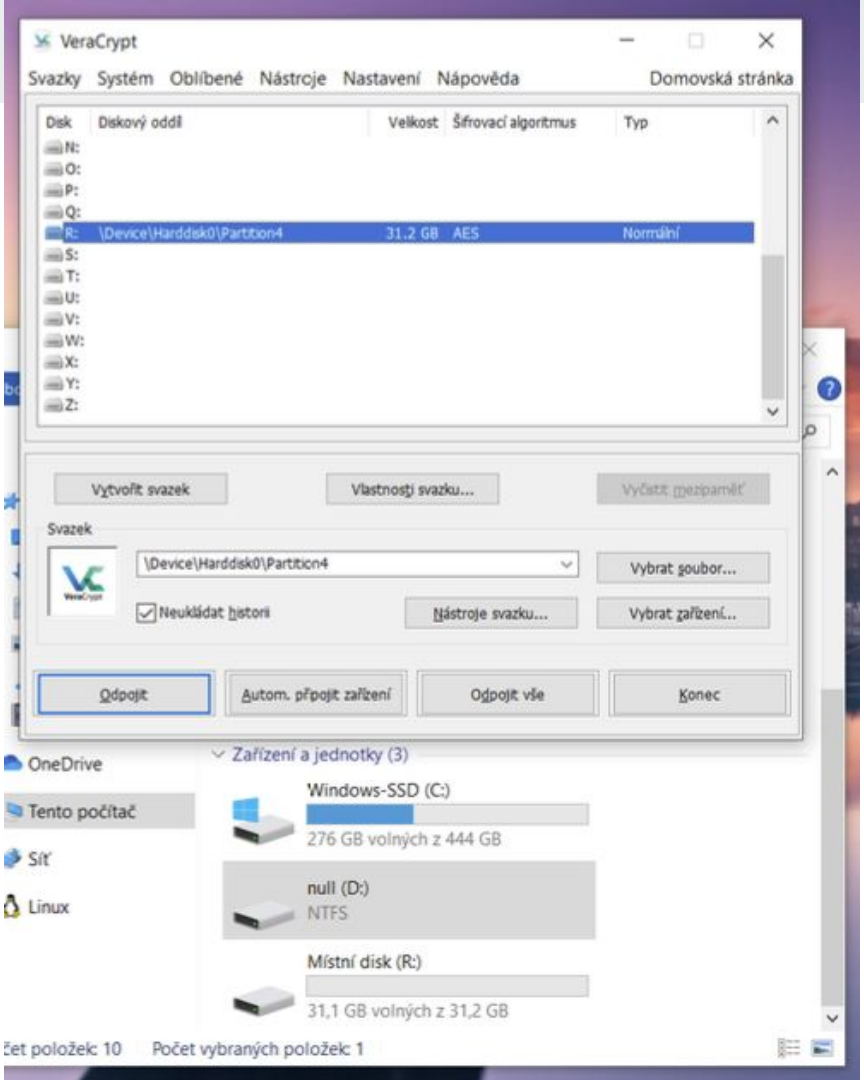
Případová studie – nasazení VeraCrypt

- **Prostředí:** Notebook s Windows 10; data původně uložena nešifrovaně na interním SSD.
- **Hrozba:** Riziko odcizení nebo neoprávněného přístupu k disku (citlivé soubory by mohl útočník číst).
- **Nasazení:** Instalace VeraCrypt a šifrování datového oddílu (D:).
- **Výsledek:** Data zůstávají chráněna i při krádeži zařízení.


VeraCrypt
Svazky Systém Oblíbené Nástroje Nastavení Nápověda Domovská stránka
Disk Diskový oddíl Velikost Šifrovací algoritmus Typ
A:
B:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
Vytvořit svazek
Vlastnosti svazku...
Vyčistit mezipaměť
Svazek
Vybrat soubor...
Neukládat historii
Nástroje svazku...
Vybrat zařízení...
Připojit
Autom. připojit zařízení
Odpojit vše
Konec


Složky (7)
3D objekty
Dokumenty
Obrázky
Videa
Zařízení a jednotk
Windows
276 GB volných z 444 GB
NTFS
Microsoft Windows
Disk v jednotce D: musí být před použitím naformátován.
Chcete provést formátování?
Formátovat disk
Zrušit


Vyberte diskový oddíl nebo zařízení
Zařízení
Disk
Velikost
Jmenovka
Pevný disk 0:
476 GB
\Device\Harddisk0\Partition1
260 MB
\Device\Harddisk0\Partition2
16.0 MB
\Device\Harddisk0\Partition3
C:
444 GB
Windows-SSD
\Device\Harddisk0\Partition4
D:
31.2 GB
\Device\Harddisk0\Partition5
1000 MB
OK
Zrušit
Svazek
Vybrat soubor...
Neukládat historii
Nástroje svazku...
Vybrat zařízení...
Připojit
Autom. připojit zařízení
Odpojit vše
Konec


VeraCrypt
Svazky Systém Oblíbené Nástrcje Nastavení Nápověda Domovská stránka
Disk Diskový oddíl Velikost Šifrovací algoritmus Typ
N:
O:
P:
Q:
R: \Device\Harddisk0\Partition4 31.2 GB AES Normální
S:
T:
U:
V:
W:
X:
Y:
Z:
Vytvořit svazek
Vlastnosti svazku...
Vyčistit mezipaměť
Svazek
\Device\Harddisk0\Partition4
Vybrat soubor...
Neukládat historii
Nástroje svazku...
Vybrat zařízení...
Odpojit
Autom. připojit zařízení
Odpojit vše
Konec
OneDrive
Tento počítač
Síť
Linux
Zařízení a jednotky (3)
Windows-SSD (C:)
276 GB volných z 444 GB
null (D:)
NTFS
Místní disk (R:)
31,1 GB volných z 31,2 GB
Počet položek: 10
Počet vybraných položek: 1

```
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.

Závěr – Shrnutí přínosů a doporučení

VeraCrypt výrazně zvyšuje důvěrnost uložených dat – i při krádeži hardware zůstávají data bezpečně šifrovaná.

Pomáhá předejít úniku informací a splnit bezpečnostní požadavky (např. legislativa GDPR) v praxi.

Password-Based Key Derivation Function 2

PBKDF2 je kryptografická funkce, která slouží k bezpečnému odvození šifrovacího klíče z hesla. Patří mezi standardy definované v RFC 8018 (dříve PKCS #5) a je široce používaná pro zvýšení bezpečnosti hesel.

Jak PBKDF2 funguje?

1. Vstup: uživatel zadá heslo (např. „mojetajneheslo“).
2. Funkce k heslu přidá náhodný „salt“ (náhodná data, která ztěžují útoky pomocí předpočítaných tabulek – tzv. rainbow tables).
3. Na kombinaci hesla a saltu opakovaně aplikuje hashovací algoritmus (např. SHA-512).
4. Počet iterací (opakování hashování) je vysoký – například 500 000 – čímž se výrazně zpomalí každé zkoušení hesla.
5. Výsledkem je odvozený šifrovací klíč, který může být použit k šifrování dat (např. AES).