Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana systémov a koncových zariadení

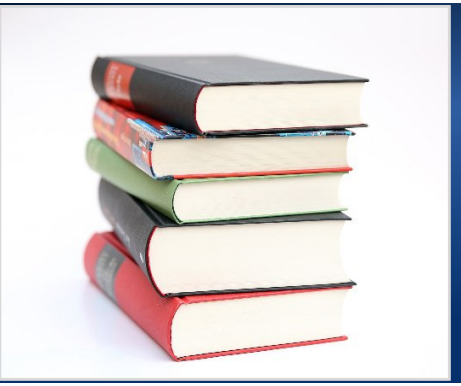
Ochrana koncových zariadení v LAN a online bezpečnosť (Blok V)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ing. Martin Kontšek, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

martin.kontsek@uniza.sk



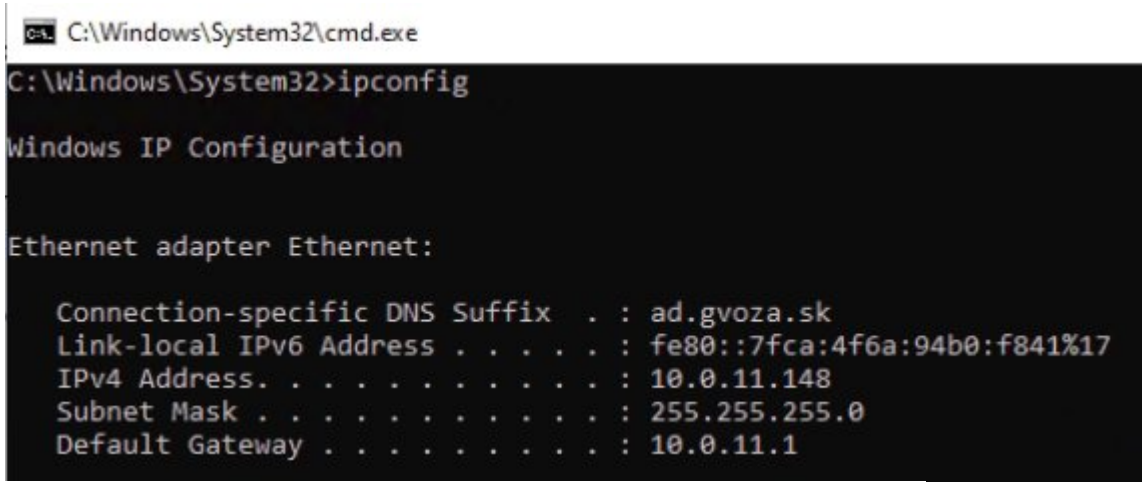
Obsah

- Windows ako operačný systém (OS) na koncovom zariadení zamestnanca verejnej správy
- Ako udržiavať pracovnú stanicu zamestnanca verejnej správy bezpečnú

Windows ako operačný systém (OS) na koncovom zariadení zamestnanca verejnej správy

Overenie IP adresy

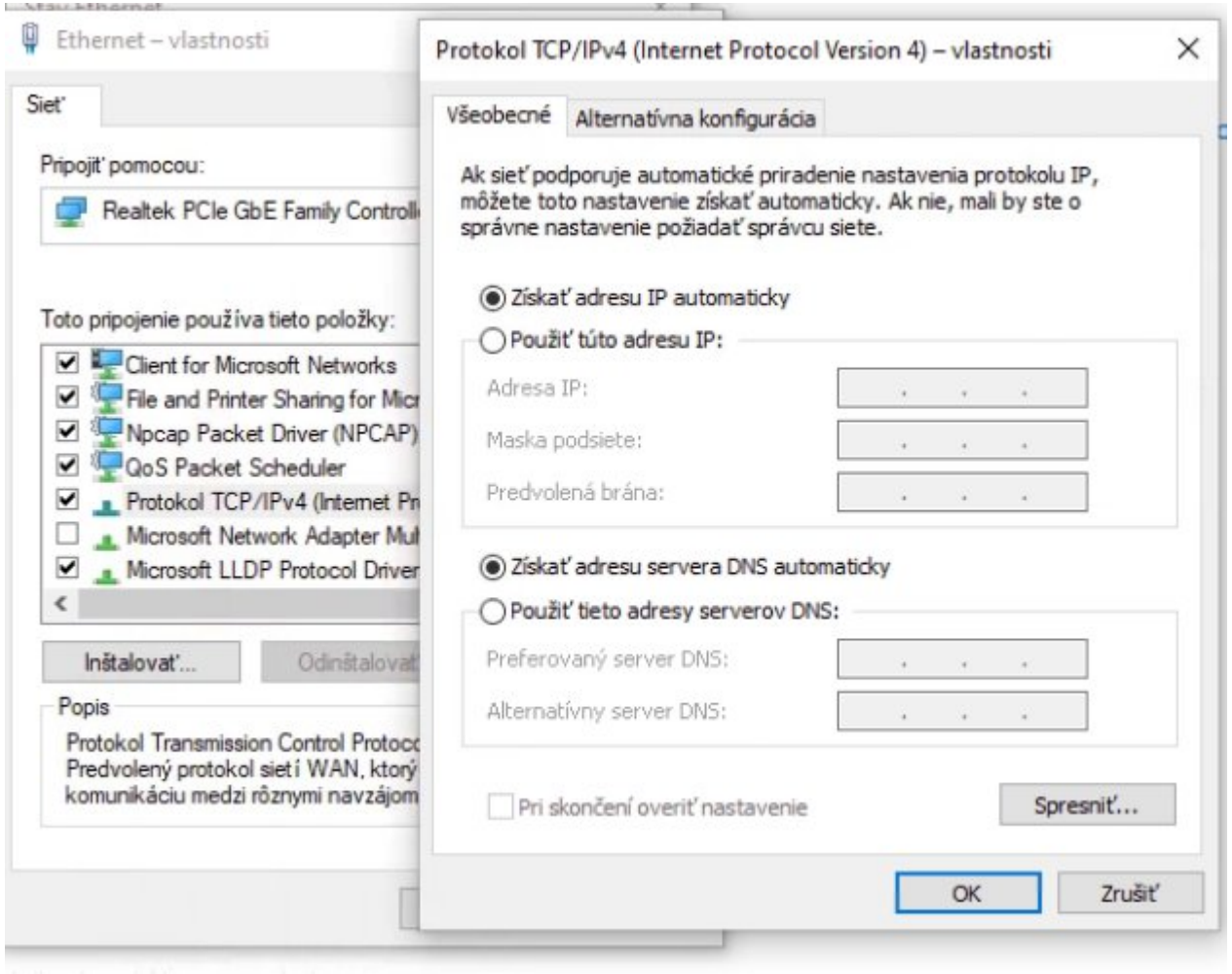
1. Win-R -> cmd -> ipconfig
2. Pravé tlačidlo na ikonu siete -> Ethernet Vlastnosti
3. Pravé tlačidlo na ikonu siete -> Zmeniť možnosti adaptéra -> pravé tlačidlo na adaptér -> Podrobnosti
4. Win-R -> ncpa.cpl -> pravé tlačidlo na adaptér -> Podrobnosti



Zmena IP adresy

1. Pravé tlačidlo na ikonu siete -> Zmeniť možnosti adaptéra -> pravé tlačidlo na adaptér -> Vlastnosti
2. Win-R -> ncpa.cpl -> pravé tlačidlo na adaptér -> Vlastnosti

- Statická konfigurácia
- Dynamická konfigurácia (DHCP)



Testovanie konektivity

1. Ping IP (ping 1.1.1.1)
2. Ping domeny (ping www.uniza.sk)
3. Overenie DNS (nslookup www.uniza.sk)
4. Trasovanie ku cieľu (tracert www.uniza.sk)
5. Zistenie mojej verejnej IP (https://ifconfig.me, https://myip.wtf)

Command Prompt

```
C:\Users\kontsek>ping wwww.google.sk

Pinging wwww.google.sk [2a00:1450:4014:80e::2003] with 32 bytes of data:
Reply from 2a00:1450:4014:80e::2003: time=8ms
Reply from 2a00:1450:4014:80e::2003: time=8ms
Reply from 2a00:1450:4014:80e::2003: time=8ms
Reply from 2a00:1450:4014:80e::2003: time=8ms

Ping statistics for 2a00:1450:4014:80e::2003:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Command Prompt

```
C:\Users\kontsek>tracert google.sk

Tracing route to google.sk [2a00:1450:4014:80a::2003]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2001:4118:300:121::1
  2    54 ms     8 ms    84 ms  vd-fri-l3-62.net.uniza.sk [2001:4118:300:100::141]
  3     3 ms     1 ms     3 ms  vd-ne-l3-23.net.uniza.sk [2001:4118:300:1ff::106]
  4    <1 ms    <1 ms    <1 ms  unizaw-l3-2.net.uniza.sk [2001:4118:300:7724::122]
  5     2 ms    <1 ms     1 ms  unizas-r-sa.net.uniza.sk [2001:4118:300:7702::221]
  6     4 ms     3 ms     3 ms  cvt-bratislava-1.sanet2.sk [2001:4118::1]
  7     5 ms     5 ms     5 ms  2001:718:0:20::1
  8     9 ms     8 ms     9 ms  2001:4860:1:1::2b36
  9     8 ms     8 ms     8 ms  2001:4860:1:1::2b36
 10     8 ms     8 ms     8 ms  2001:4860:0:1::9829
 11     8 ms     8 ms     8 ms  2001:4860:0:1::389b
 12     8 ms     8 ms     8 ms  prg03s10-in-x03.1e100.net [2a00:1450:4014:80a::2003]

Trace complete.
```

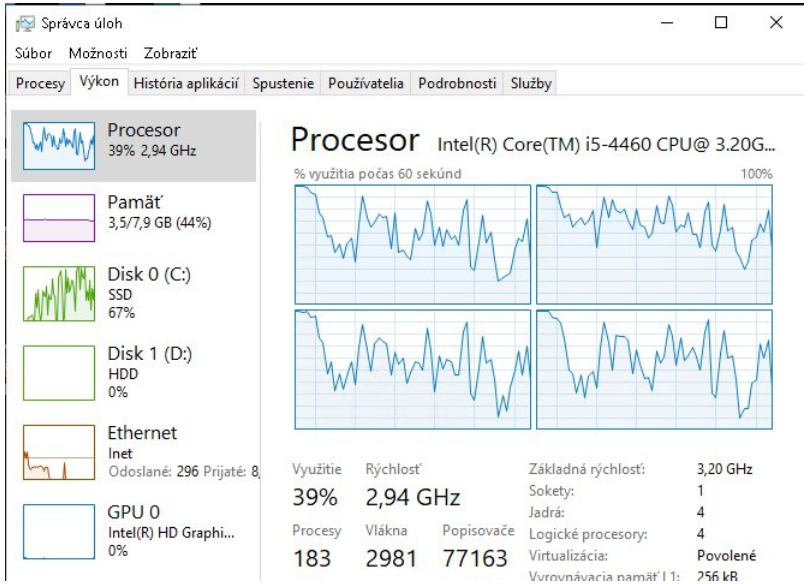
Command Prompt

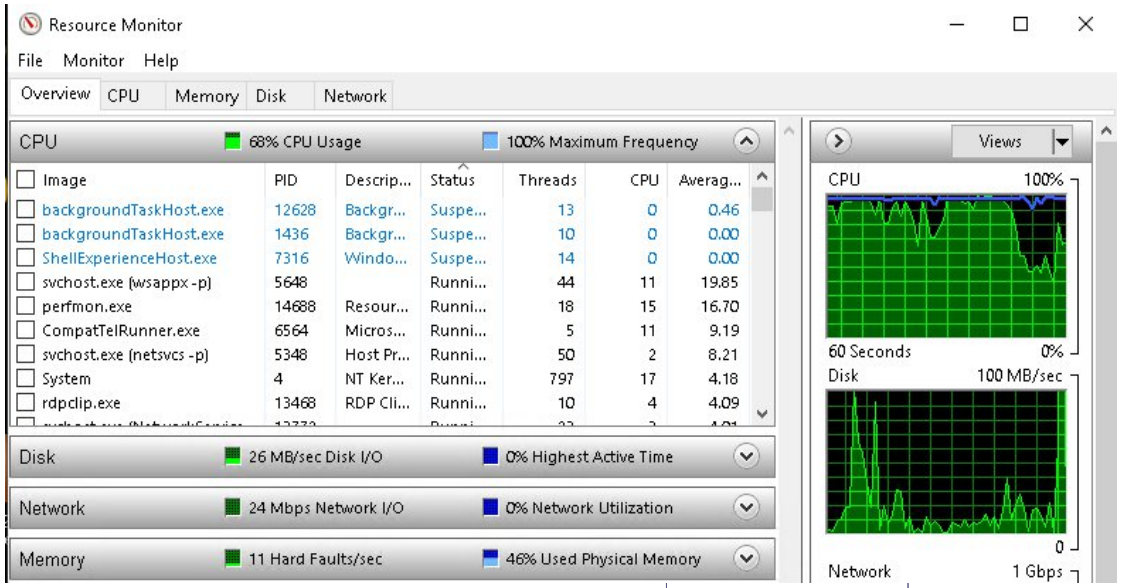
```
C:\Users\kontsek>nslookup wwww.uniza.sk
Server:  UnKnown
Address:  158.193.152.4

Non-authoritative answer:
Name:    wwww5.uniza.sk
Addresses:  2001:4118:300:48::212
          158.193.48.212
Aliases:  wwww.uniza.sk
```

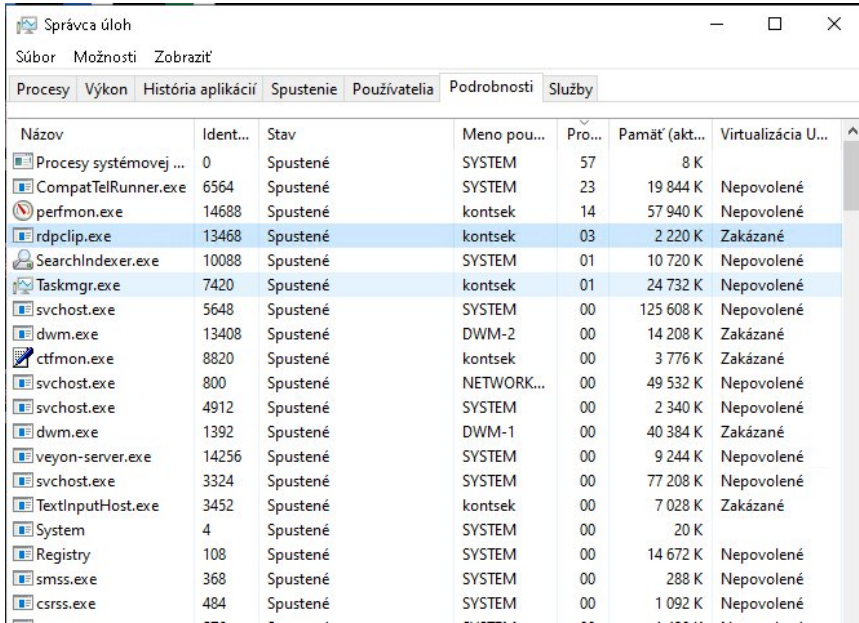

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prehľad výkonu, bežiacich procesov, služieb a aplikácií

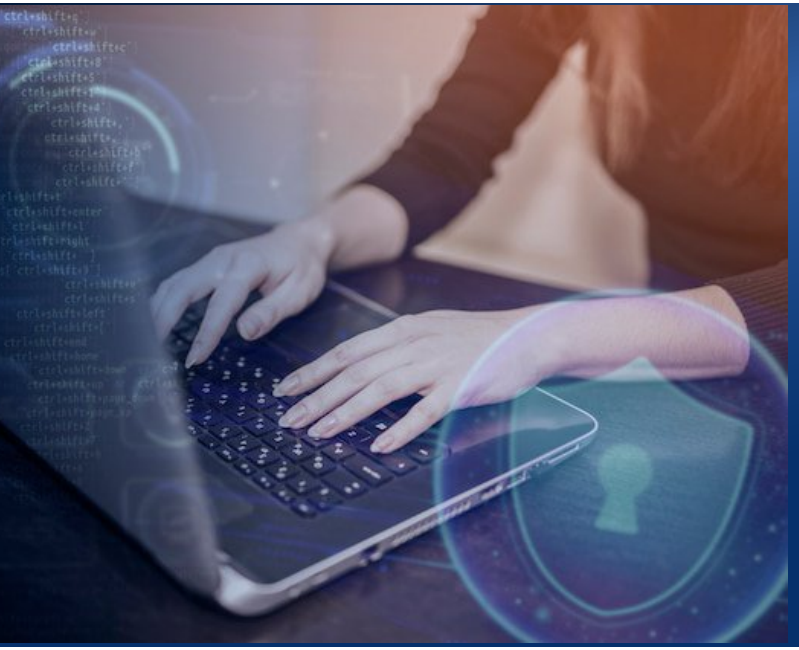
1. Správca úloh
   1. CTRL+SHIFT+ESC
   2. Pravé tlačidlo na panel úloh -> Správca úloh
   3. Štart menu -> task
2. Štart menu -> resource (detail o výkone)
3. Štart menu -> perfmon (dlhodobé štatistiky)







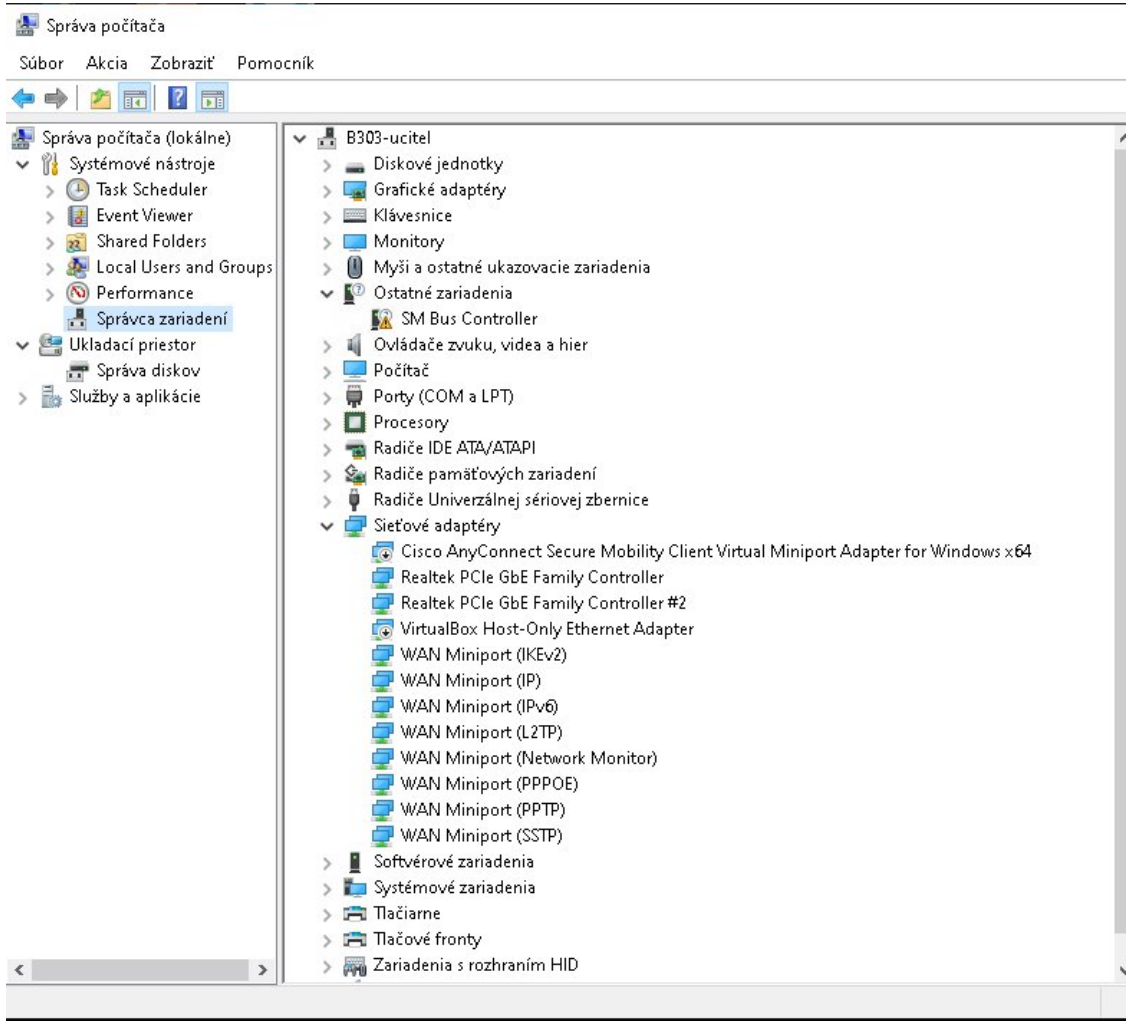
Ako udržiavať pracovnú stanicu zamestnanca verejnej správy bezpečnú



Dôležitosť aktualizácií a bezpečnostných záplat

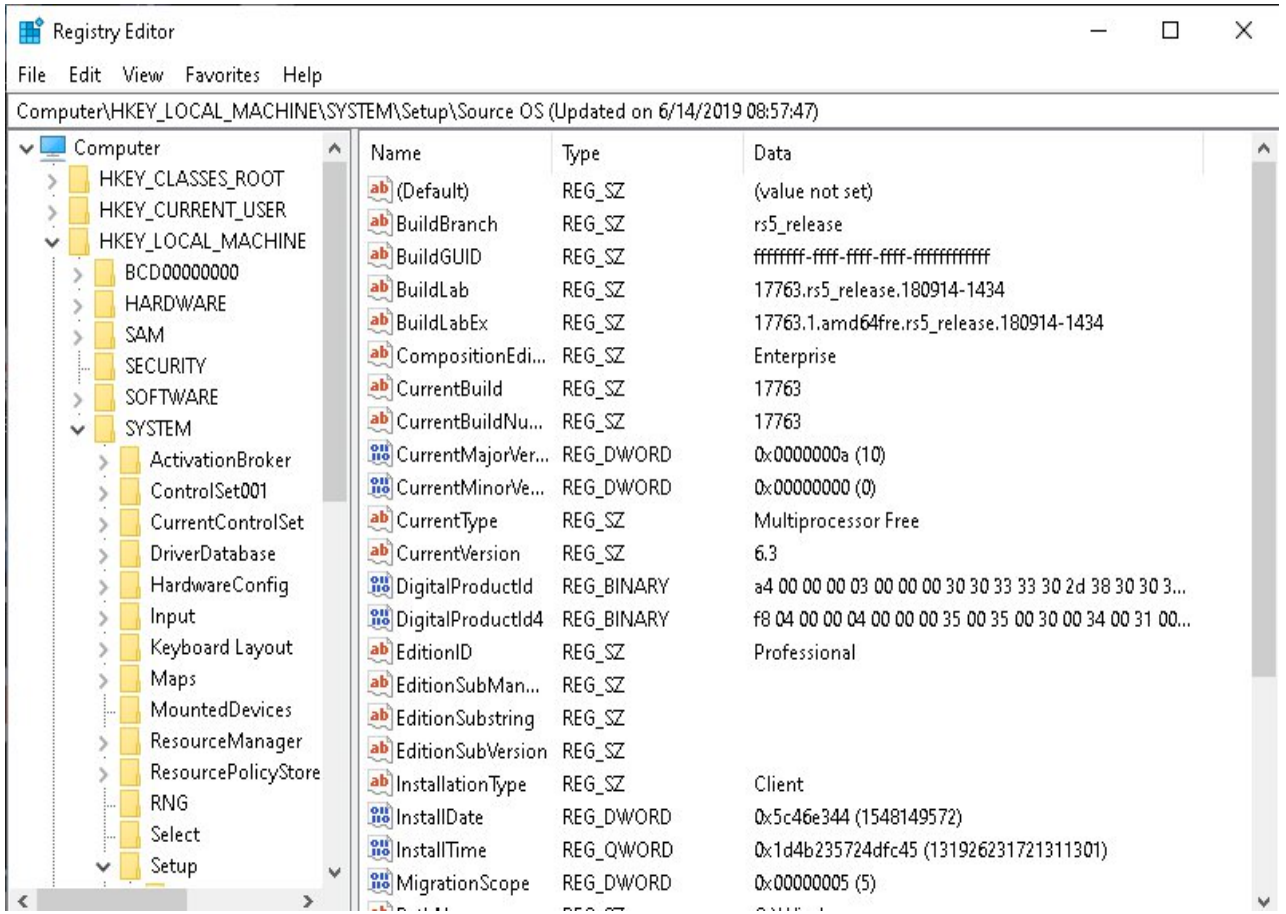
Administratívne nástroje - Správa počítača

- **Správa počítača**
  - a) Pravé tlačítko na Štart -> Správa počítača
  - b) Win+R -> compmgmt.msc
  - **Plánovač úloh** - Automatizácia úloh (zálohovanie, spúšťanie skriptov)
  - **Protokol udalostí** – systémové, aplikačné a bezpečnostné logy
  - **Zdieľané priečinky** – kontrola zdieľaných zdrojov
  - **Lokálni používatelia a skupiny**
  - **Správca zariadení** – ovládače, hardvér
  - **Správa diskov** – vytváranie, formátovanie, zmena veľkosti oddielov na disku
  - **Služby a aplikácie** – správa služieb, možnosť spustenia, zastavenia, nastavenia typu spustenia (automaticky, manuálne, zakázané)



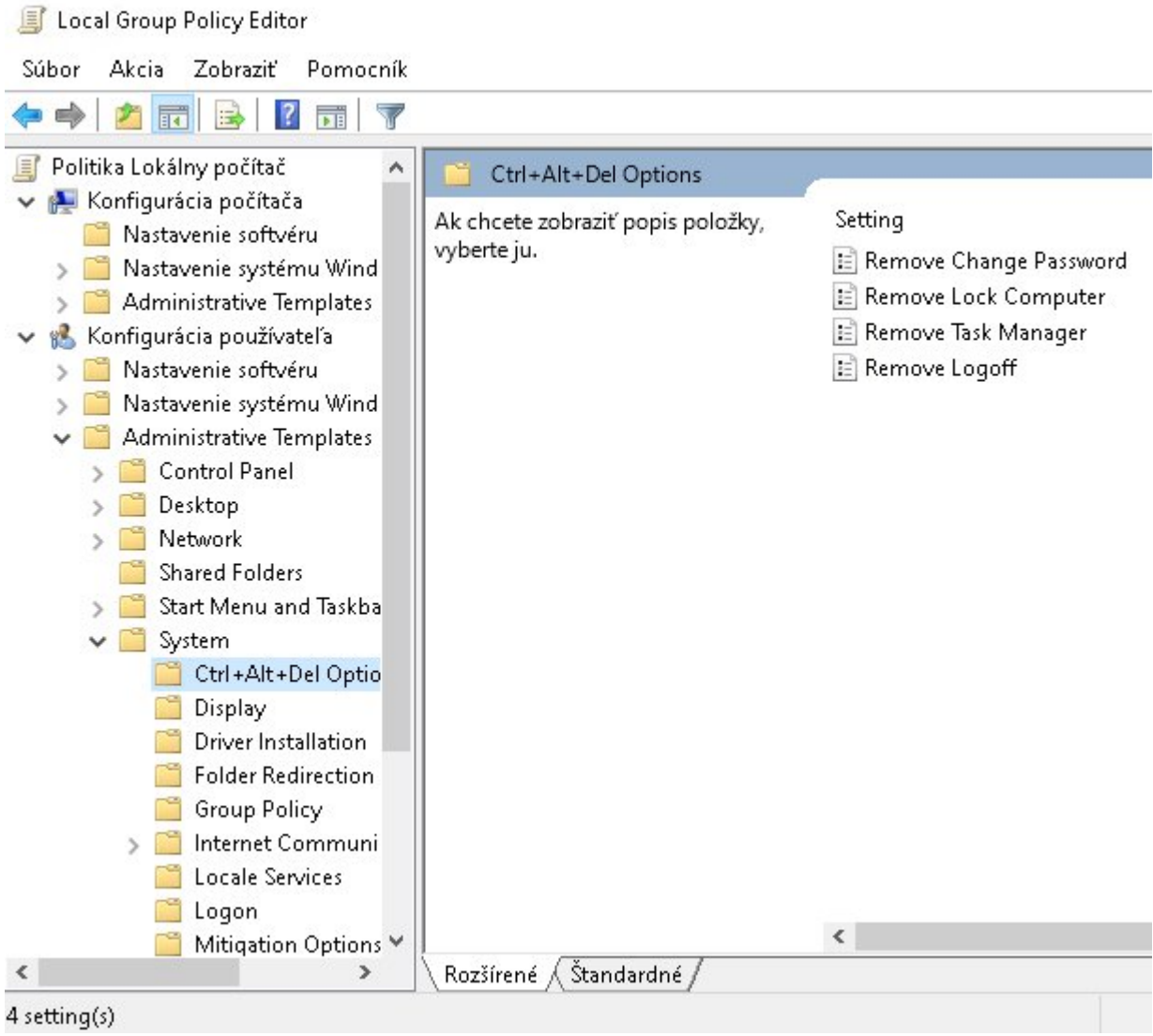
Administratívne nástroje - Editor registrov

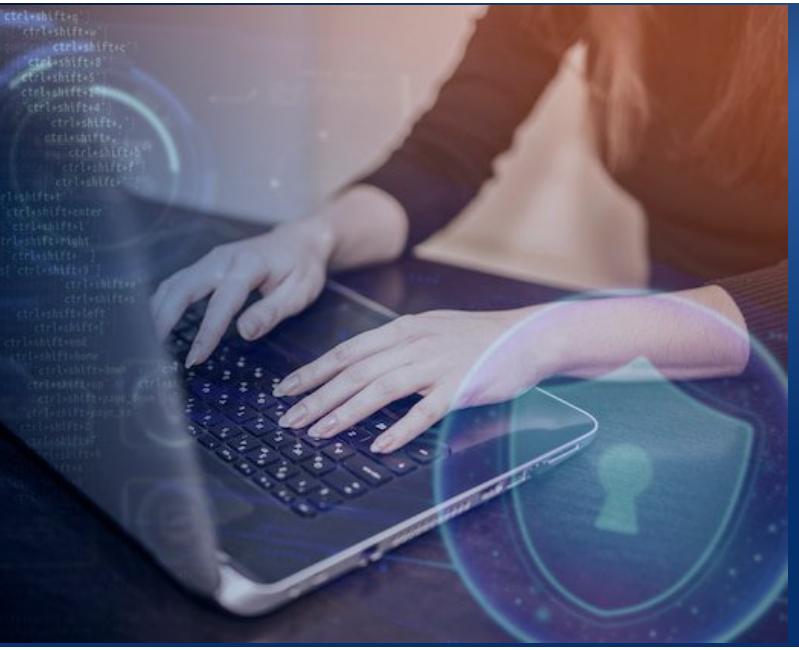
- **Editor registrov**
  a) Win+R -> regedit
- umožňuje používateľovi prezerať, upravovať a spravovať Windows Registry – hierarchickú databázu, ktorá uchováva konfiguračné nastavenia a možnosti operačného systému, hardvéru, softvéru a používateľských profilov.
- Zmeny môžu ovplyvniť stabilitu systému
- Odporúča sa záloha pred úpravami
- Hlavné vetvy (tzv. hives):
  - HKEY_CLASSES_ROOT (HKCR) – informácie o typoch súborov a asociáciách
  - HKEY_CURRENT_USER (HKCU) – nastavenia aktuálneho používateľa
  - HKEY_LOCAL_MACHINE (HKLM) – globálne nastavenia systému
  - HKEY_USERS (HKU) – nastavenia všetkých používateľov
  - HKEY_CURRENT_CONFIG (HKCC) – nastavenia aktuálnej konfigurácie hardvéru



Administratívne nástroje – Local Group Policy Editor

- **Lokálny editor skupinových politík**
  a) Win+R -> gpedit.msc
- umožňuje konfigurovať a spravovať nastavenia systému, používateľov a bezpečnosti bez potreby zásahu do registrov.
- Umožňuje centrálne riadiť správanie systému – napr. aktualizácie, prístup k funkciám, zabezpečenie, skrývanie prvkov rozhrania.
- Príklady použitia
  - Zakázanie prístupu k USB portom
  - Vynútenie silného hesla
  - Obmedzenie prístupu k ovládaciemu panelu
  - Skrytie ikon, funkcií, nastavení
  - Zakázanie prístupu k správcu úloh



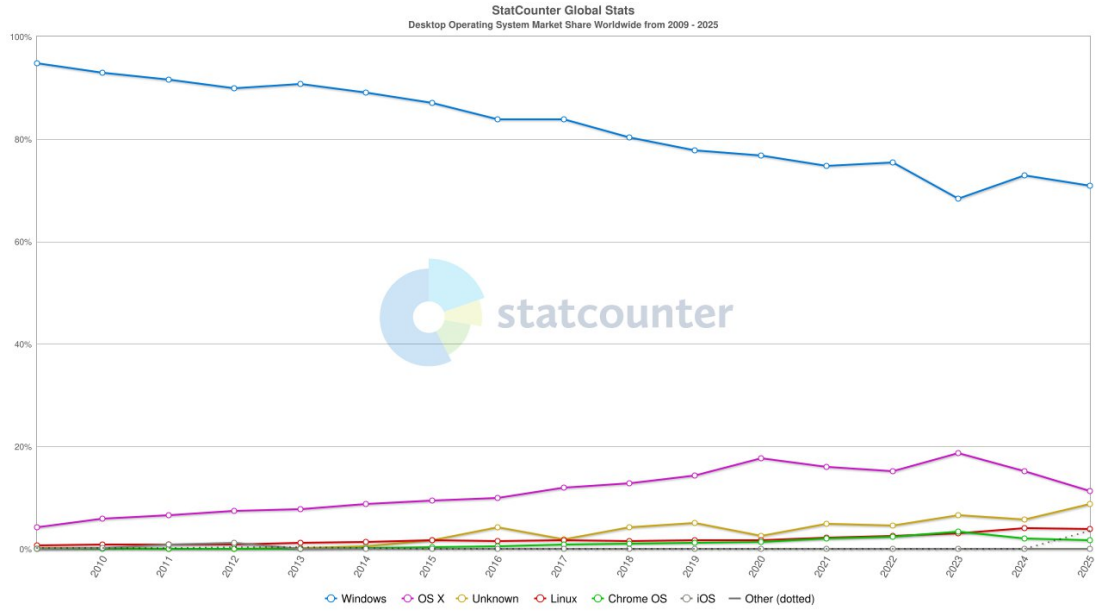


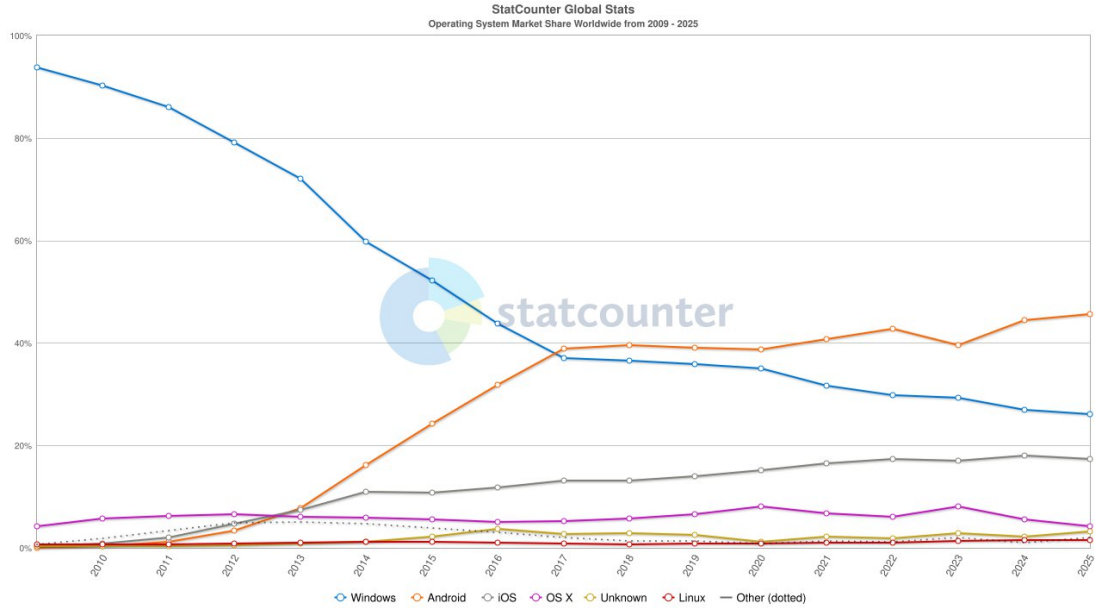
Dôležitosť aktualizácií a bezpečnostných záplat

Ochrana systémov a koncových zariadení

Dôležitosť aktualizácií

- Windows je najrozšírenejší OS na desktope (69%)
- častý cieľ kybernetických útokov
- Aktualizácie opravujú chyby, zraniteľnosti a zlepšujú stabilitu.
- Bezpečnostné záplaty chránia pred známymi hrozbami.





Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

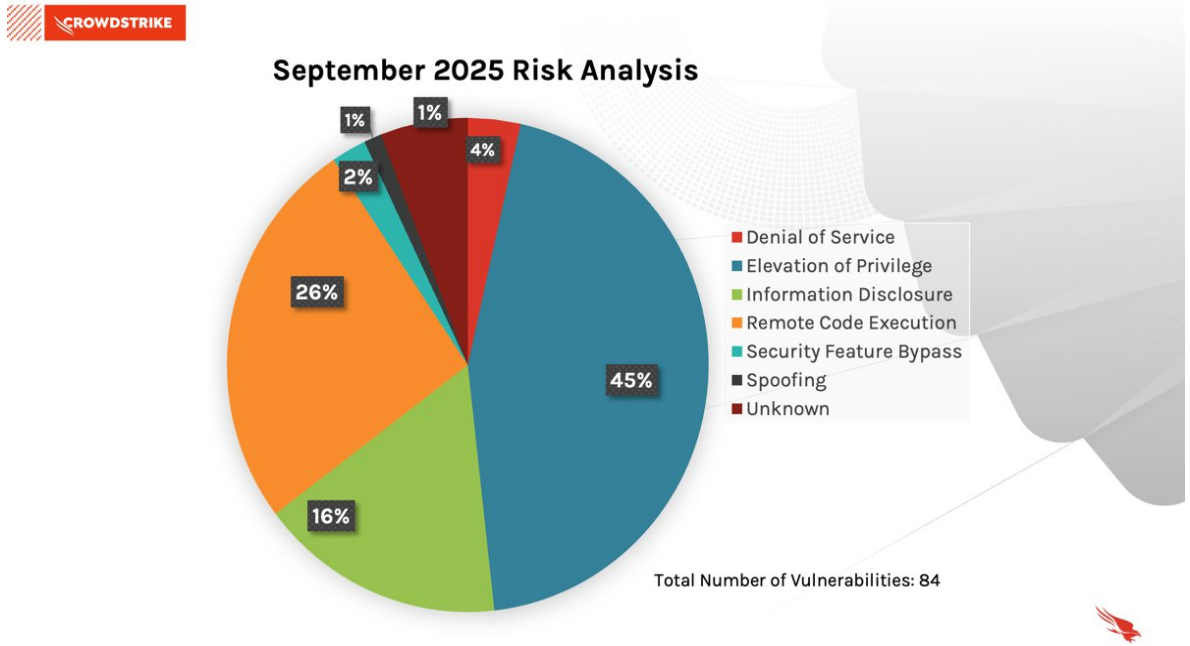
Typy aktualizácií vo Windows

- Kumulatívne aktualizácie
  - obsahujú všetky predchádzajúce opravy, čím zjednodušujú správu systému.
- Bezpečnostné záplaty
  - riešia konkrétne zraniteľnosti, ktoré by mohli byť zneužité.
- Feature Updates
  - prinášajú nové funkcie a dizajnové zmeny (napr. prechod z 24H2 na 25H2, prechod z Windows 10 na Windows 11).
- Driver Updates
  - aktualizujú ovládače hardvéru pre lepšiu kompatibilitu (môžu spôsobiť problémy, hlavne pri staršom hardvéri).
- Optional Updates
  - voliteľné aktualizácie, ktoré nie sú kritické, ale môžu zlepšiť funkcionalitu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Patch Tuesday

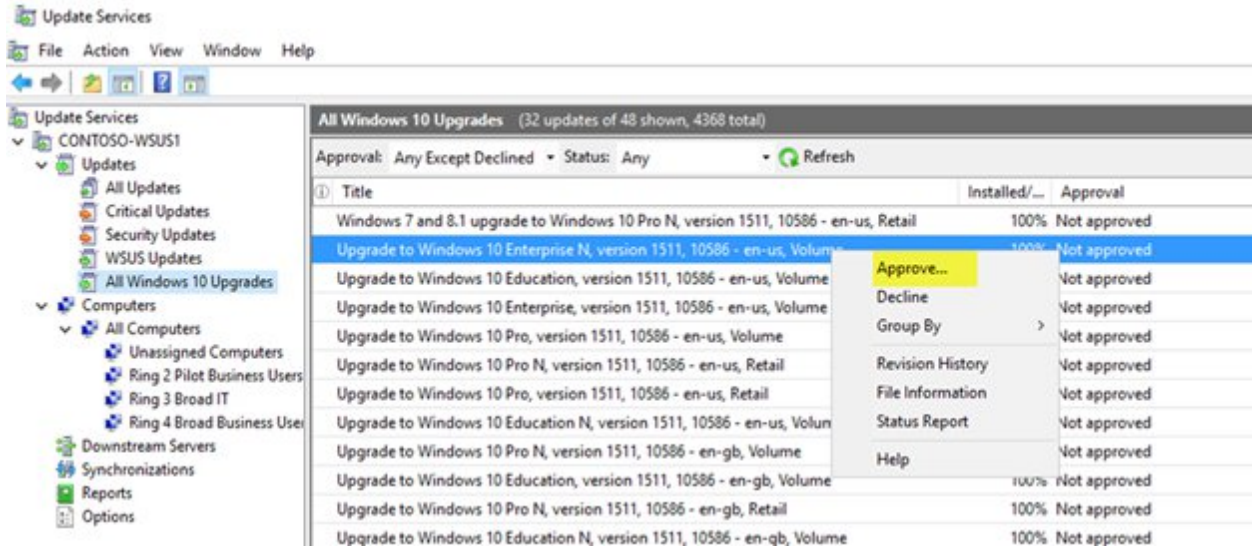
- Druhý utorok v mesiaci.
- Deň vydávania aktualizácií od Microsoftu.
- Zamerané na bezpečnostné záplaty a opravy chýb.
- Dôležité pre plánovanie aktualizácií vo firmách administrátormi.
- https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-september-2025/



Ako funguje Windows Update

- Windows Update komunikuje so servermi Microsoftu.
- Sťahuje a inštaluje aktualizácie podľa nastavení.
- Možnosť aktualizácie online alebo offline balíky (.msu).

- Firemné prostredie
  - Centrálna správa cez Group Policy, Intune, WSUS (Windows Server Update Services).
  - Politiky odkladu aktualizácií.
- Pilotné skupiny na testovanie.
  - Testovanie na neprodukčných strojoch.
  - Kontrola kompatibility s aplikáciami.
  - Plánovanie aktualizačných okien.
- Reporting cez Windows Update Analytics.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Odporúčané nastavenia a riziká neaktualizovaného systému

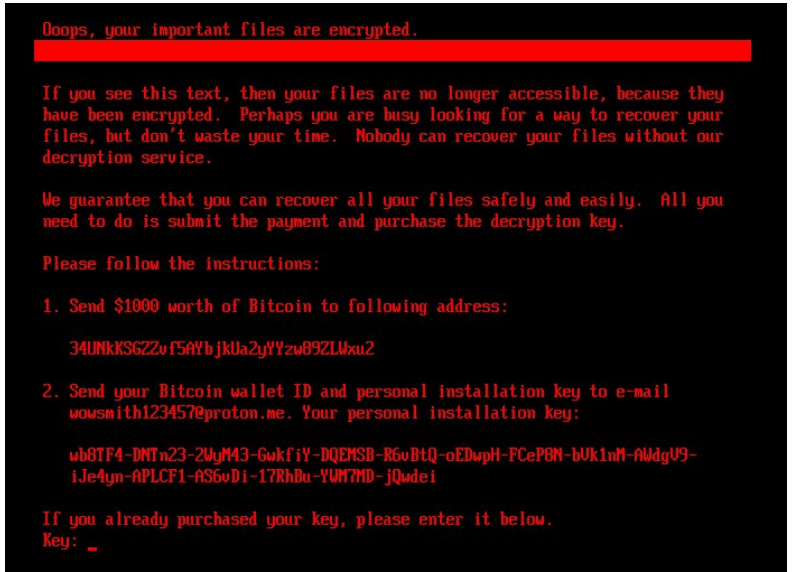
- Odporúčané nastavenia
  - Zapnuté automatické aktualizácie.
  - Odloženie veľkých aktualizácií o 7–30 dní.
  - Vytváranie záloh pred aktualizáciou.
  - Monitorovanie cez Windows Security Center.

- Riziká neaktualizovaného systému
  - Vzdialený prístup útočníka, ransomware, malware, phishing, porušenie legislatívy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Incidenty spôsobené neaktualizovaným Windows

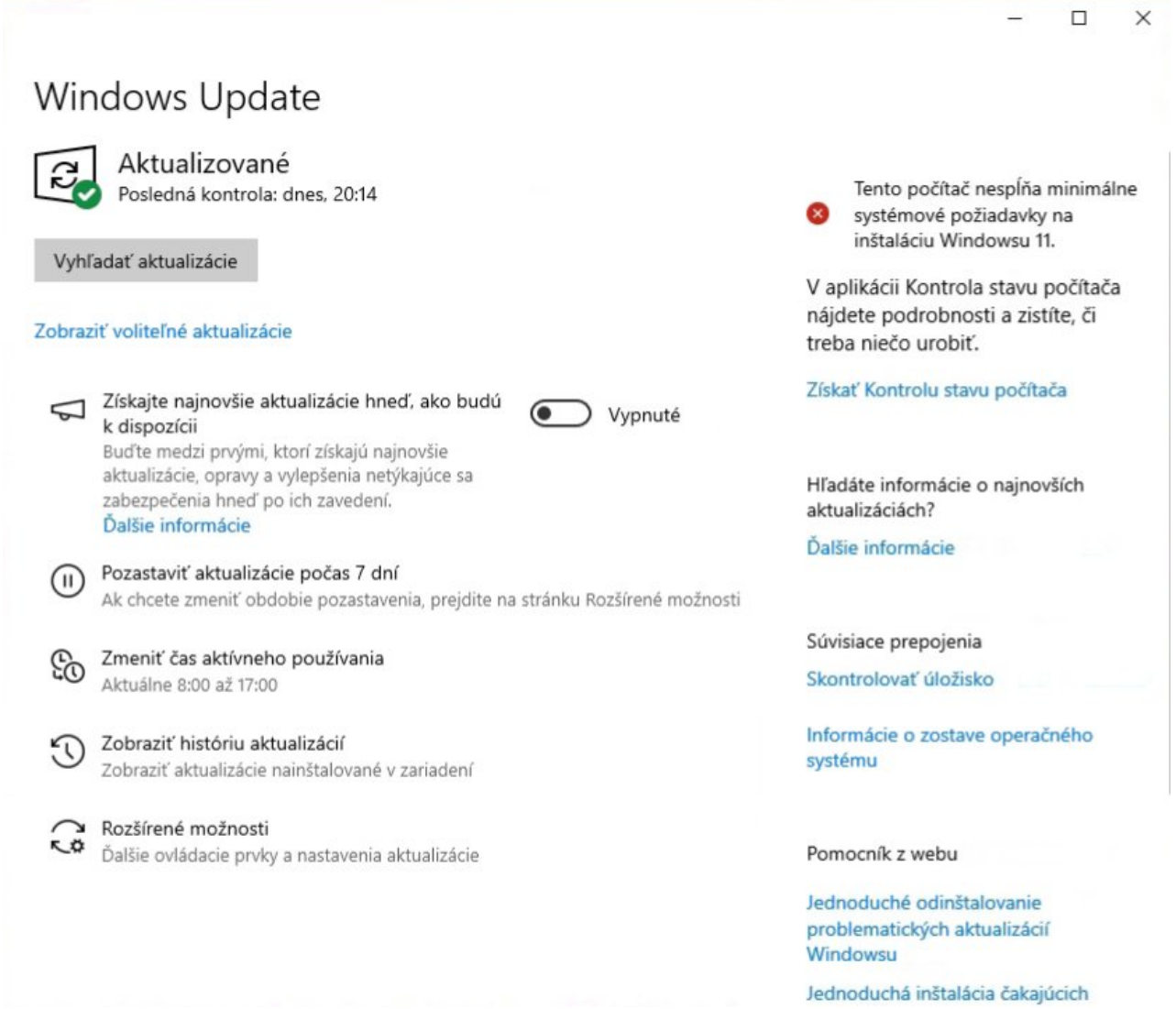
- WannaCry (2017)
  - využil zraniteľnosť EternalBlue v SMBv1, ktorá bola opravená 2 mesiace pred útokom – milióny systémov však neboli aktualizované.
  - šifrovanie dát, výpadky nemocníc, firiem, dopravných systémov
- NotPetya (2017)
  - Podobne ako WannaCry, zneužil SMBv1 zraniteľnosť.
  - Zasiahol najmä Ukrajinu, ale aj globálne firmy ako Maersk, Merck.
  - Spôsobil škody vo výške miliárd dolárov
- BlueKeep (2019)
  - RDP zraniteľnosť, ktorá umožňovala vzdialené ovládanie systému.
- Zerologon (2020)
  - Kritická zraniteľnosť v Netlogon protokole umožňovala privilegovaný prístup k doméne.
  - Bola zneužitá v útokoch na vládne inštitúcie a podniky.
- ProxyShell útoky (2021–2023)
  - Séria zraniteľností v Microsoft Exchange Serveri.
  - Umožňovali vzdialené spustenie kódu bez autentifikácie.
  - Zneužité v ransom útokoch, napriek dostupným záplatám.
- HybridPetya (2025)
  - Nový variant ransomwaru schopný obísť UEFI Secure Boot.
  - Zneužíva staršie, neaktualizované systémy s nedostatočnou ochranou.
  - Ukazuje, že aj moderné technológie môžu byť zraniteľné bez aktualizácií.

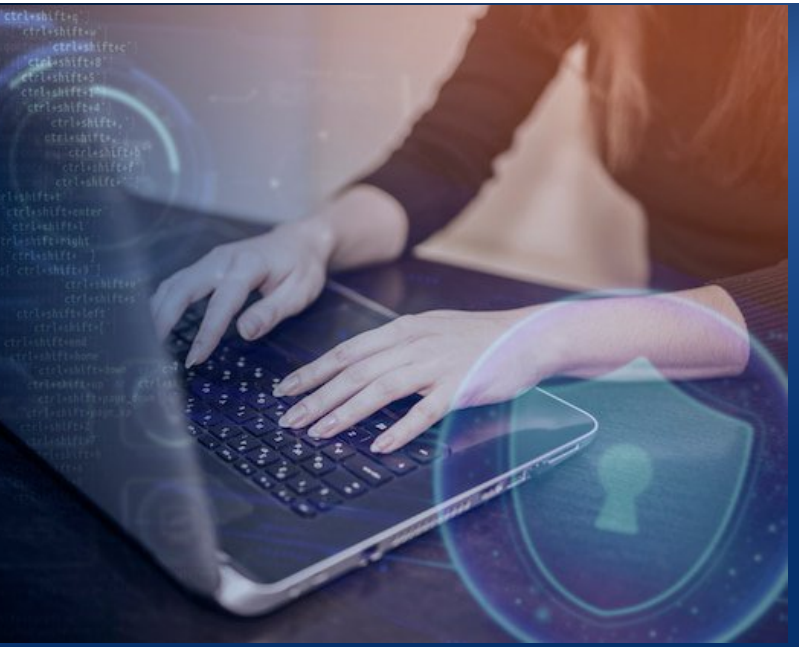


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako skontrolovať stav aktualizácií

- Otvoriť Nastavenia > Aktualizácia a zabezpečenie -> Windows Update.
- Skontrolovať dostupné aktualizácie.
- História aktualizácií – zobrazenie nainštalovaných záplat.
- Možnosť odinštalovania problémovej aktualizácie.





Dôležitosť zálohovania dát, praktické kroky ako zálohovať a obnova dát po incidente

Zálohovanie dát

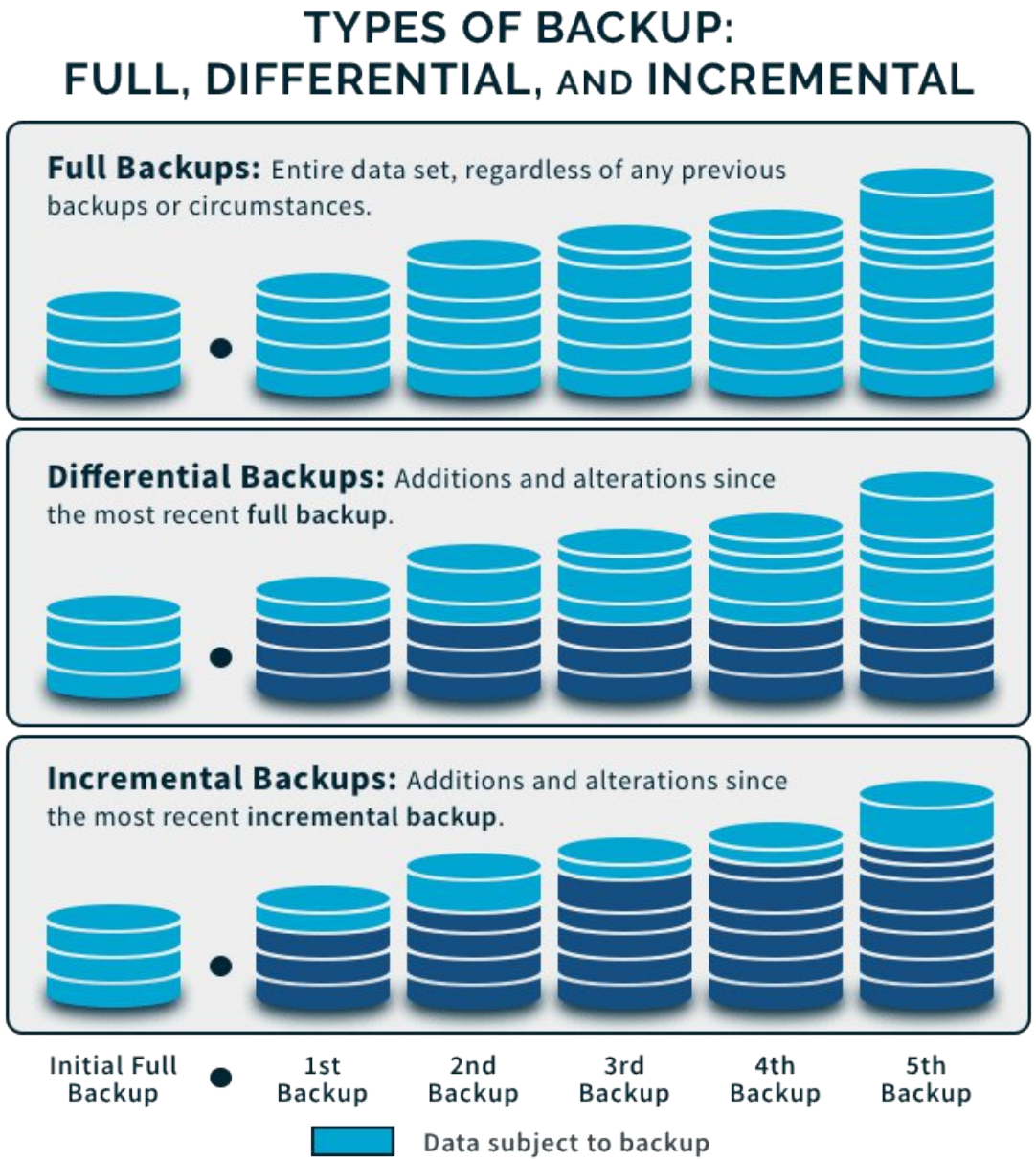
- Proces vytvárania kópií dát na bezpečné miesto, ktoré možno obnoviť v prípade ich straty.
- Cieľ: Zabezpečiť kontinuitu práce, ochranu osobných údajov a minimalizáciu škôd.

- Ochrana pred stratou dát spôsobenou:
  - Hardvérovým zlyhaním (napr. zlyhanie pevného disku)
  - Ransomvérom alebo vírusmi
  - Neúmyselným vymazaním
  - Prírodnými katastrofami: Požiar, záplavy, blesky.
  - Krádežou alebo stratou zariadenia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy záloh

- Plná záloha
  - Kompletná kópia všetkých dát
  - Jednoduchá obnova, ale veľká veľkosť
- Inkrementálna záloha
  - Len zmenené dáta od poslednej zálohy
  - Úspora miesta, potenciálne zložitejšia obnova
- Diferenciálna záloha
  - Zmeny od poslednej plnej zálohy
  - Rýchlejšia obnova ako inkrementálna, rastúca veľkosť
- Obraz disku (disk image)
  - Kompletná kópia systému vrátane OS
  - Obnova celého systému, záloha nielen užitočných dát ale aj OS a dočasných súborov



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kam zálohovať

- Externý HDD/SSD – rýchle, dostupné, ale náchylné na fyzické poškodenie
- USB kľúč – vhodné na dokumenty, nie na systémové zálohy
- NAS – ideálne pre domácnosti a firmy

- Cloudové služby:
  - OneDrive, Google Drive, Dropbox
  - automatická synchronizácia, dostupnosť kdekoľvek
  - Backblaze, Acronis, iDrive
  - Špecializované služby – pokročilé funkcie, šifrovanie

Softvér na zálohovanie pre Windows - vstavaný

- Windows Zálohovanie
  - Bezplatné, vstavané vo Windows 10/11
  - Zálohovanie súborov, nastavení, aplikácií, motívov, Wi-Fi informácií.
  - Ukladanie len do OneDrive (potrebný Microsoft účet)
- História súborov
  - Bezplatné, vstavané vo Windows 10/11
  - zálohuje súbory z priečinkov ako Dokumenty, Obrázky, Hudba, Videá a Plocha.
  - Umožňuje obnoviť predchádzajúce verzie súborov.
  - Zálohy sa ukladajú na externý disk, sieťové úložisko alebo druhý interný disk.
- Zálohovanie a obnovenie (Windows 7)
  - Bezplatné, vstavané vo Windows 10/11, staršia aplikácia
  - Zálohovanie súborov, obraz systému, obnova aj cez obnovenie pri štarte
  - Zálohy sa ukladajú na externý disk, sieťové úložisko alebo druhý interný disk, nepodporuje cloud

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

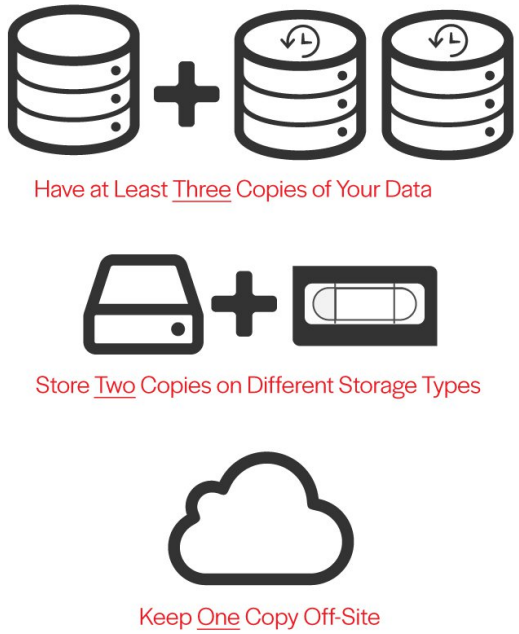
Softvér na zálohovanie pre Windows – doinštalovať

- AOMEI Backupper
  - Bezplatná aj platená verzia
  - Bezplatne záloha súborov, zložiek ale aj celého systému
  - Obnova priamo vo windows, ale aj z USB ak systém neštartuje
- Acronis Cyber Protect Home Office
  - Platený (predplatné)
  - Zálohovanie celého systému, súborov, cloudové zálohy, ochrana proti ransomvéru.
- Iperius Backup
  - Bezplatná obmedzená aj platená verzia
  - Zálohovanie súborov, diskov, databáz, cloudové zálohy (Google Drive, Dropbox, OneDrive).
- DataNumen Backup
- EaseUS Todo Backup
- Macrium Reflect
- Paragon Backup & Recovery

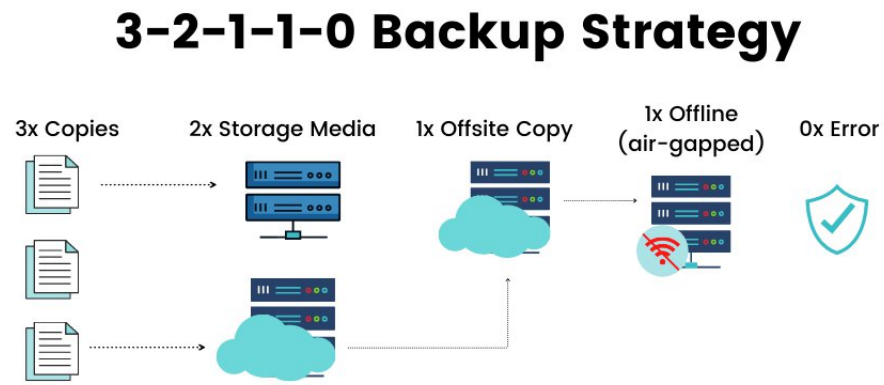
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Odporúčania pre zálohovanie

- Pravidlo 3-2-1:
  - 3 kópie dát (originál + 2 zálohy)
  - 2 rôzne typy médií (napr. disk + cloud)
  - 1 záloha mimo lokalitu (napr. cloud)



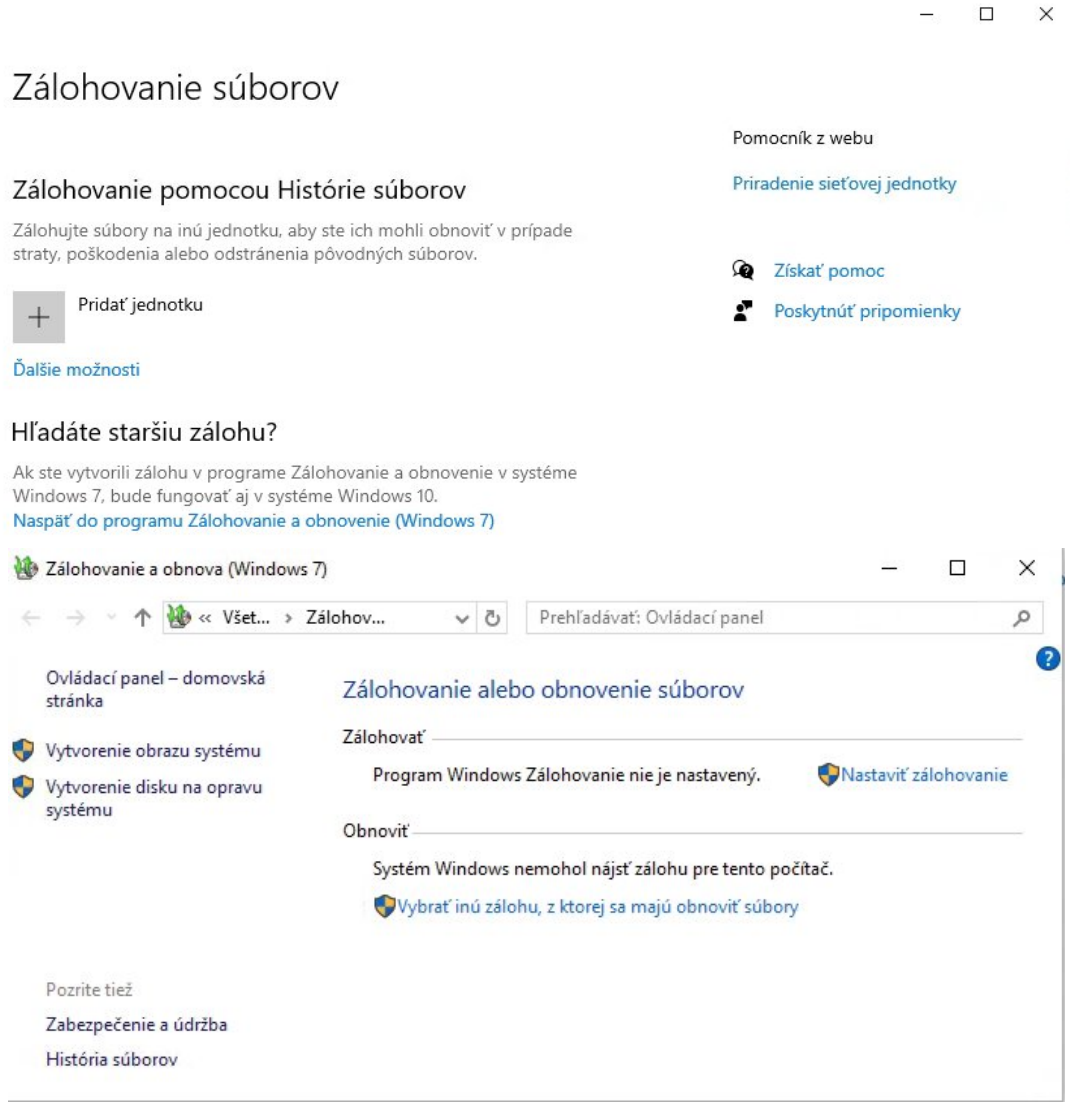
- Plánované automatické zálohy (napr. každý deň o 20:00)
- notifikácie o úspechu/zlyhaní zálohy
- Pravidelné testovanie obnovy dát (kontrola integrity)
- Zálohovanie pred veľkými aktualizáciami
- Šifrovanie záloh



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Praktické kroky zálohovania vo Windows

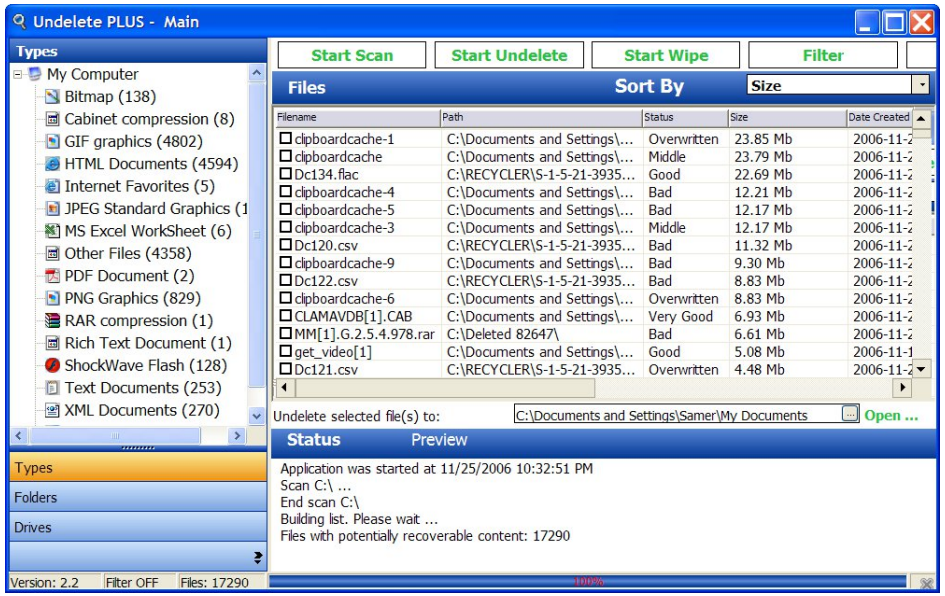
- **História súborov (File History):**
- Nastavenie: Nastavenia → Aktualizácia a zabezpečenie → Zálohovanie
- Vyber externý disk alebo sieťové umiestnenie
- Automatické zálohovanie vybraných priečinkov

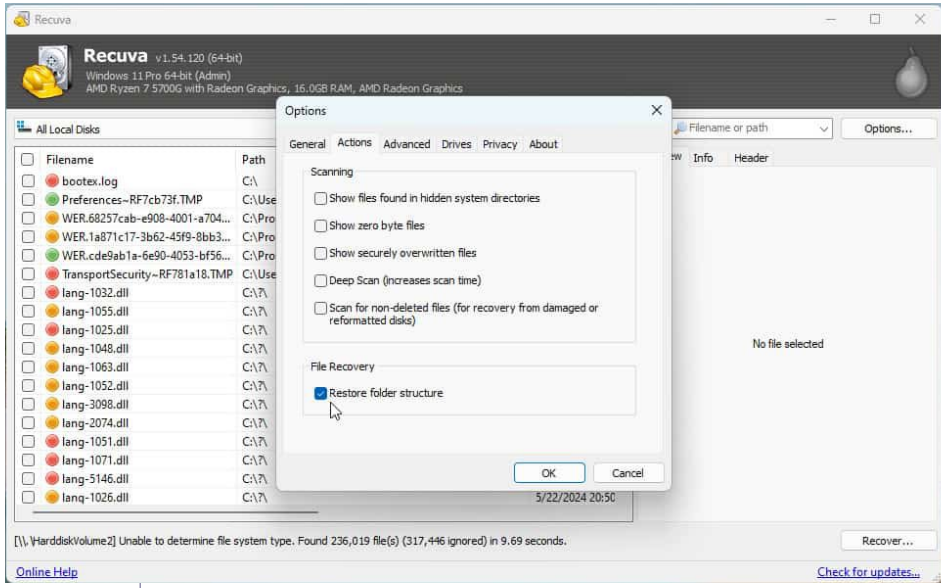


- **Zálohovanie a obnovenie (Windows 7):**
- Otvoriť Ovládací panel > Systém a zabezpečenie > Zálohovanie a obnovenie (Windows 7).
- Kliknúť na Nastaviť zálohovanie.
- Vybrať cieľ (napr. externý disk).
- Vybrať čo zálohovať – automaticky alebo manuálne.
  - Nastaviť plán (napr. týždenne).

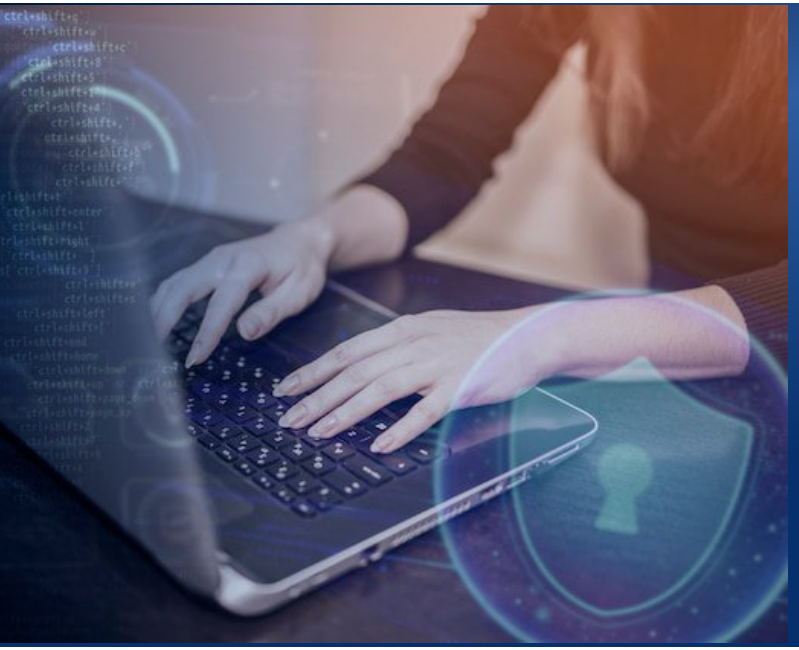
Obnova dát po incidente

- Obnova súborov programom História súborov:
  - File History → „Obnoviť osobné súbory“
  - Vyhľadať požadovaný súbor → kliknúť „Obnoviť“
- Obnova systému z obrazu disku:
  - Spustiť PC z obnovovacieho disku
  - Vybrať systémový obraz → obnoviť systém
- Obnova z cloudového úložiska:
  - Prihlásiť sa do cloudovej služby
  - Stiahnuť zálohované súbory
- Nemám zálohy
  - Dostupné programy na obnovu stratených súborov
  - Záchrana dát profesionálnou firmou





Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Šifrovanie diskov

Šifrovanie diskov

- Šifrovanie
  - Proces konverzie dát do formátu, ktorý je nečitateľný bez správneho kľúča.
- Dôvod šifrovania
  - Ochrana citlivých údajov pred neoprávneným prístupom.
  - Zabezpečenie dát pri strate alebo krádeži zariadenia.
  - Dodržiavanie legislatívy.
  - Zabezpečenie zariadení mobilných pracovníkov.
  - Dôvera zákazníkov a partnerov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy šifrovania vo Windows

- BitLocker
  - edície Pro, Enterprise, Education
  - Šifruje celý disk alebo vybrané oddiely
  - Integrácia s TPM (Trusted Platform Module)
  - Možnosť nastaviť PIN, heslo alebo USB kľúč
- Device Encryption
  - edícia Home
  - Automaticky aktivované na kompatibilných zariadeniach
  - Vyžaduje:
  - TPM 2.0, Modern Standby, Prihlásenie cez Microsoft účet
  - Menej možností ako BitLocker (bez pin a USB)

- EFS (Encrypting File System)
  - edície Pro, Enterprise, Education
  - Šifrovanie jednotlivých súborov a priečinkov
  - Použiteľné cez vlastnosti súboru → „Rozšírené“ → „Šifrovať obsah“

- Externé nástroje

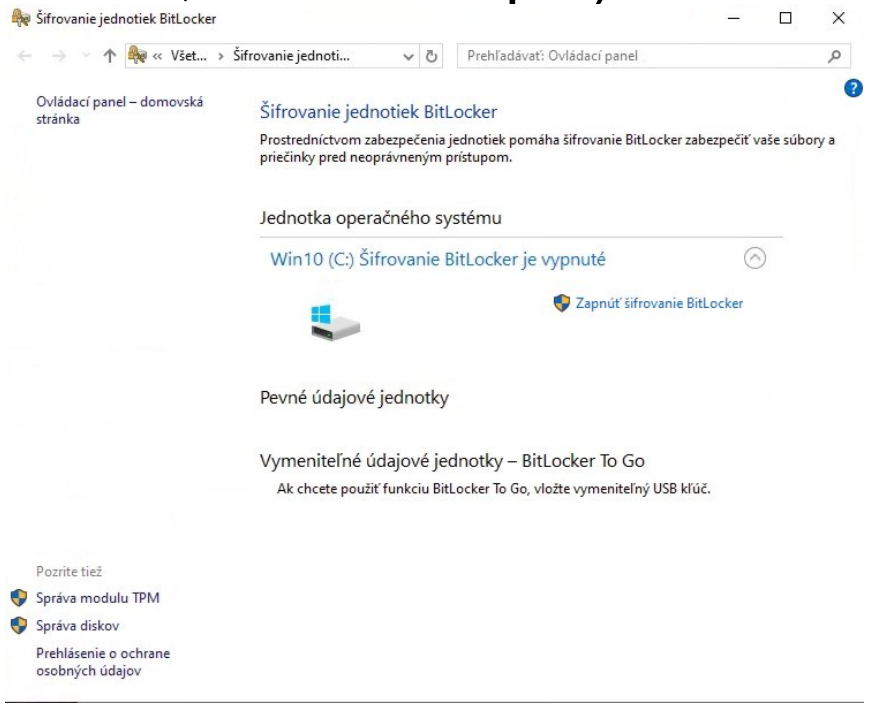
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

BitLocker

- Šifrovací algoritmus
  - AES (128-bit alebo 256-bit)
- Kľúč na dešifrovanie
  - Uložený v TPM čipe (hardvérový komponent, ktorý bezpečne uchováva šifrovacie kľúče)
  - TPM + PIN
  - na USB kľúči
- Obnova
  - Pomocou obnovovacieho kľúča (Recovery Key)

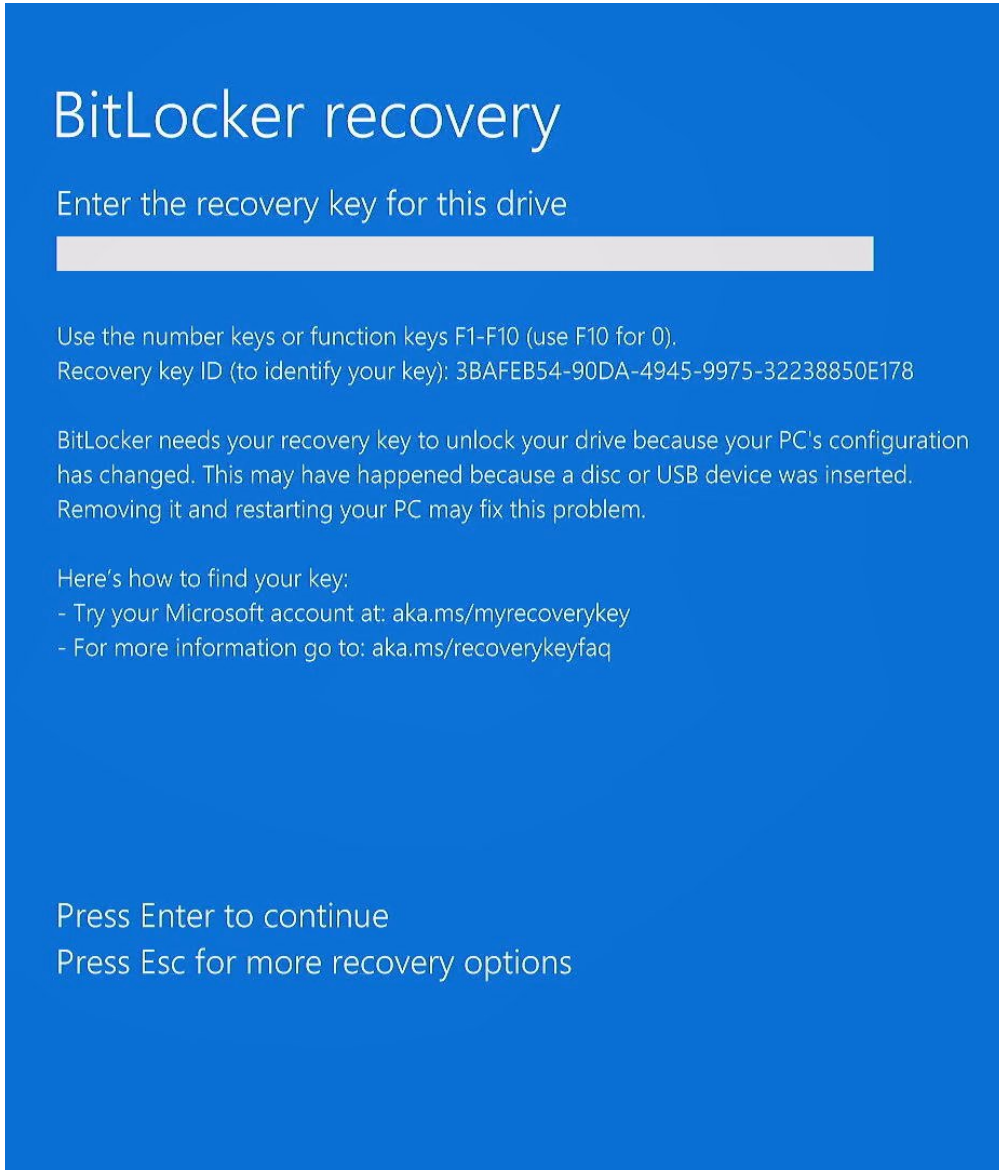
Zapnutie BitLockeru

1. Otvoriť Ovládací panel → Spravovať šifrovanie BitLocker
2. Vybrať disk → kliknúť „Zapnúť BitLocker“
3. Vybrať spôsob odomykania (heslo, USB, TPM)
4. Uložiť obnovovací kľúč (do Microsoft účtu, USB, súboru, tlačená kópia)
5. Vybrať režim šifrovania:
   a) Použiť celý disk
   b) Použiť len obsadenú časť
6. Spustiť šifrovanie



Obnovovací kľúč BitLocker

- 48-miestny kód na odomknutie disku, ak sa stratí prístup
- Bez obnovovacieho kľúča nie je možné obnoviť prístup k dátam
- Kde sa ukladá
  - Microsoft účet
  - USB kľúč
  - Tlačená kópia
  - Firemný IT systém
- Kedy je potrebný
  - Po zmene hardvéru
  - Po aktualizácii BIOS/UEFI
  - Pri strate TPM alebo hesla



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

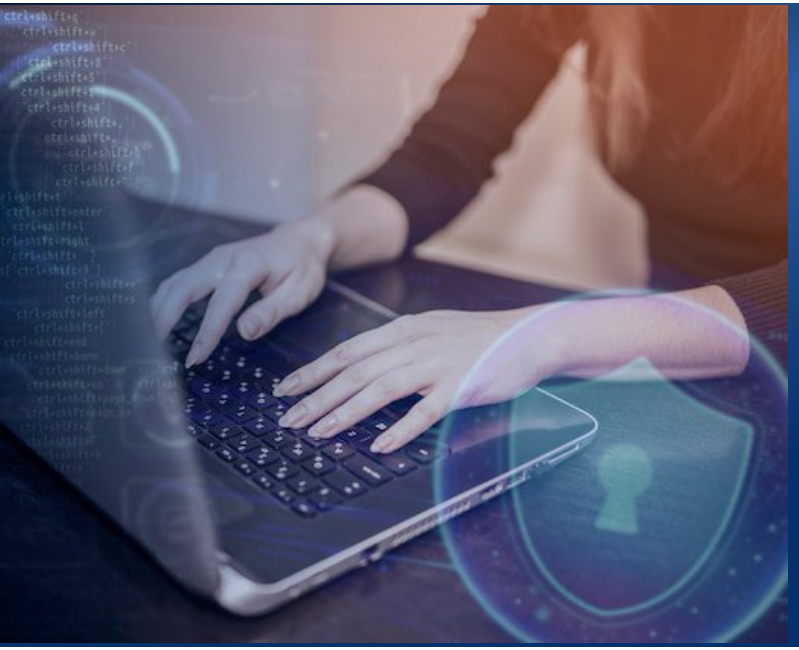
Riziká a obmedzenia šifrovania

- Strata obnovovacieho kľúča = strata dát
- Mierne zníženie výkonu (pri starších zariadeniach)
- Kompatibilita s niektorými nástrojmi (napr. zálohovací softvér)
- Nutnosť správneho nastavenia
- Potreba TPM alebo USB pri niektorých režimoch

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Odporúčania pre bezpečné šifrovanie

- Ulož obnovovací kľúč na viac miest
- Používaj silné heslá alebo PIN
- Pravidelne aktualizuj systém
- Kombinuj šifrovanie s antivírusom a zálohovaním, dvojfaktorovou authentikáciou
- V prípade firemného prostredia – centrálna správa cez Active Directory, Intune, Microsoft Endpoint Manager



Antimalvérová ochrana a HIPS

Antimalvérová ochrana

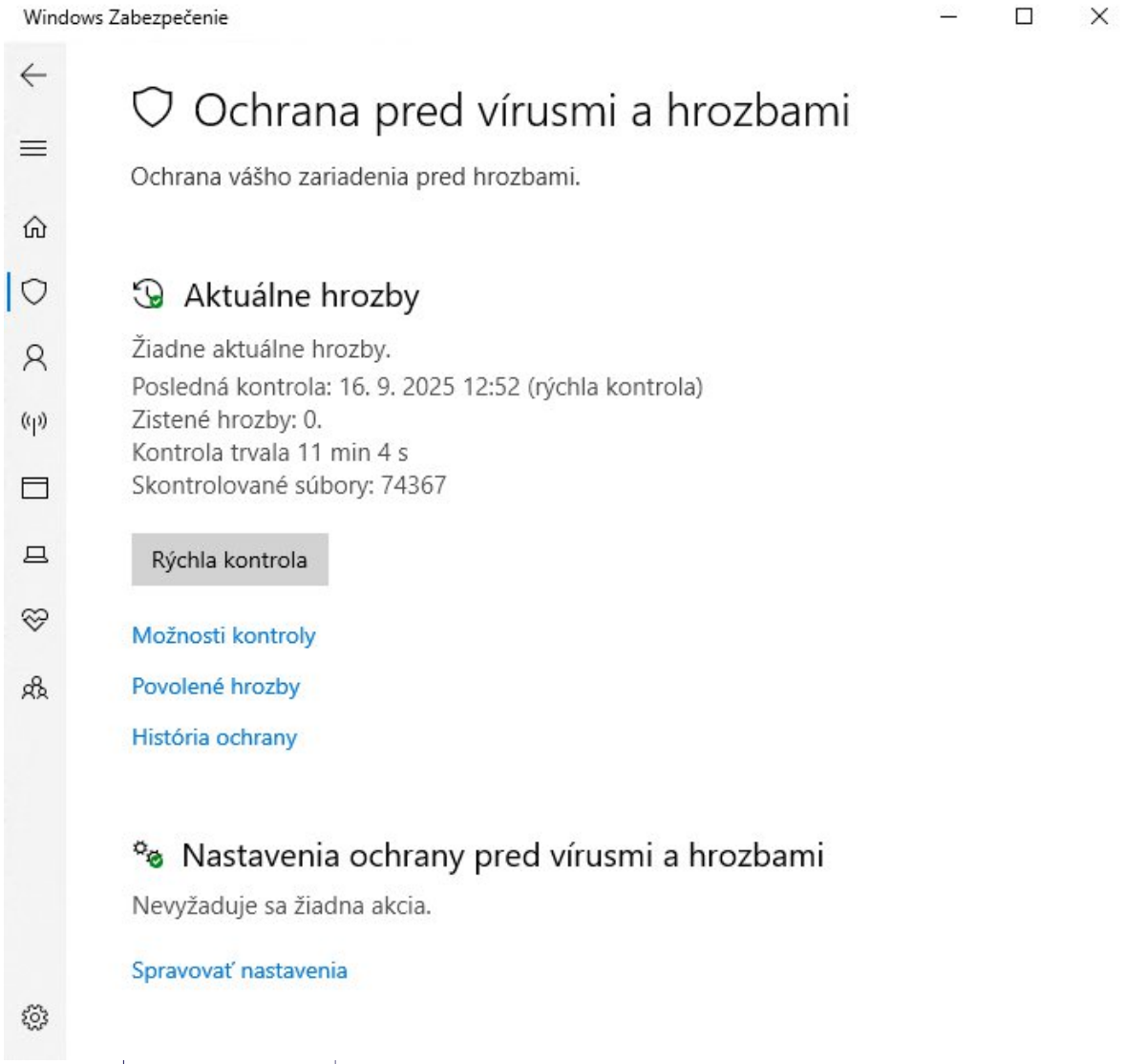
- Malvér
  - škodlivý softvér, ktorý ohrozuje bezpečnosť systému.
- Antimalvér
  - softvér na detekciu, blokovanie a odstránenie malvéru.
- Windows má vstavanú ochranu
  - Microsoft Defender Antivirus.

Typ	Popis	Príklad
Ransomvér	Šifruje súbory, žiada výkupné	WannaCry
Trójsky kôň	Vydáva sa za legitímny softvér	Emotet
Spyware	Sleduje aktivitu používateľa	Agent Tesla
Rootkit	Skrýva prítomnosť malvéru	ZeroAccess
Adware	Zobrazovanie reklám	Fireball

Najčastejšie typy malvéru vo Windows

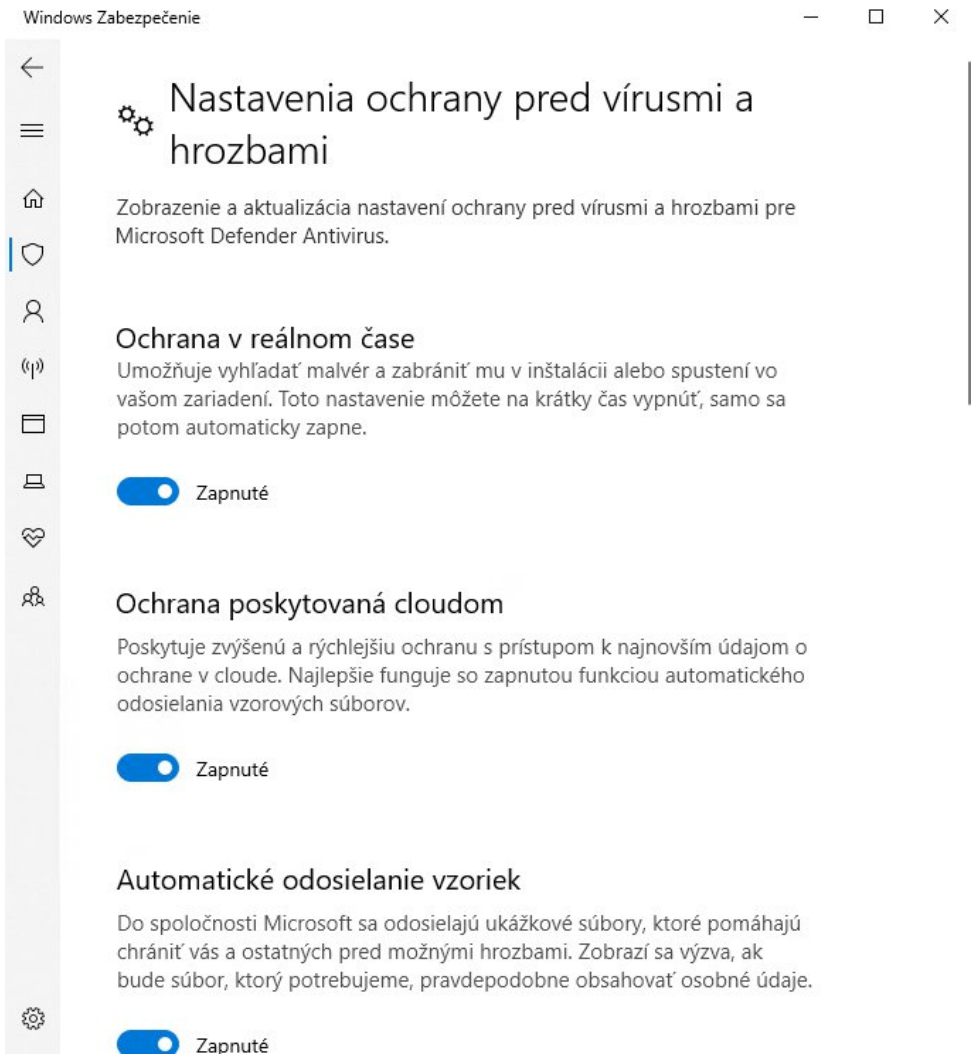
Microsoft Defender Antivirus a Windows Zabezpečenie

- Integrovaný vo Windows 10/11
- Real-time ochrana
- Cloudová detekcia
- Ochrana pred ransomware
- Automatické aktualizácie
- Integrácia s Windows Zabezpečenie
- Štart → Nastavenia → Aktualizácia a zabezpečenie → Windows Zabezpečenie



Aktivita: Microsoft Defender Antivirus

- Overenie - Zapnuté ochrany
- Spustenie rýchlej kontroly



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďalšie antimalvér nástroje pre Windows

- ESET NOD32 Antivirus
  - Ochrana v reálnom čase, detekcia malvéru a ransomware
- Norton AntiVirus
  - Ochrana v reálnom čase, detekcia malvéru a ransomware
- Kaspersky Standard Antivirus
- Bitdefender Antivirus Free
  - Ochrana v reálnom čase, detekcia malvéru, nízka záťaž systému.
- Avira Free Security
  - Antivírus, VPN (obmedzená), správca hesiel, ochrana webu.
- Malwarebytes Free
  - Manuálne skenovanie malvéru, adware, spyware.
- AVG AntiVirus Free
  - Ochrana pred vírusmi, škodlivými webmi, e-mailovými hrozbami.
- ClamWin
  - Open-source, manuálny vírus skener

Hostiteľský systém na prevenciu narušenia (HIPS)

- Host-based Intrusion Prevention System
- Monitoruje správanie aplikácií a systémových procesov (behaviorálna analýza)
- Detekuje pokusy o narušenie systému
- Vo Windows je HIPS súčasťou niektorých bezpečnostných balíkov

Funkcia	Antimalvér	HIPS
Detekcia známych hrozieb	áno	nie
Detekcia neznámych hrozieb	čiastočne	áno
Reakcia na správanie	nie	áno
Ochrana pred zero-day útokmi	čiastočne	áno

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako HIPS funguje vo Windows

- Sleduje
  - Zmeny v registroch
  - Pokusy o modifikáciu systémových súborov
  - Neštandardné sieťové spojenia
  - Spúšťanie neautorizovaných procesov

- Reaguje
  - Blokovaním
  - Upozornením
  - Logovaním

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady HIPS riešení pre Windows

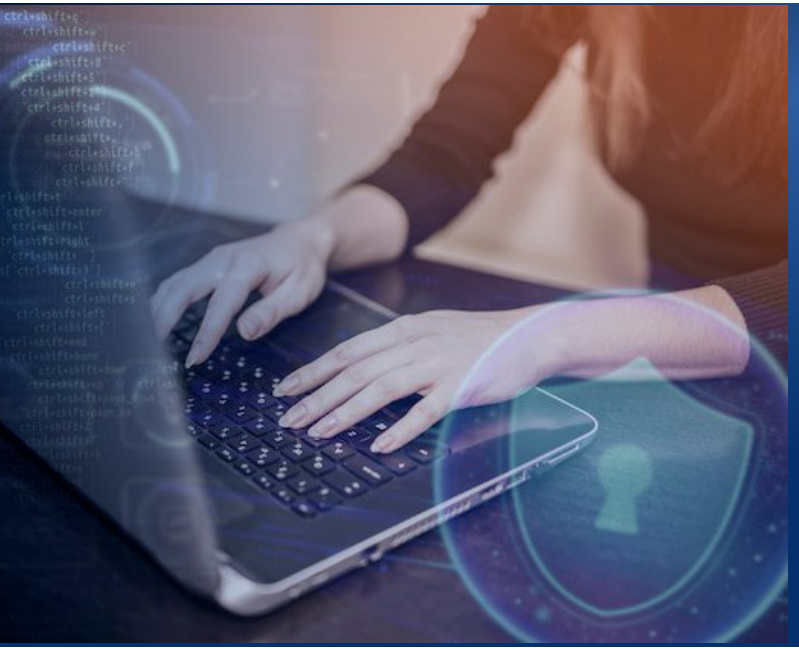
- ESET Internet Security
  - Antimalvér, HIPS, firewall
- Comodo Internet Security
  - Antimalvér, HIPS, firewall, sandbox
- Kaspersky Endpoint Security
  - Antimalvér, HIPS, firewall
- Sophos Endpoint Intercept X
  - Behaviorálna analýza

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Odporúčania pre antimalvér a HIPS

- Aktivuj real-time ochranu v Defenderi
- Pravidelne aktualizuj Windows a Defender
- Nepoužívaj viacero antimalvér programov naraz
- Vykonávaj pravidelné skeny
- Používaj HIPS v kombinácii s Defenderom alebo iným antimalvérom
- Prispôsob pravidlá podľa typu používateľa (domáci vs. firemný)
- Monitoruj logy a incidenty
- Testuj kompatibilitu s aplikáciami
- Vzdelávaj používateľov o reakciách systému

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Aplikačná bezpečnosť

Podvodné rozšírenia prehliadačov

- Rozšírenia (extensions) sú malé programy, ktoré rozširujú funkcie prehliadača (napr. Chrome, Firefox).
- Podvodné rozšírenia
  - Zbierajú citlivé údaje (heslá, históriu, cookies)
  - Zobrazujú nežiadanú reklamu (adware)
  - Presmerúvajú na škodlivé weby
  - Inštalujú ďalší malvér
- Ako rozpoznať
  - Neznámy vývojár alebo chýbajúce recenzie
  - Po inštalácii sa zmení domovská stránka alebo vyhľadávač
  - Prehnané oprávnenia (napr. čítanie všetkých údajov na navštívených stránkach)
  - Náhle spomalenie prehliadača
- https://www.techradar.com/pro/security/keep-an-eye-on-your-meta-business-account-these-fake-extensions-could-steal-your-credentials

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

AdBlocker

- Rozšírenie prehliadača, ktoré blokuje reklamy, sledovacie skripty a škodlivé prvky.

- Rýchlejšie načítanie stránok
- Menej rušivých prvkov
- Ochrana pred malvérom v reklamách (malvertising)

- Odporúčané doplnky:
  - Ghostery
  - uBlock Origin
  - AdGuard
  - Adblock Plus

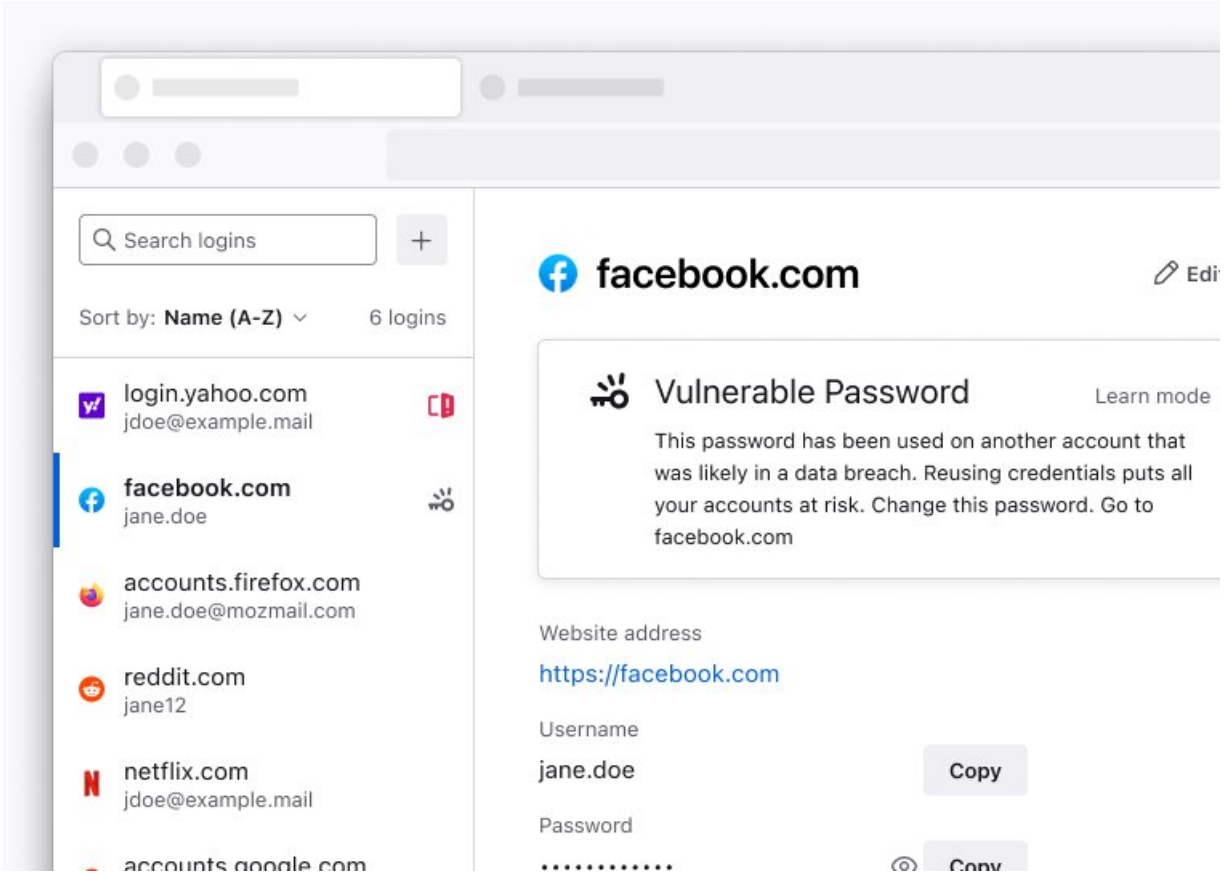
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Manažéri hesiel v prehliadači

- Ukladanie, generovanie a automatické vyplňovanie silných hesiel.

- Vo Windows prehliadačoch:
  - Microsoft Edge: integrovaný manažér hesiel + synchronizácia cez Microsoft účet
  - Google Chrome: synchronizácia cez Google účet
  - Firefox: synchronizácia
  - Nie vždy sú samotné heslá šifrované, niekedy dokonca viditeľné bez zadania hesla

- Doplnky do prehliadača od vývojárov samostatných správcov hesiel



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

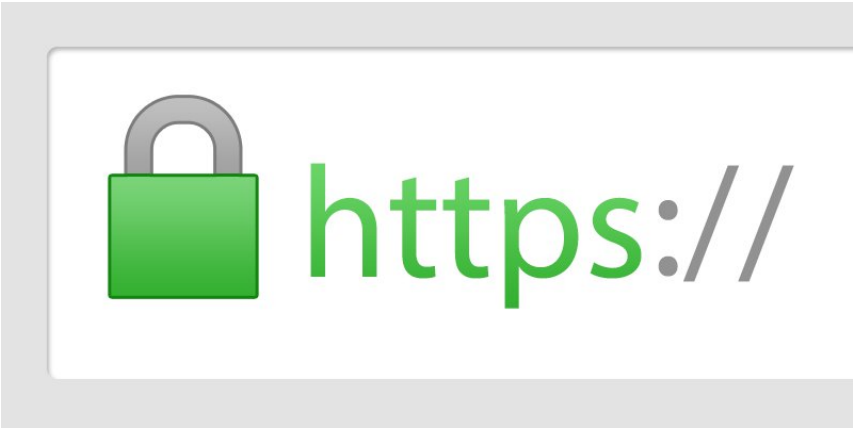
DNS služby pre vyššiu bezpečnosť

- DNS filtrácia
  - Pri pokuse o prístup na stránku DNS služba overí, či je doména na zozname
  - Ak áno, požiadavka je zablokovaná alebo presmerovaná.
- Blokuje
  - Reklamné servery
  - Malvérové stránky
  - Obsah pre dospelých alebo nevhodný obsahu
  - Niektoré služby po prihlásení umožňujú prispôsobenie
- Príklady služieb
  - Quad9 (malware block 9.9.9.9)
  - AdGuard DNS (ads, tracker block 94.140.14.14)
  - OpenDNS (ads, nevhodny obsah block 208.67.222.123)
  - NextDNS
  - CleanBrowsing

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

HTTP vs. HTTPS – bezpečnosť komunikácie

- HTTP: nešifrovaný prenos dát → riziko odpočúvania
- HTTPS: šifrovaný prenos pomocou SSL/TLS
- Ako rozpoznať bezpečnú stránku
  - Ikona zámku v adresnom riadku
  - Adresa začína na https://



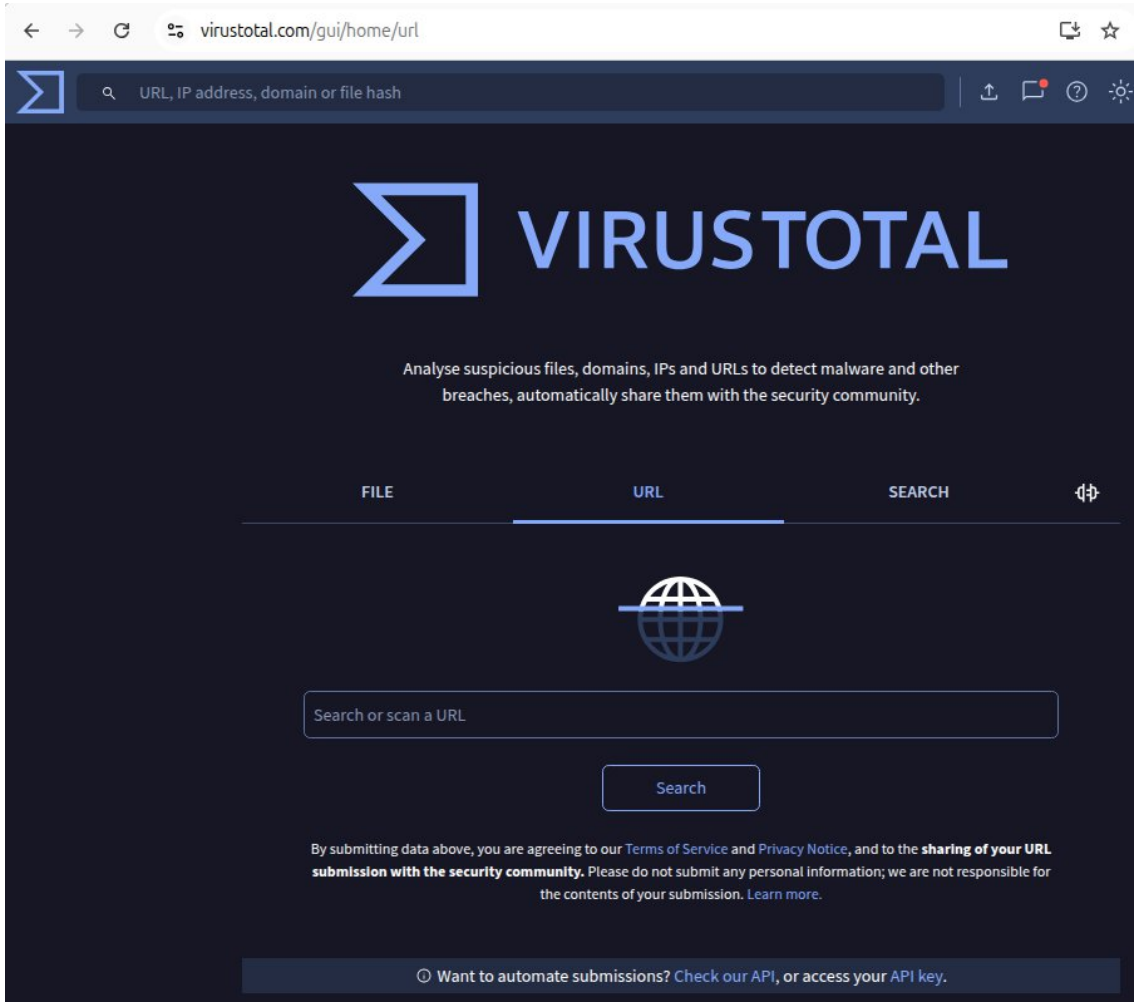
- Riziká HTTP:
  - Phishing
  - Únik prihlasovacích údajov
  - Man-in-the-middle útoky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Detekcia nekorektných URL adries

- Ako rozpoznať podvodné adresy
  - Preklepy: micros0ft.com, g00gle.com
  - Dlhé a podozrivé URL: login-secure-verification.com
  - Použitie neznámych domén: .xyz, .top, .click

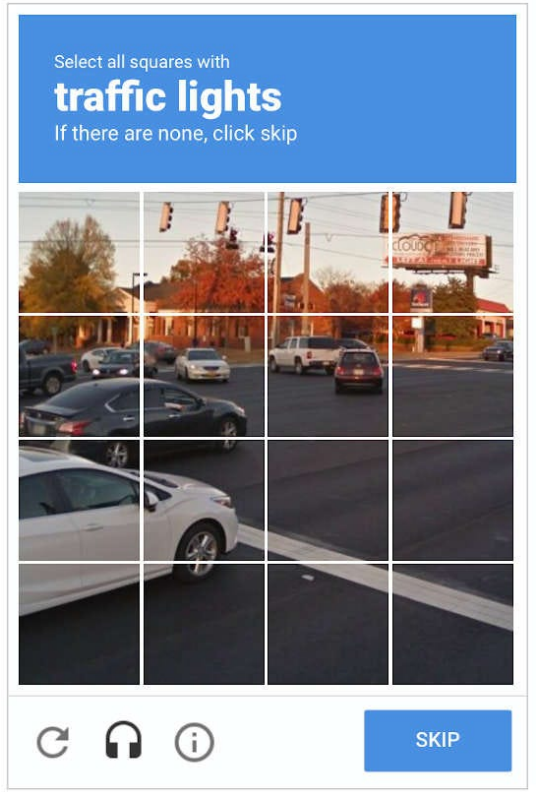
- Nástroje:
  - VirusTotal (analýza URL)
  - Microsoft Defender SmartScreen
  - Rozšírenia prehliadača na kontrolu reputácie stránok
    - WOT (Web of Trust)

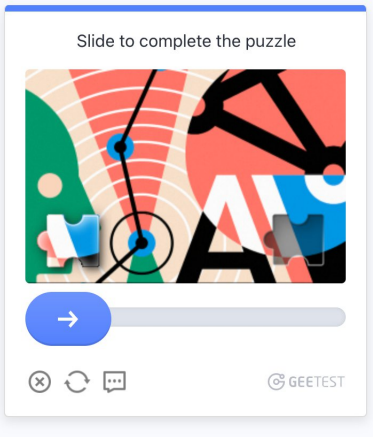


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

CAPTCHA

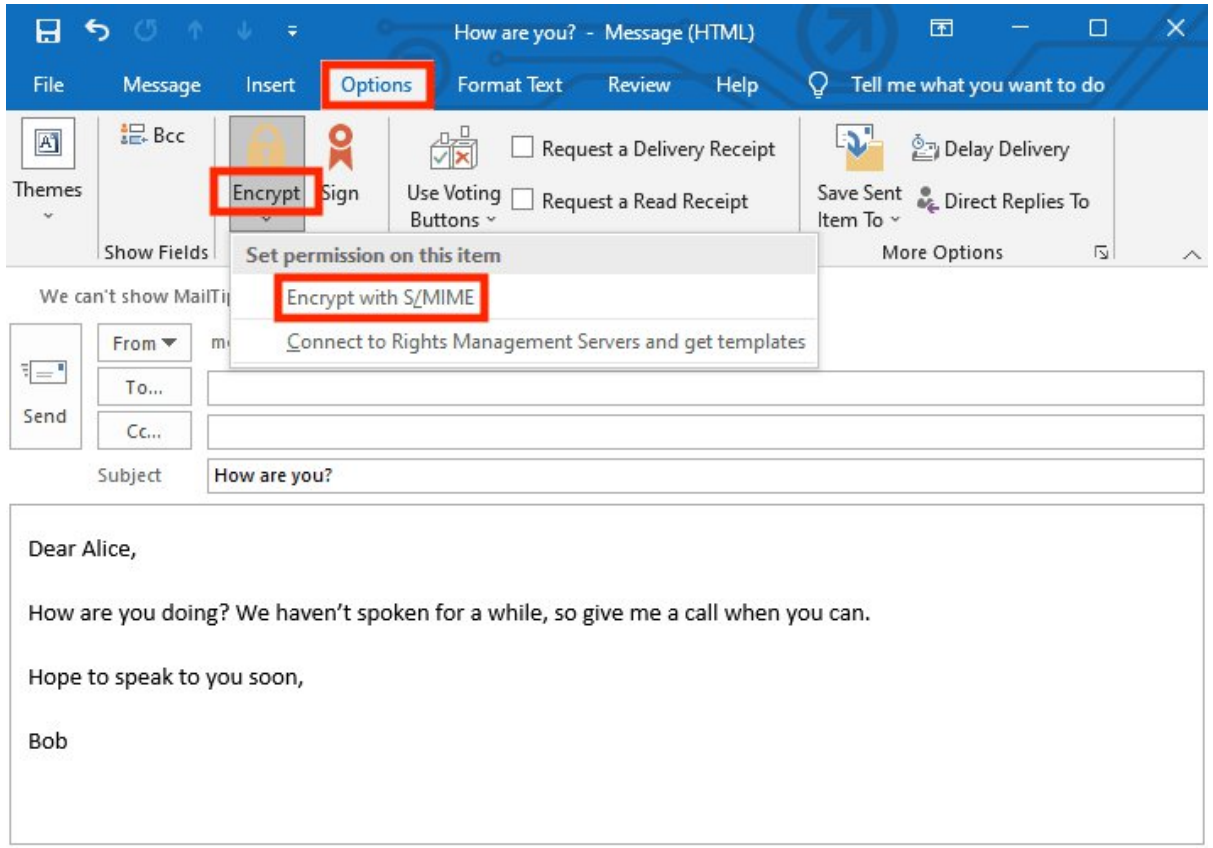
- Ochrana pred automatizovanými útokmi (botmi)
- Overenie, že používateľ je človek
- Typy
  - Textové (napíš kód)
  - Obrázkové (vyber semafory)
  - Neviditeľné (Google reCAPTCHA v3)
- Problémy
  - Niektoré CAPTCHA systémy môžu byť zneužité na sledovanie
  - Malvér môže simulovať interakciu s CAPTCHA
  - Falošné CAPTCHA stránky → phishing

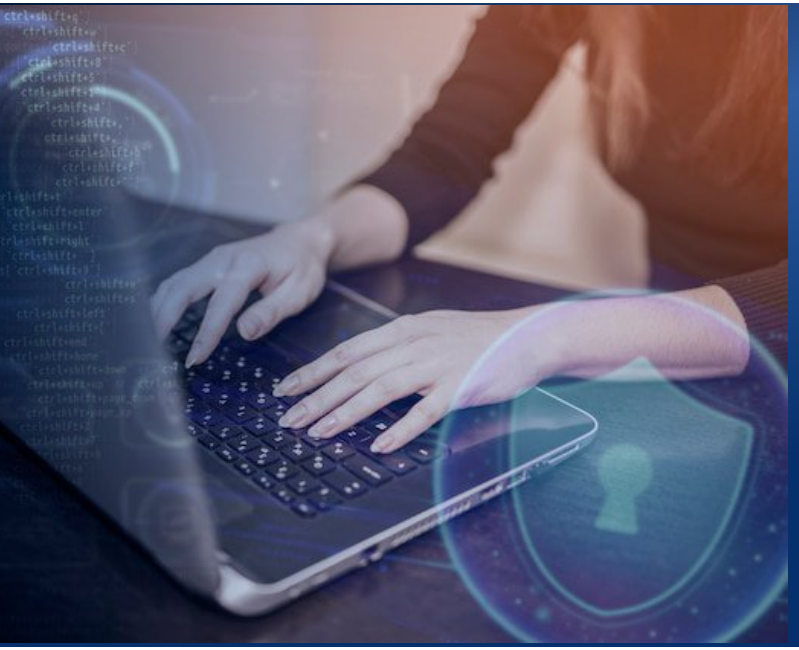




Šifrovanie emailov

- Ochrana citlivých údajov (heslá, dokumenty, osobné informácie)
- Typy šifrovania:
  - End-to-end (napr. ProtonMail, Tutanota)
  - PGP/GPG – manuálne šifrovanie pomocou verejného a súkromného kľúča
- Vo Windows:
  - Outlook podporuje S/MIME certifikáty
  - Thunderbird + Enigmail (PGP)
- Odporúčania:
  - Neposielať citlivé údaje nešifrovane
  - Používať dôveryhodné e-mailové služby





Fyzická bezpečnosť

Kontrola prístupu ku koncovému zariadeniu

- Zámky a uzamykacie mechanizmy:
  - Kensington lock (mechanický zámok pre notebooky)
  - Uzamykateľné skrinky pre stolné PC

- Autentifikácia používateľa:
  - Heslo k účtu Windows
  - PIN alebo biometria (Windows Hello – odtlačok prsta, rozpoznanie tváre)

- Automatické uzamknutie obrazovky:
  - Nastavenie časovača nečinnosti
  - Funkcia „Dynamic Lock“ (uzamknutie pri vzdialení používateľa)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana pred fyzickým poškodením

- Preventívne opatrenia:
  - Používať obaly, tašky a ochranné puzdrá
  - Vyhýbať sa extrémnym teplotám, vlhkosti a prachu
  - Nepokladať nápoje vedľa klávesnice

- Hardvérové riešenia:
  - SSD disky (odolnejšie voči otrasom ako HDD)
  - Odolné notebooky (napr. s MIL-STD certifikáciou)

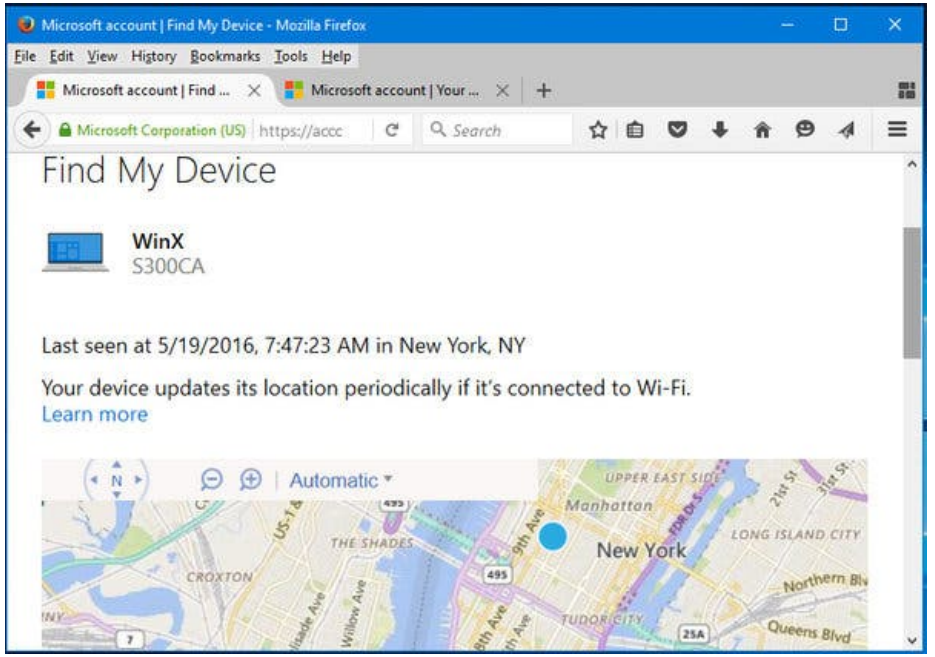
- Zálohovanie dát:
  - Pravidelné zálohy na externý disk alebo cloud
  - Obnova dát v prípade poškodenia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana pred krádežou

- Fyzické zabezpečenie:
  - Pripútanie zariadenia k pevnému bodu
  - Používanie uzamykateľných miestností alebo skriniek

- Softvérové riešenia:
  - Lokalizačné služby (napr. „Find My Device“ vo Windows)
  - Šifrovanie disku (BitLocker)
  - Vzdialené vymazanie dát (pri firemnom nasadení cez Intune)



Bezpečné likvidovanie starých zariadení

- Pred likvidáciou:
  - Odstrániť všetky osobné údaje
  - Odhlásiť sa zo všetkých účtov
  - Vymazať disk pomocou nástrojov:
    - Windows Reset → „Odstrániť všetko“
    - DBAN (Darik's Boot and Nuke)

- Fyzická likvidácia:
  - Rozbitie/skartovanie disku (ak nie je možné softvérovo vymazať)
  - Recyklácia cez certifikované firmy
  - Repasovanie

- Firemné prostredie:
  - Dodržiavanie GDPR pri likvidácii dát
  - Dokumentácia procesu likvidácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Ochrana systémov a koncových zariadení

Ochrana koncových zariadení v LAN a online bezpečnosť (Blok V)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ing. Martin Kontšek, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

martin.kontsek@uniza.sk