Instalace OS

Windows – poinstalační nastavení

(základy bezpečnosti)

Základní poinstalační nastavení

- **Základní nastavení**
  1. Zabezpečit účet Administrátor !!!
  2. Nastavení Řízení uživatelských účtů (User Account Control)
  3. Aktualizace OS (Windows update)
  4. Základní bezpečnostní nastavení (Defender, FireWall)
  5. Vytvořit běžný účet
  6. Instalace všech potřebných aplikací
  7. Základní vyčištění systému
  8. Systém Bodu Obnovení (SBO)

Základní poinstalační nastavení

1. **Zabezpečení účtu Administrator:**
   - Defaultní účet od Microsoftu
   - 100% práva k nastavení OS
   - Po instalaci – neaktivní: nelze se přihlásit
   - Nemá nastaveno heslo: pouze ENTER!!!
   - Použití: výjimečné případy kdy „nestačí“ účet správce

Základní poinstalační nastavení

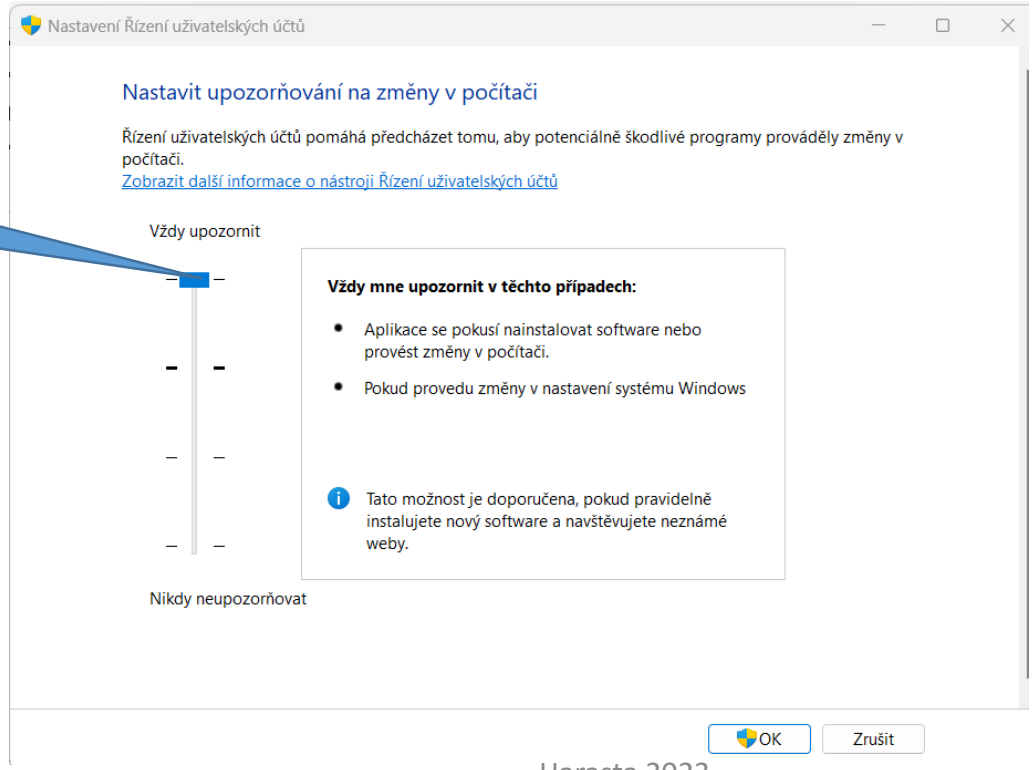
- **Aktivace účtu** (GUI/CMD – cmd.exe):
  - Spustit cmd.exe jako „správce“
  - CMD: net user administrator /active:yes
    - Účet je nabízen při přihlášení
- **Deaktivace účtu:**
  - CMD: net user administrator /active:no
    - Účet je nedostupný default - po instalaci
- **Změna hesla:**
  - CMD: net user administrator nové_heslo
    - Lze změnit i při neaktivním účtu „administrator“

Základní poinstalační nastavení

2. User Account Control (UAC):

- Vyhledat: Změnit nastavení řízení uživatelských účtů

Nastavit na nevyšší úroveň



Základní poinstalační nastavení

- **Důsledek**:
  - Ztmavnutí obrazovky při pokusu „zasáhnutí“ do systému
  - Dialog.okno: potvrdit heslem správce
    - Z běžného (bezpečnějšího) účtu
  - Okamžitá odezva:
    - snaha změnit „něco“ v systému

Základní poinstalační nastavení

- Základní obrana proti instalaci malware z internetu!!!
- Základní obrana proti instalaci malware z portable aplikací!!!
- Zásahy do OS povolujte jen u ověřeného SW!!!

Základní poinstalační nastavení

3. **Aktualizace systému:**
   - Proprietární SW - uzavřený systém
   - Neustálý zájem hackerů
   - Žádný program není 100%
     - Obsahuje slabá místa/chyby

- Aktualizace OS Windows – nutné ALE:
  - Nebezpečí u staršího HW
  - Nemusí po aktualizaci korektně fungovat
  - Ve firemním prostředí – nejprve vyzkoušet!!!

Základní poinstalační nastavení

4. Základní bezpečnostní nastavení (Defender/Firewall)

- **Defender**:
  - „Bezplatná“ antivirová ochrana od MicroSoftu
  - Detekce hrozeb v reálném čase.
  - Integrovaný firewall.
  - Rodičovská kontrola.
  - Cloudová knihovna antivirové ochrany (pro zrychlení celkového výkonu).
  - SandBox.

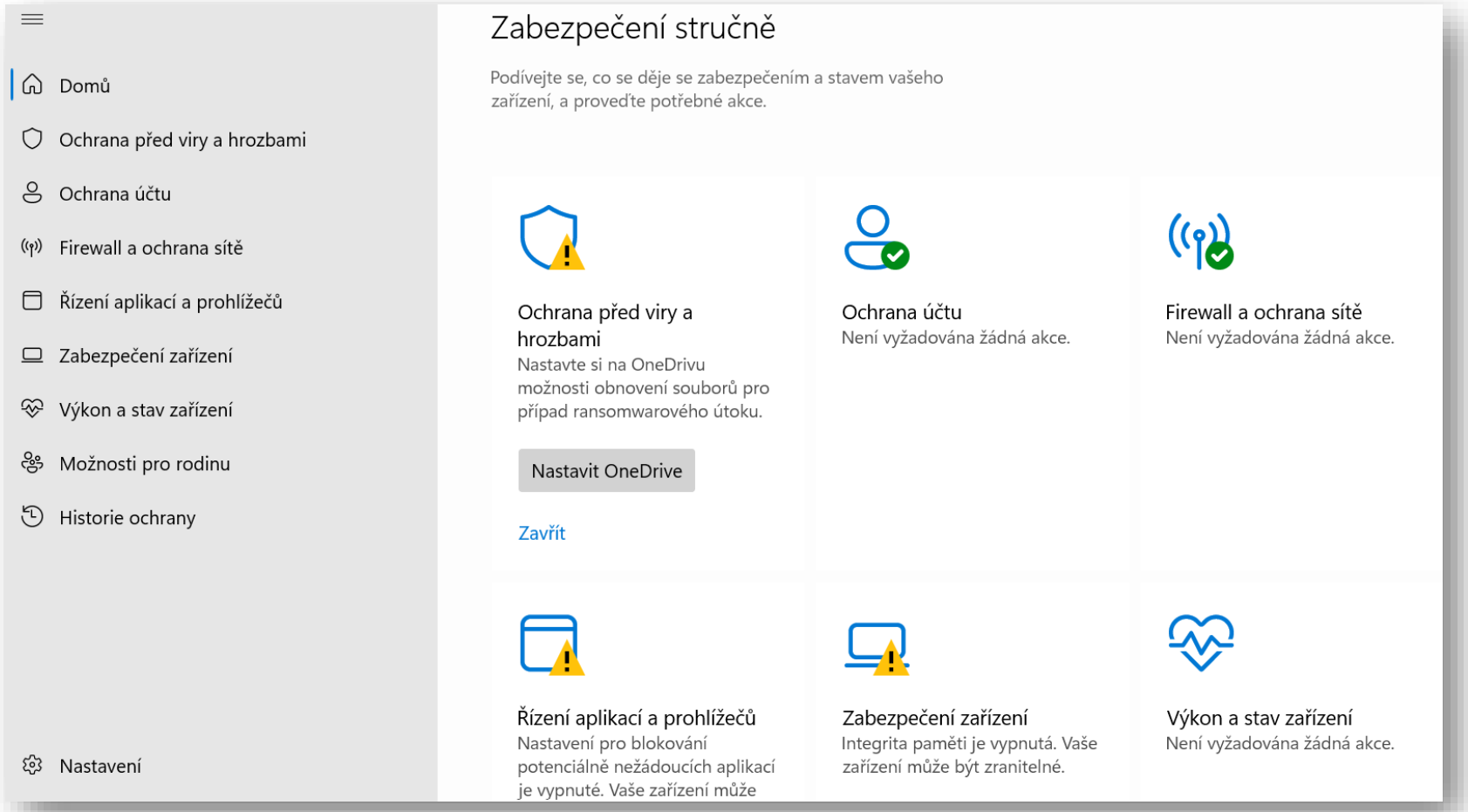
Základní poinstalační nastavení

- **Defender** – výhody:
  - Dostatečná ochrana OS
    - Integrovaná ochrana do systému
  - „Bezplatný“
  - SandBox? – defaultně vypnutý
    - Virtualizace - Izolované spouštění aplikací
    - Odděleno od OS – neovlivní „hostitelský“ OS
    - Po ukončení aplikace – vše se „vymaže“
    - Minimálně 4 GB paměti RAM (doporučeno 8 GB)
    - Minimálně 1 GB volného místa na disku (doporučen disk SSD)
    - Minimálně 2 jádra procesoru (doporučena 4 jádra s technologií HyperThreading)

Základní poinstalační nastavení

- **Defender** – nevýhody:
  - Není tak úspěšný jako specializovaný SW 3.stran
    - Aktualizace databází – není tak častá
  - Nemá VPN
    - Virtual Privat Network
  - SandBox – zatím v testovacím režimu? (defaultně zatím vypnutý)

Základní poinstalační nastavení



Základní poinstalační nastavení

- **Alternativy Defenderu:**
- Bezplatné:
  - Bitdefender free
  - Avira free security
  - Panda free antivirus
  - TotalAV free antivirus
  - Malwarebytes free

Základní poinstalační nastavení

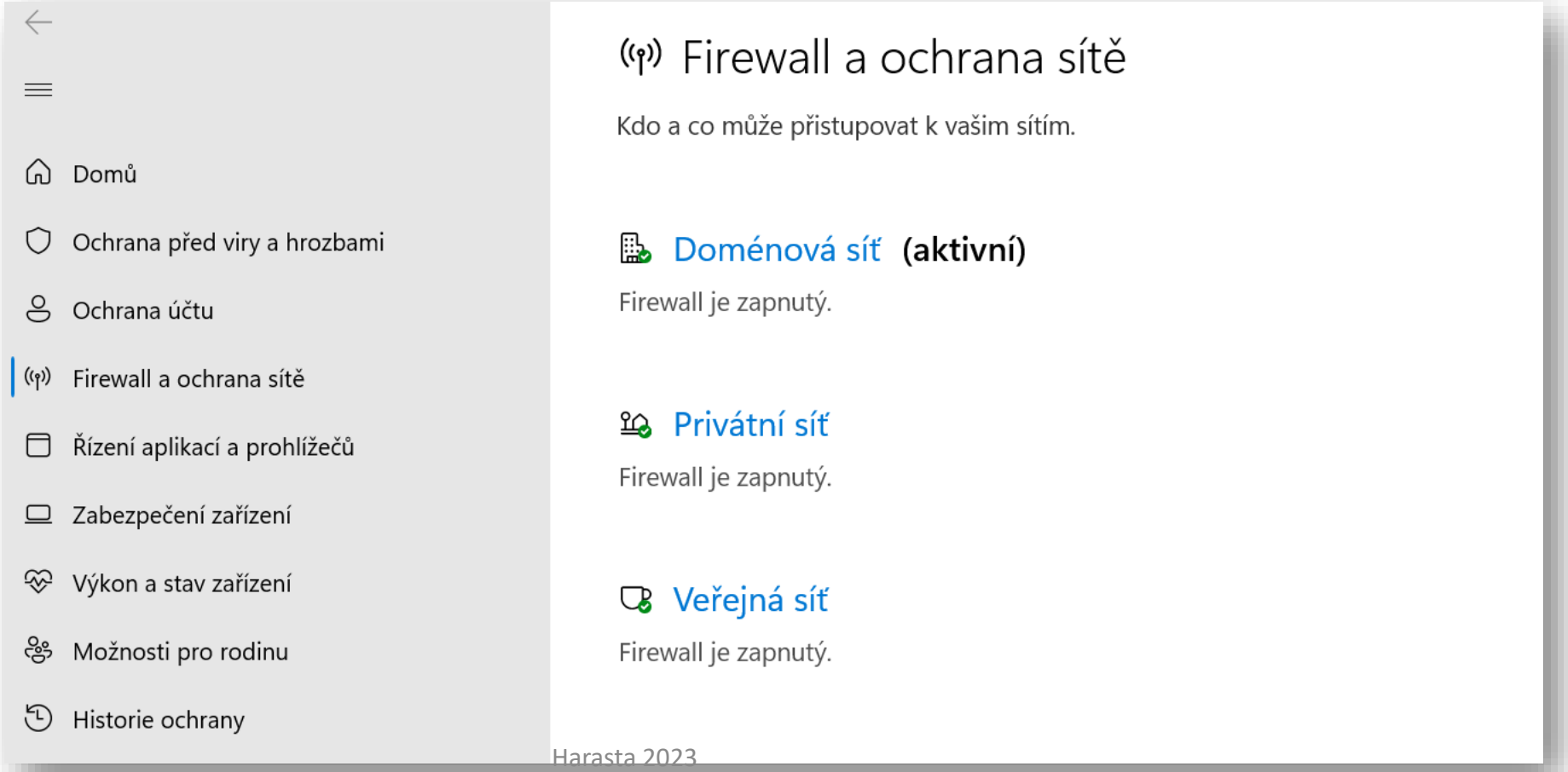
- **Alternativy Defenderu:**
- Placené (2023):
  - BitDefender
  - Norton Antivirus
  - Avast
  - AVG
  - Eset

Základní poinstalační nastavení

- **Firewall – součást Defenderu:**
  - Nechrání před viry
  - Kontroluje „komunikaci“ mezi programy (Server – klient)
    - Služby – porty (protokoly)
    - IPAdresy
  - Základní síťová ochrana

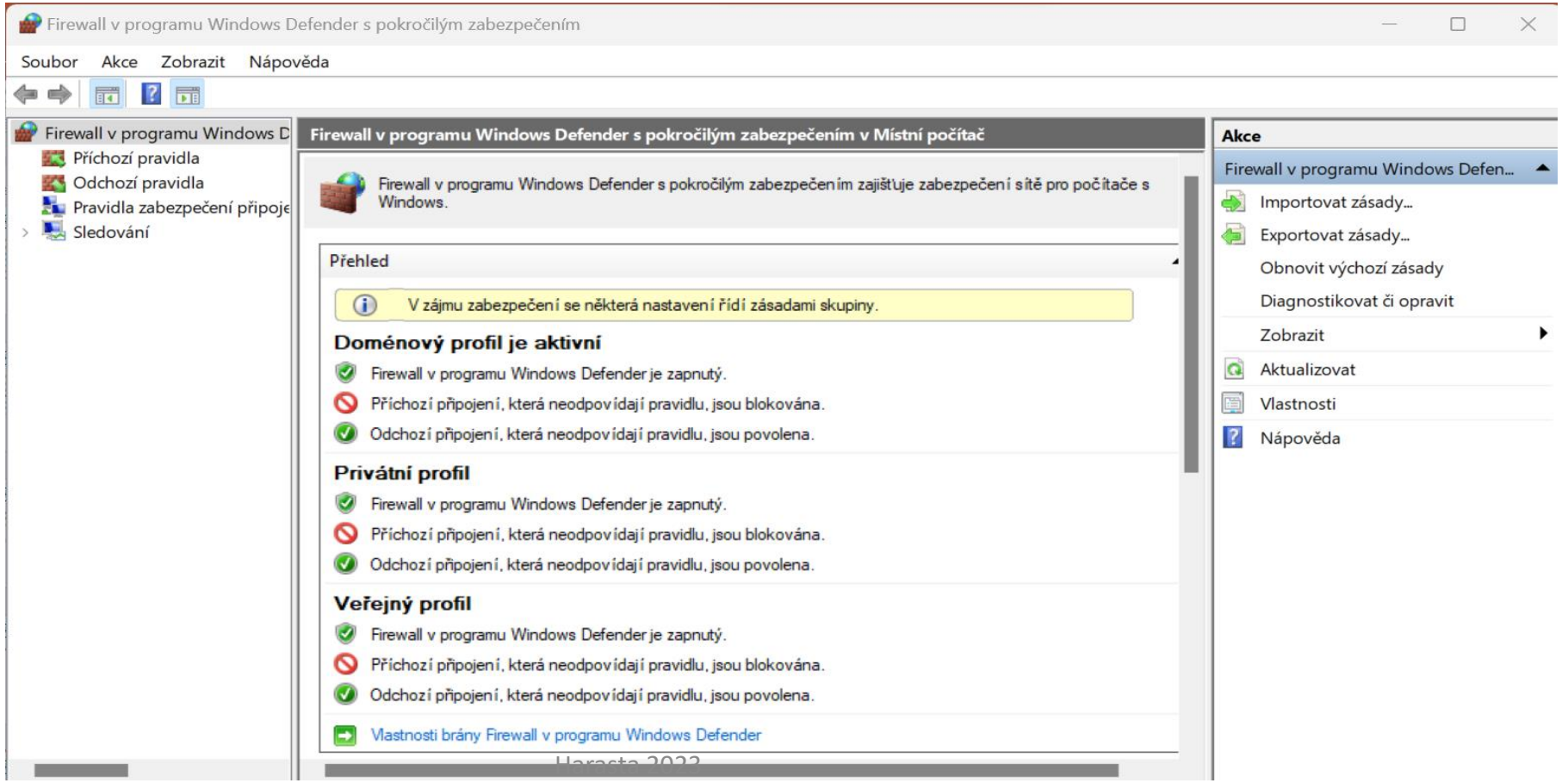
Základní poinstalační nastavení

- **Firewall** – základní nastavení:



Základní poinstalační nastavení

- **Firewall** – pokročilé nastavení:



Základní poinstalační nastavení

5. **Vytvořit běžný účet** (lokální „standardní“ účet):
   - Omezená práva – zvýšená bezpečnost
   - Nemůže měnit důležitá nastavení OS
   - Zcela dostačující pro práci s PC:
     - V kombinaci s UAC
     - Lze provádět většinu činností – známe-li heslo správce
- Vytvoření cmd.exe:
  - Spustit CMD jako správce!!! (potvrdit heslem správce)
  - **net user** nazev_uctu heslo **/add**
- Zrušení:
  - **net user** nazev_uctu **/del**

Základní poinstalační nastavení

- Standardní účet:
  - Ve skupině „Users“
  - net localgroup – výpis existujících skupin
  - net localgroup Users – výpis členů skupiny Users
- Vytvoření / zrušení nové skupiny:
  - net localgroup xxx /add – vytvoření nové skupiny xxx
  - net localgroup xxx /delete – zrušení nové skupiny xxx
- Přidání účtu do skupiny:
  - net localgroup xxx yyy /add – přidání účtu yyy do skupiny xxx
  - Účet yyy a skupina xxx musí existovat

Základní poinstalační nastavení

- Vytvoření administrátorského účtu:
  - Vytvořit standardní účet
  - Přidat účet do skupiny „Administrators“

- Př.:
  - net user milan heslo /add – vytvoření účtu milan (psw:“heslo“)
  - net localgroup administrators milan /add
- Odebrání administrátorských práv:
  - net localgroup administrators milan /delete

Základní poinstalační nastavení

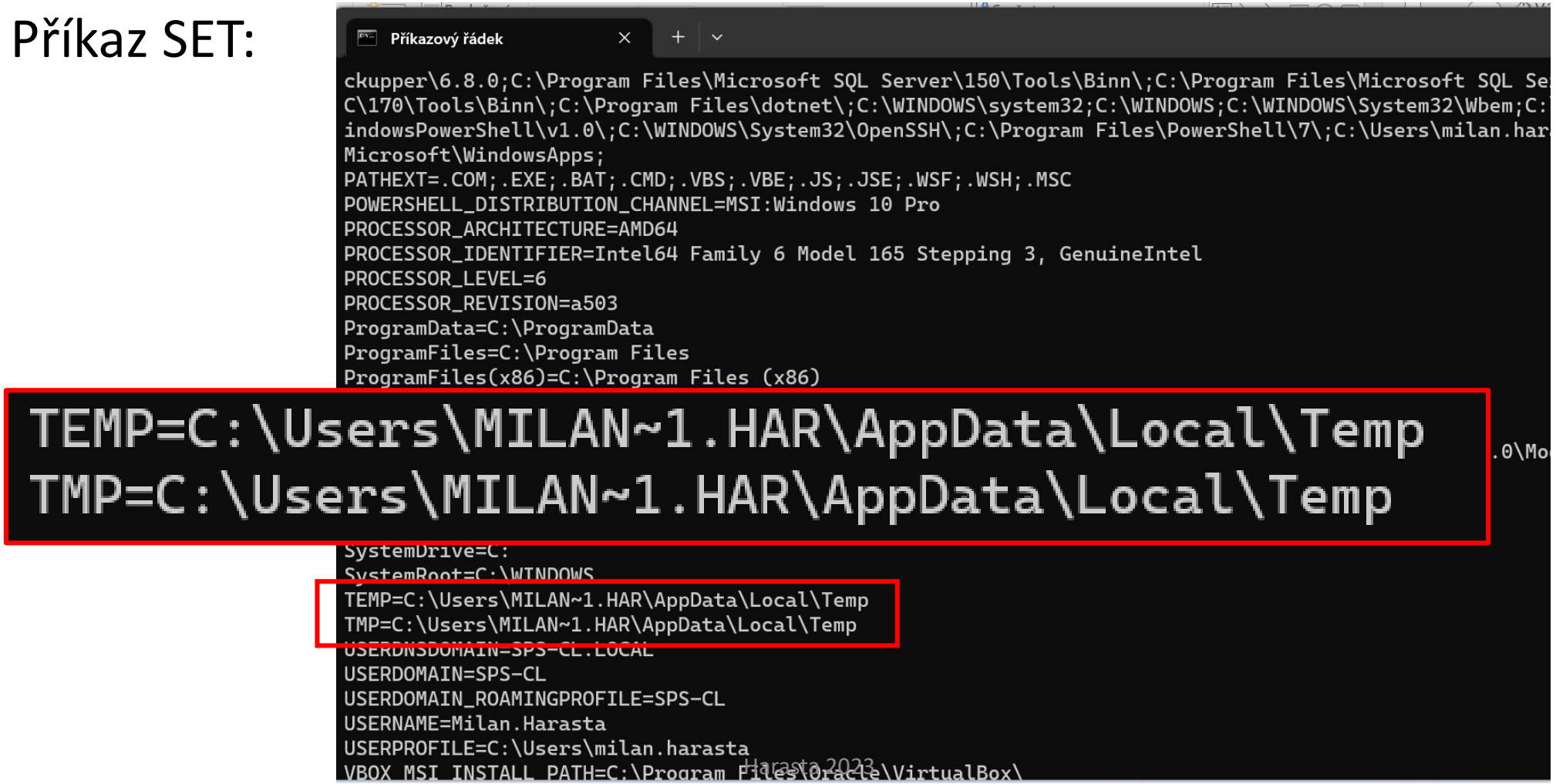
6. Instalace všech potřebných aplikací
   - Můžeme instalovat ve „Standardním“ účtu
     - Potvrdíme heslem správce (UAC)
   - Některé aplikace – vyžadují instalaci ve „Správcovském“ účtu
- Většina aplikací:
  - Multiuživatelské instalace
  - Aplikace dostupné i pro „budoucí“ účty

Základní poinstalační nastavení

7. Základní vyčištění systému
   - Nepotřebné soubory:
   - Instalační soubory aktualizací OS
   - :
     - C:\Users\<účet>\Stažené
   - Dočasné „pracovní“ soubory
     - Systémové
     - Aplikační (tempy, cache…)

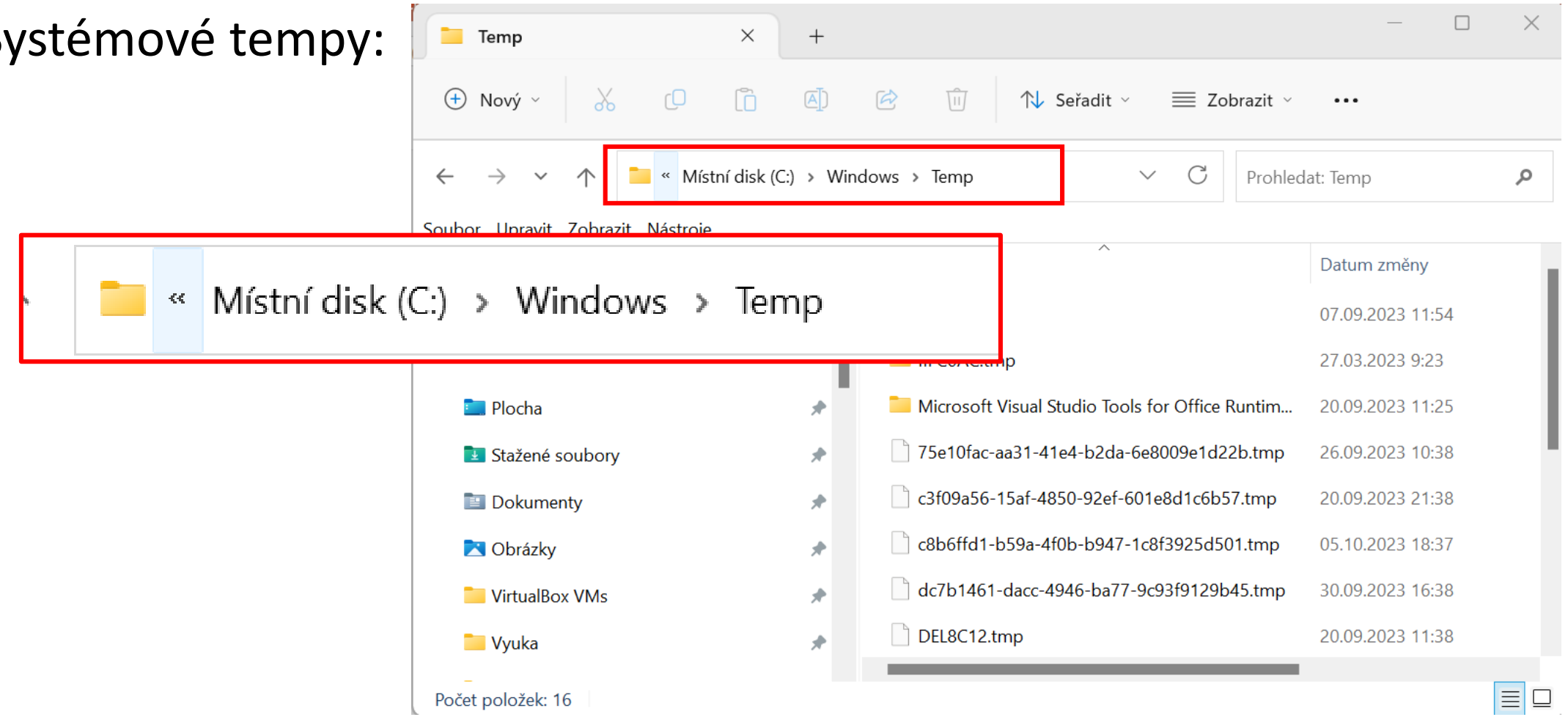
Základní poinstalační nastavení

- Příkaz SET:



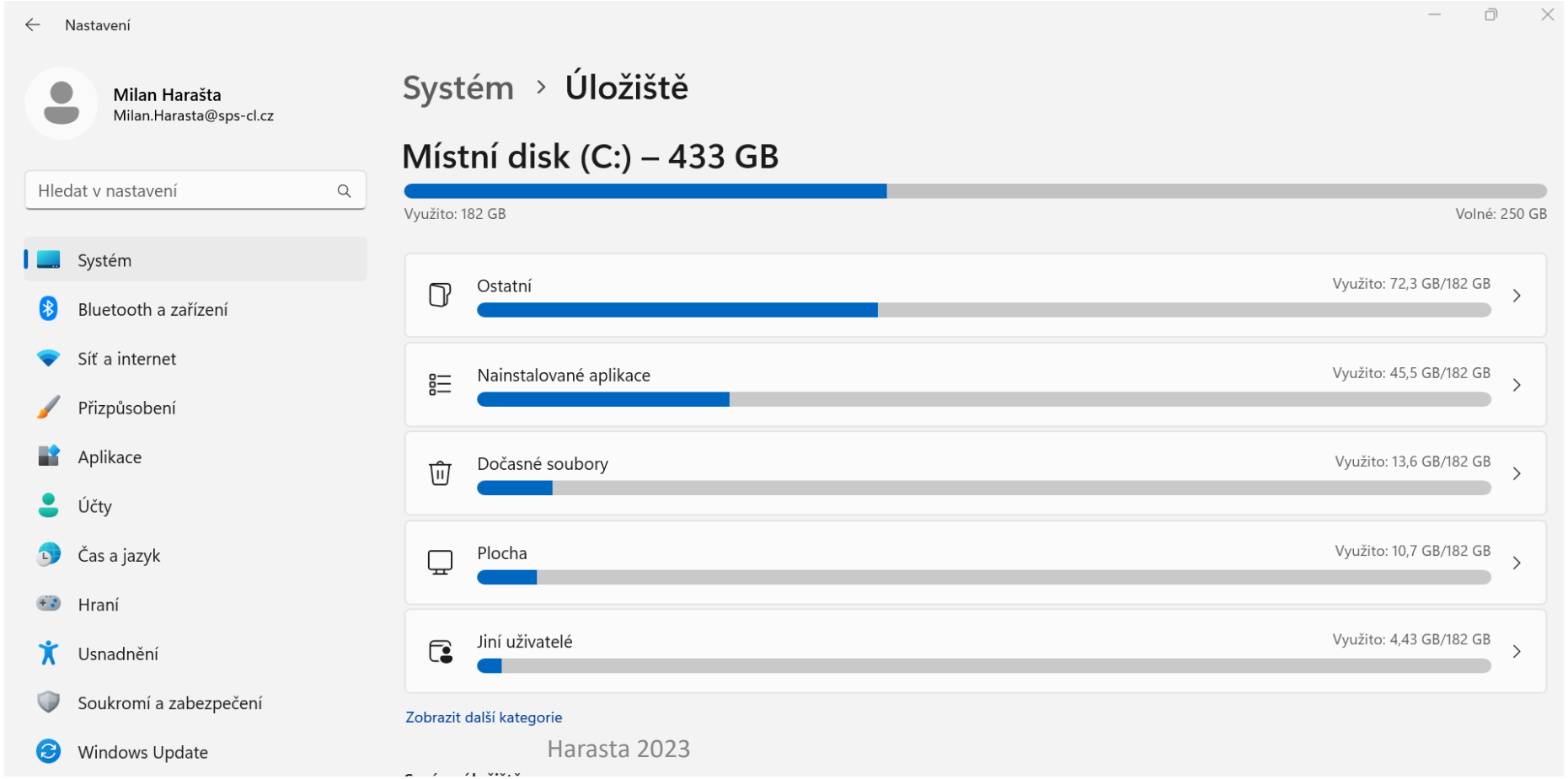
Základní poinstalační nastavení

- Systémové tempy:



Základní poinstalační nastavení

- Čištění OS Windows (1)

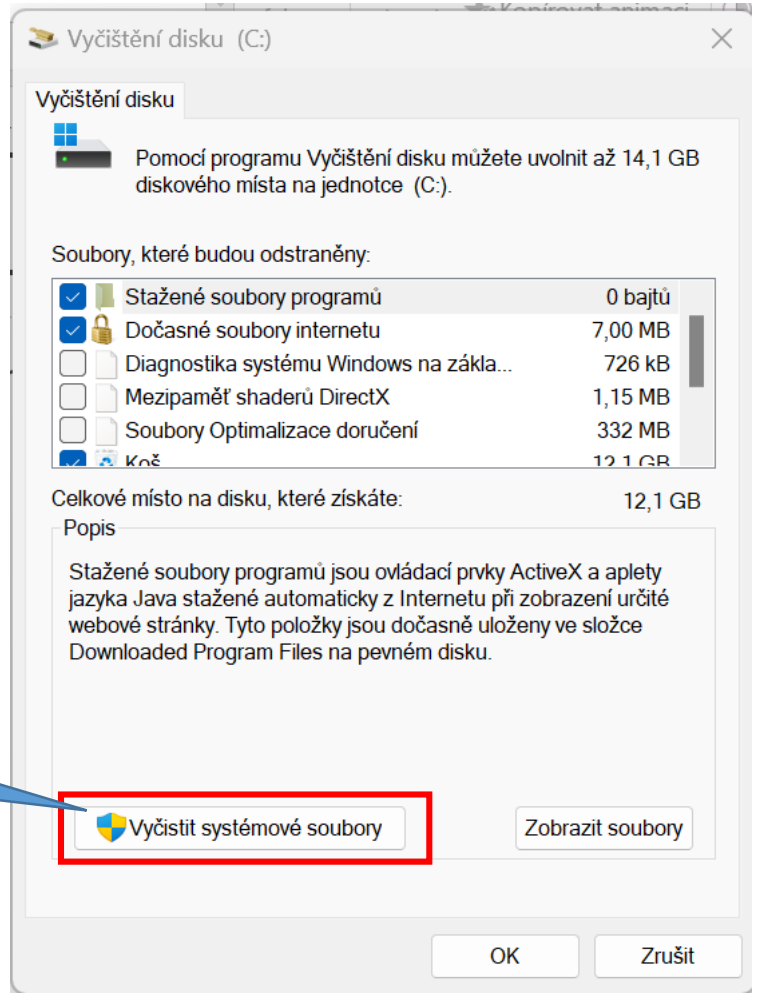


Harasta 2023

Základní poinstalační nastavení

- Čištění OS Windows(2): cleanmgr.exe

Soubory aktualizací, SBO…



Základní poinstalační nastavení

- Čištění OS Windows(3): SW 3.stran
  - Ccleaner
  - Glary Utilities
  - …

Základní poinstalační nastavení

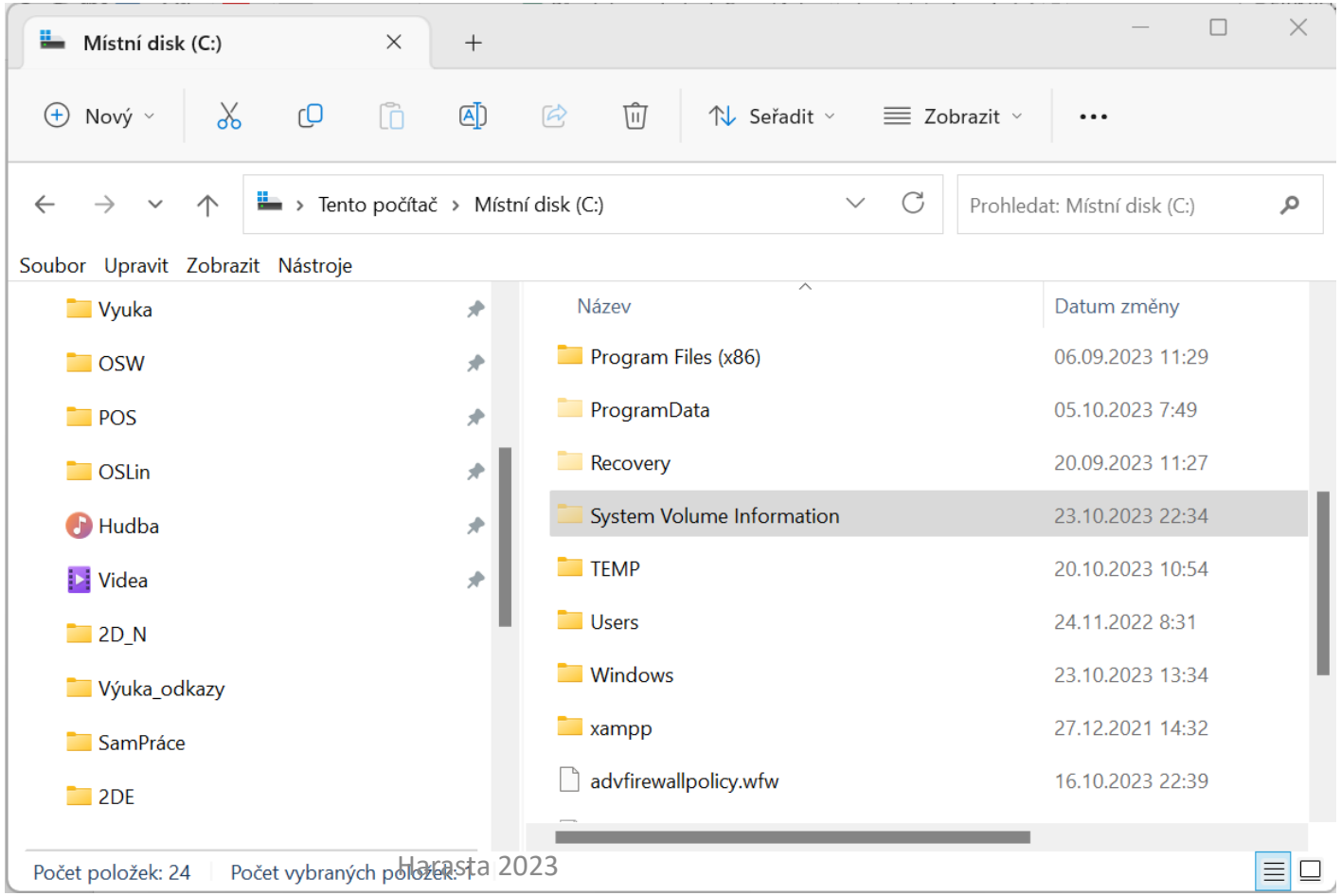
8. Systém Bodů Obnovení (SBO):
   - Vytváření „bodů obnovení“ při instalaci:
     1. nové aplikace,
     2. ovladače
     3. aktualizace Windows
     4. a při ručním vytvoření bodu obnovení
   - Obnovení neovlivní osobní soubory
   - Odeberou se aplikace, ovladače a aktualizace:
     - Nainstalované po vytvoření bodu obnovení

Základní poinstalační nastavení

- SBO:
  - Nejjednodušší způsob řešení problémů s OS
- **!!!:**
  - Je-li OS zavirován:
  - Netušíme kdy k napadení došlo
  - Pravděpodobně zavirovány i body obnovy
  - Před odvirováním – vymazat body obnovy!
    - Jinak odvirování – neúčinné

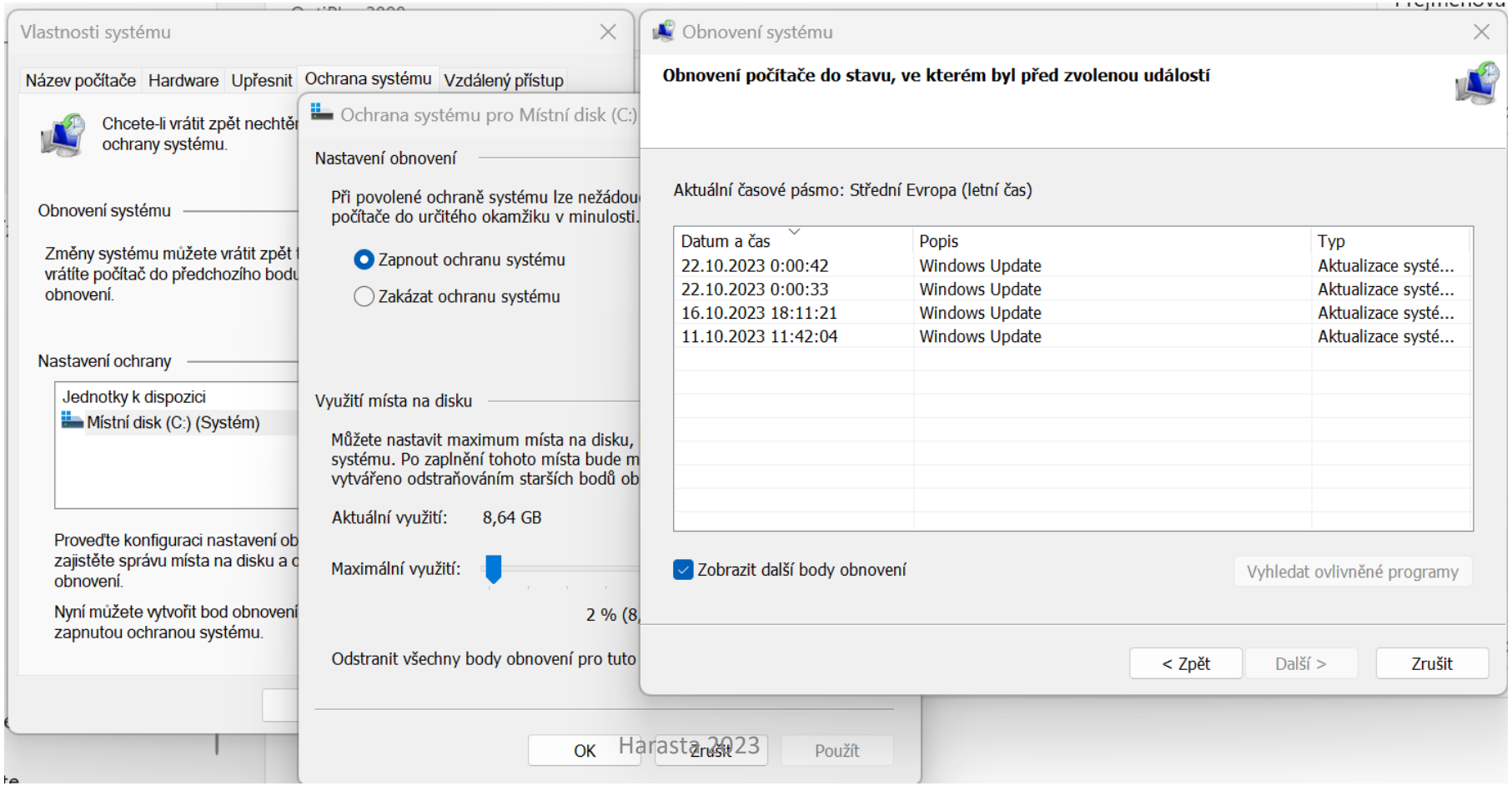
Základní poinstalační nastavení

- Adresář pro SBO:



Základní poinstalační nastavení

- Zapnutí systému bodu obnovení:



Základní poinstalační nastavení

- Ruční vytvoření bodu obnovení:
  - „Vytvořit bod obnovení“