Windows 11 hardening manuál

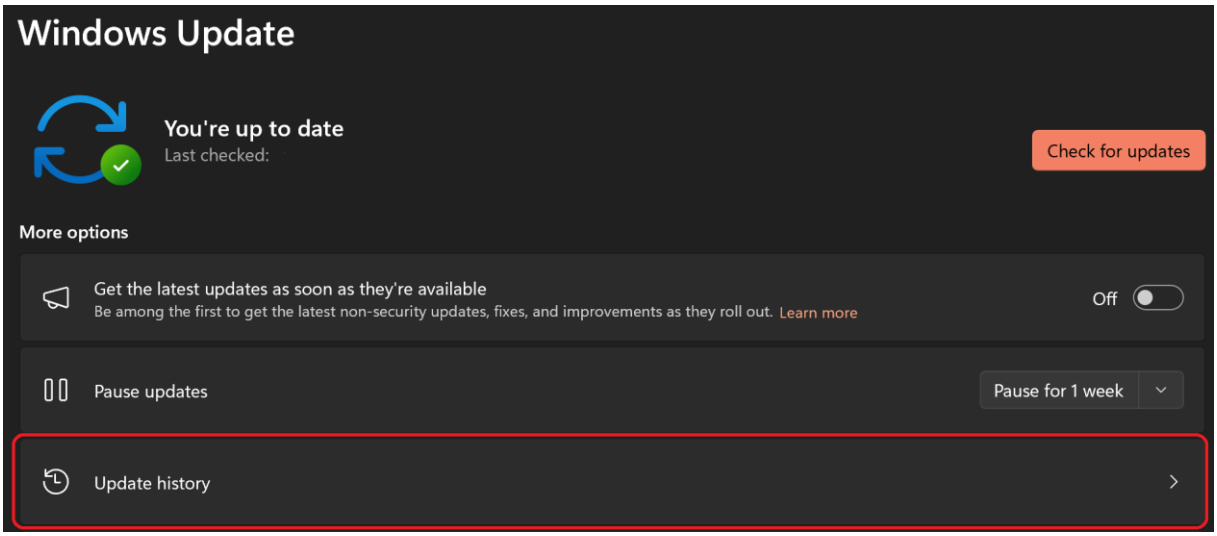
1. Pravidelná aktualizácia softvéru

Nastavenie automatických aktualizácií pre OS, firmware, ovládače a aplikácie 3. strán. Pomocou pravidelných aktualizácií a aplikácie bezpečnostných záplat dokážeme eliminovať veľkú časť bezpečnostných nedostatkov.

Automatické aktualizácie

V rámci automatických aktualizácií je vhodné si priebežne kontrolovať, či boli aktualizácie korektne nainštalované.

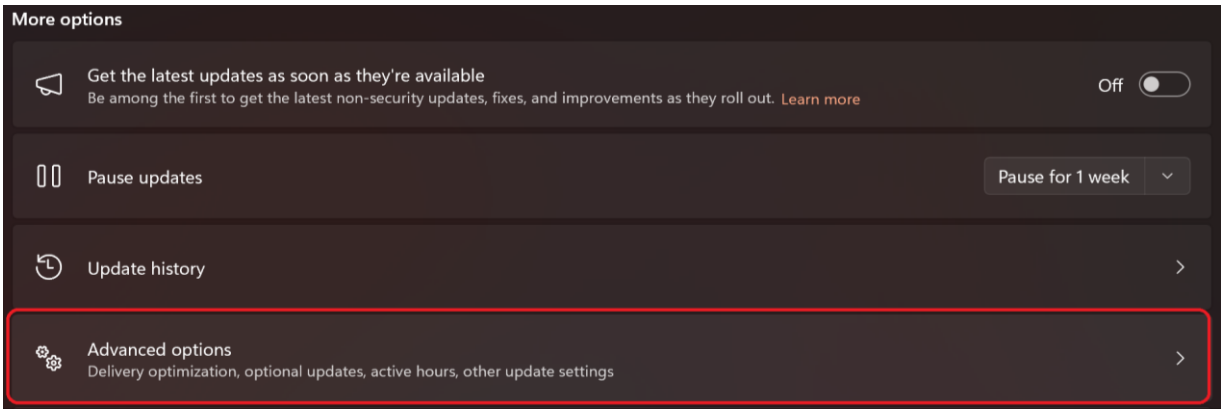
1. Otvoríme nastavenia *Windows Update*
2. V prípade kontroly korektnosti aktualizácie pod tlačidlom *Check for updates* nájdeme v prípade nesprávne nainštalovaných aktualizácií zoznam čakajúcich aktualizácií
3. V prípade, že si chceme zobraziť históriu nainštalovaných aktualizácií, prejdeme do sekcie *More options* a klikneme na možnosť *Update history*



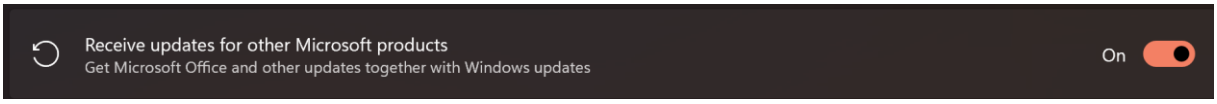
Rozšírené nastavenia

V rozšírených nastaveniach môžeme nájsť možnosti aktualizácií pre aplikácie tretích strán, ako aj pre produkty spoločnosti Microsoft.

1. Otvoríme nastavenia *Windows Update*
2. Vyberieme možnosť *Advanced options*

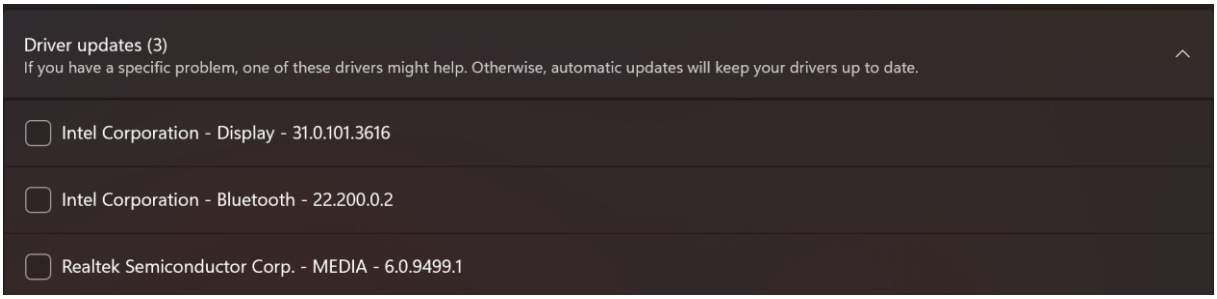


3. Povolíme nastavenia *Receive updates for other Microsoft products*



4. Pre povolenie aktualizácií aplikácií tretích strán zvolíme možnosť *Optional updates* v sekcii *Additional options*

5. Zaklikneme položky, ktoré chceme aktualizovať v rámci bežných aktualizácií



Pre aktualizácie je vhodné používať aj aplikácie výrobcov, v rámci ktorých sú kritické aktualizácie systému častokrát skôr, ako v kumulatívnej aktualizácii Microsoftu.

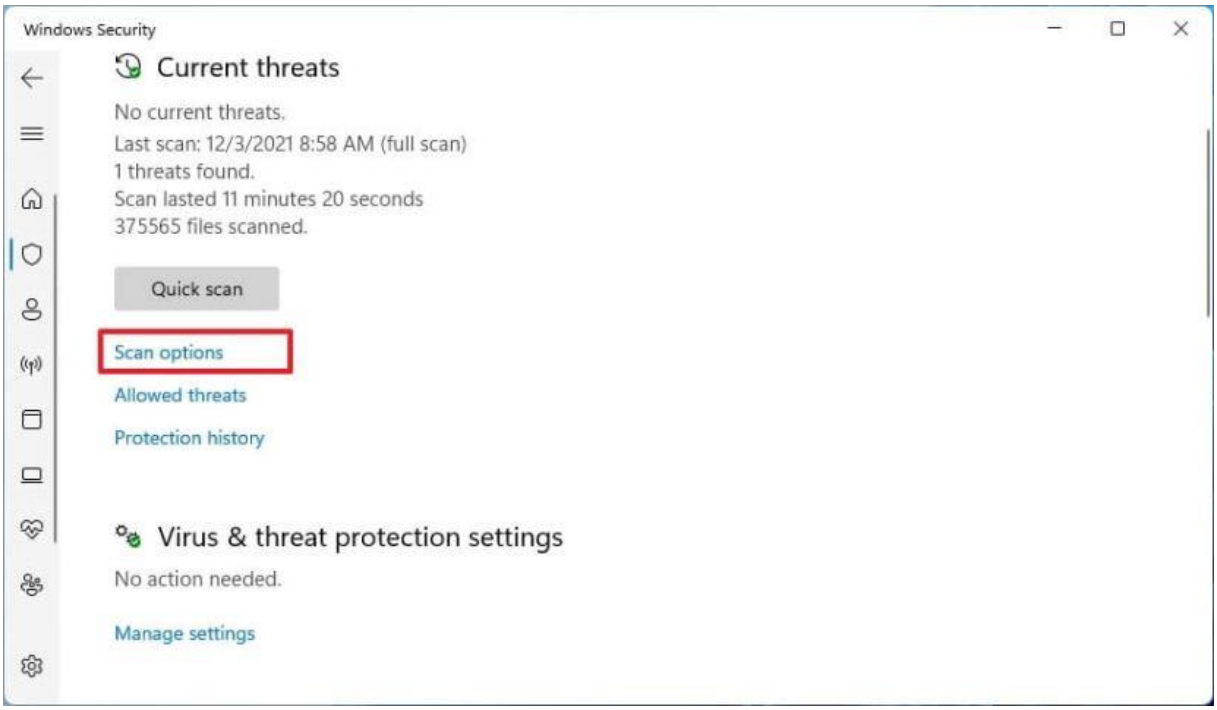
2. Antivírusová ochrana

Windows 11 disponuje antivírusom Microsoft Defender, ktorý umožňuje detekciu a riešenie väčšiny druhov malvéru. Microsoft Defender dovoľuje niekoľko druhov skenov: celkový sken, offline sken a periodický sken. Na zabezpečenie systému je však možné využiť aj aplikácie tretích strán (ESET, Bitdefender, ...)

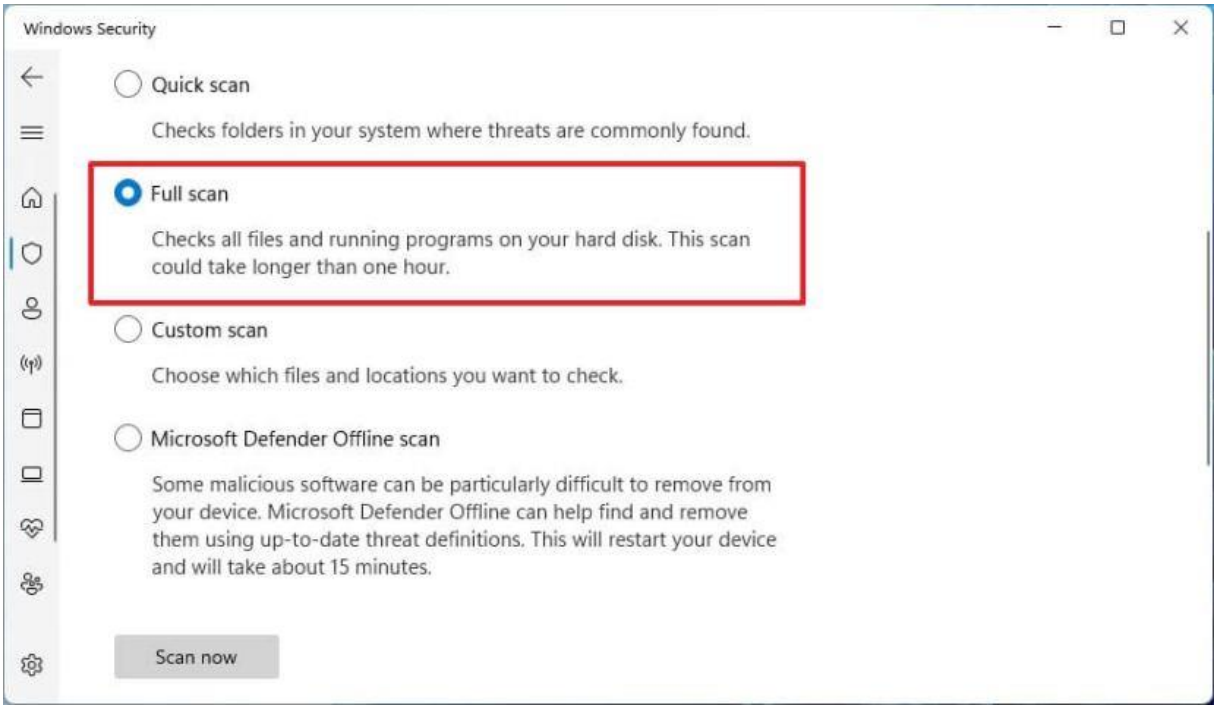
Celkový sken

Vykonávanie hĺbkového skenu systému.

1. Otvoríme nastavenia *Windows Security*
2. Klikneme na *Virus & threat protection*
3. Klikneme na položku *Scan options*



4. Vyberieme možnosť *Full scan* a klikneme na *Scan now*



Offline sken

V tomto móde sa počítač reštartuje a sken prebieha v bezpečnostnom móde na základe aktuálnych threat listov.

1. Otvoríme nastavenia *Windows Security*
2. Klikneme na *Virus & threat protection*
3. Klikneme na položku *Scan options*
4. Vyberieme možnosť *Microsoft Defender Offline scan* a klikneme na *Scan now*

Periodický sken

Periodické skeny sú najlepším spôsobom prevencie a zároveň slúžia na odstraňovanie hrozieb, ktoré neboli zachytené ostatnými bezpečnostnými prvkami.

1. Otvoríme nastavenia *Windows Security*
2. Klikneme na *Virus & threat protection*
3. Klikneme na *Microsoft Defender Antivirus options*
4. Zapneme prepínač *Periodic scanning*

Ransomware ochrana

Kontrolovaný prístup je ďalším užitočným krokom obrany voči ransomware útokom. Pokiaľ sa aplikácia pokúsi o zmenu súborov v chránenej oblasti, aplikácia je zapísaná na *blacklist* a používateľ je oboznámený o podozrivej aktivite.

1. Otvoríme nastavenia *Windows Security*
2. Klikneme na *Virus & threat protection*
3. Klikneme na *Manage ransomware protection* pod položkou *Ransomware protection*
4. Zapneme prepínač *Controlled folder access*

3. Nastavenia zdieľania a tlače

Zdieľanie súborov a tlačiarní môže viesť k neoprávnenému prístupu k citlivým informáciám. Preto je vhodné, aby sme zdieľanie nepovolili, pričom prístup jednotlivca k tlači a súborom sa takto neobmedzí. Zdieľaniu vieme následne zamedziť dvomi spôsobmi:

1. Vypnutie v nastaveniach: *Network & internet > Advanced network settings > Advanced sharing settings > File and printer sharing*
2. Aplikovanie nastavení *Group policy* pomocou *Local Group Policy Editor*:
    a. *Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup* a nastavenie *Prevent the computer from joining a homegroup* na *enabled*
    b. *User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing* a nastavenie *Prevent users from sharing files within their profile* na *enabled*

4. Použitie firewall-u

Firewall nám umožňuje monitorovanie prichádzajúcej a odchádzajúcej sieťovej komunikácie a následne povolenie, resp. blokovanie daného spojenia. Na zabezpečenie systému je však možné využiť aj aplikácie tretích strán (Norton, SolarWinds, ...)

1. Otvoríme nastavenia *Windows Security*

2. Klikneme na *Firewall & network protection*
3. Vyberieme aktívnu sieť
4. Povolíme *Microsoft Defender Firewall*

5. Použitie Microsoft account (Windows Hello)

Zabezpečenie prostredia môžeme zvýšiť implementáciou biometrických údajov pomocou nastavenia *Windows Hello.* Tieto nastavenia nám umožňujú využiť biometriu tváre, biometriu odtlačkov prstov (ak je na zariadení dostupný skener), prípadne PIN, ktorý je bezpečnejší ako štandardné heslo a poskytuje dobrý kompromis, nakoľko je možné v rámci PIN využiť aj frázy, nie len číselné kódy.

1. Otvoríme nastavenia *Accounts*
2. Klikneme na *Sign-in options*
3. V rámci následných možností si vyberieme konkrétny spôsob zabezpečenia pomocou biometrie

4. Pokračujeme na základe pokynov ku korektnému nastaveniu vybraného zabezpečenia

6. Inštalácia aplikácií z dôveryhodných zdrojov

Windows Security disponuje možnosťou *Reputation-based protection settings*, ktorá poskytuje ochranu voči nechceným aplikáciám, súborom a webstránkam. Toto nastavenie umožňuje detekciu a blokovanie aplikácií a súborov s nízkou reputáciou. Ideálnym riešením predchádzania inštalácie škodlivých aplikácií je inštalácia z dôveryhodných zdrojov, ako napr. Microsoft Store.

1. Otvoríme nastavenia *Windows Security*
2. Klikneme na *App & browse control*
3. Klikneme na *Reputation-based protection settings*
4. Zapneme nastavenie *Potentially unwanted app blocking*
5. Zaklikneme možnosti blokovania *Block Apps* a *Block downloads*

7. Povolenie šifrovania (Bitlocker)

Bitlocker je ďalším z dôležitých bezpečnostných nastavení, ktoré nám umožňuje šifrovanie disku a následnú ochranu dát v prípade nepovoleného prístupu k nim (dostupné len pre verziu Windows 11 Pro). **Dešifrovací kľúč je vhodné uložiť na bezpečnom mieste mimo daný PC, pre prípad problému so zariadením.**

1. Otvoríme nastavenia *Privacy & Security*
2. Klikneme na *Device encryption* v časti *Security*

3. Zapnutie nastavenia *Device encryption*

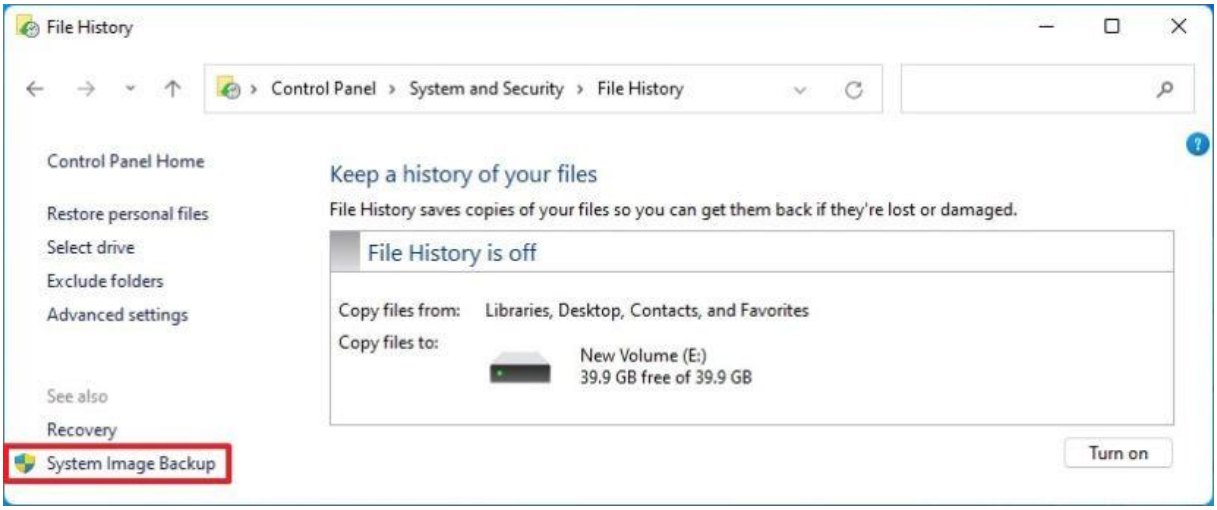
8. Zálohovanie dát

Vytváranie systémových záloh je dôležité v prípade kritického narušenia systému. Windows 11 umožňuje vytvorenie zálohy celého systému, avšak je možné použiť aj aplikácie tretích strán. Zálohu systému je následne vhodné udržiavať na externom offline úložisku pre prípad problému s PC. V rámci zálohovania vieme vykonať celkovú zálohu alebo pravidelnú inkrementálnu zálohu:

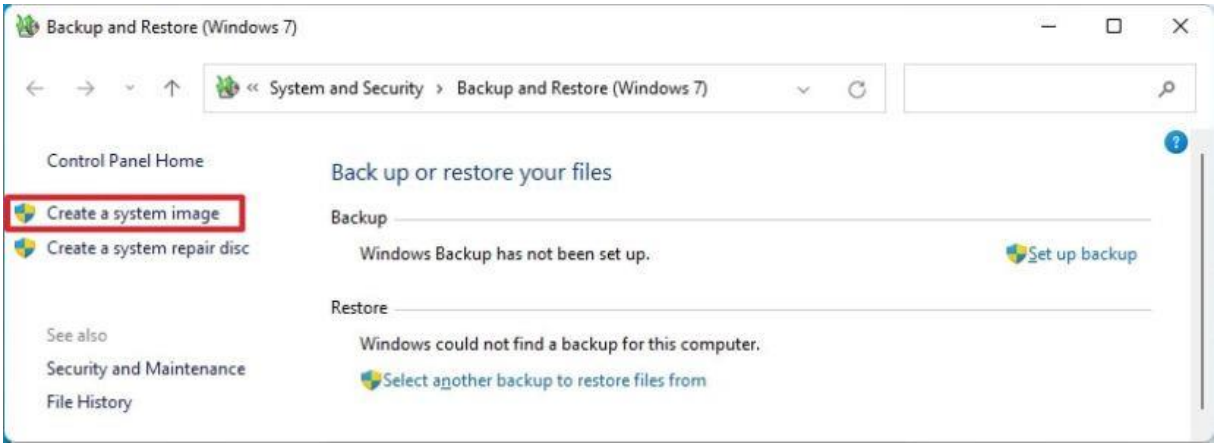
- **Celková záloha** predstavuje úplnú zálohu systému. Ich nevýhodou je časová náročnosť, a teda nie sú vhodné na dennú zálohu.
- **Inkrementálna záloha** zálohujú len tie dáta, ktoré boli zmenené od poslednej zálohy. Ide o rozumný kompromis medzi objemom zálohovaných dát a rýchlosťou vykonania zálohy.

1. Otvoríme okno kontrolného panelu
2. Klikneme na *System and Security*
3. Klikneme na *File History*

4. Klikneme na *System Image Backup* z bočného menu



5. Klikneme na *Create a system image*



6. Ďalej postupujeme podľa pokynov dialógových okien

9. Nastavenia User Account Control (UAC)

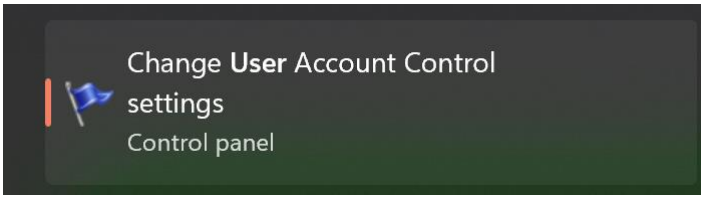
Nastavenia UAC umožňujú obmedziť prístup len vybraným používateľom tým, že pred výkonom citlivých operácií systém požiada o prihlasovacie údaje do systému (je nutná autorizácia). Vynútenie autorizácie je možné aplikovaním nastavení Group policy pomocou Local Group Policy Editor. V sekcii *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options* vykonáme nasledovné zmeny:

User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests

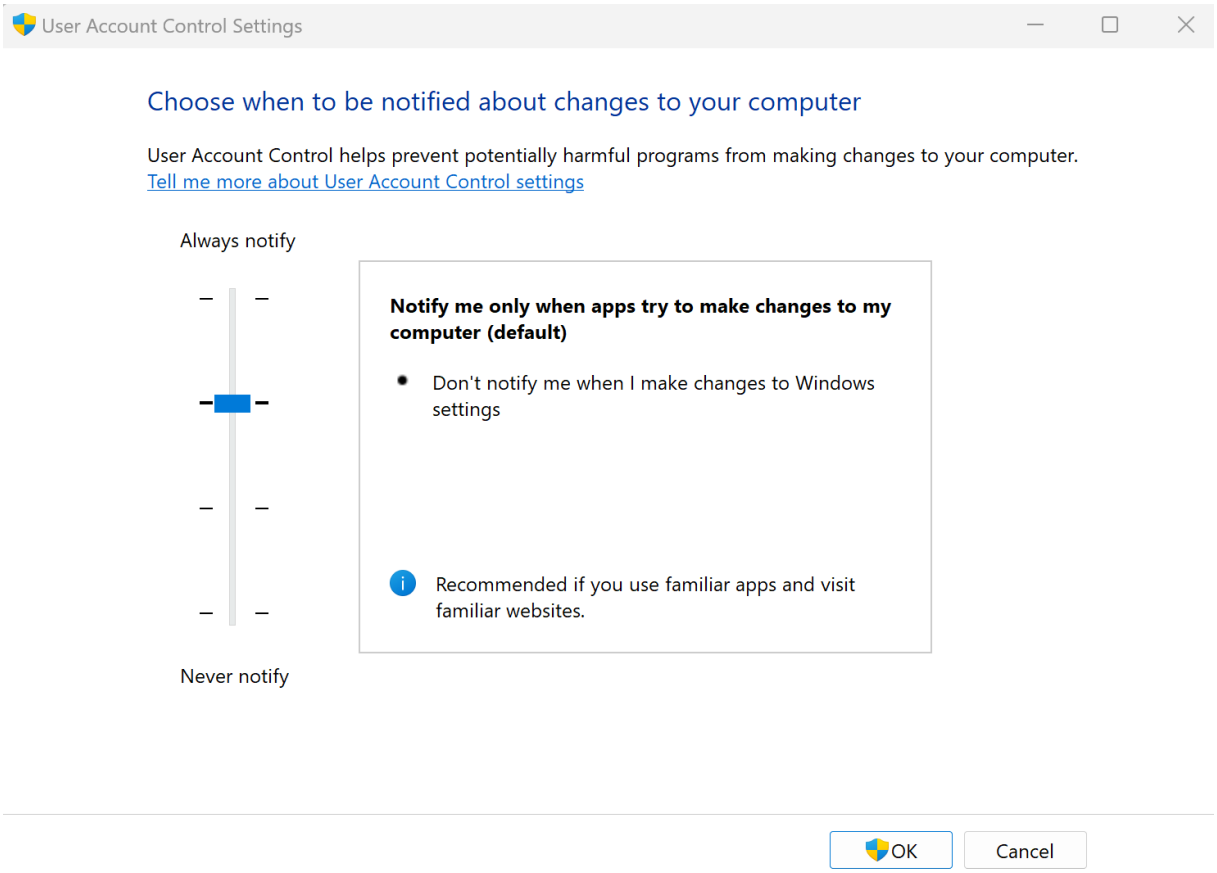
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Pre prípad rýchlejšieho prístupu k zmenám je možné použiť aj grafické rozhranie.

1. Vo vyhľadávaní PC nájdeme *Change User Account Control settings*



2. Zmeníme nastavenia podľa našich preferencií



10. Zákaz automatického spustenia pripojiteľných USB zariadení

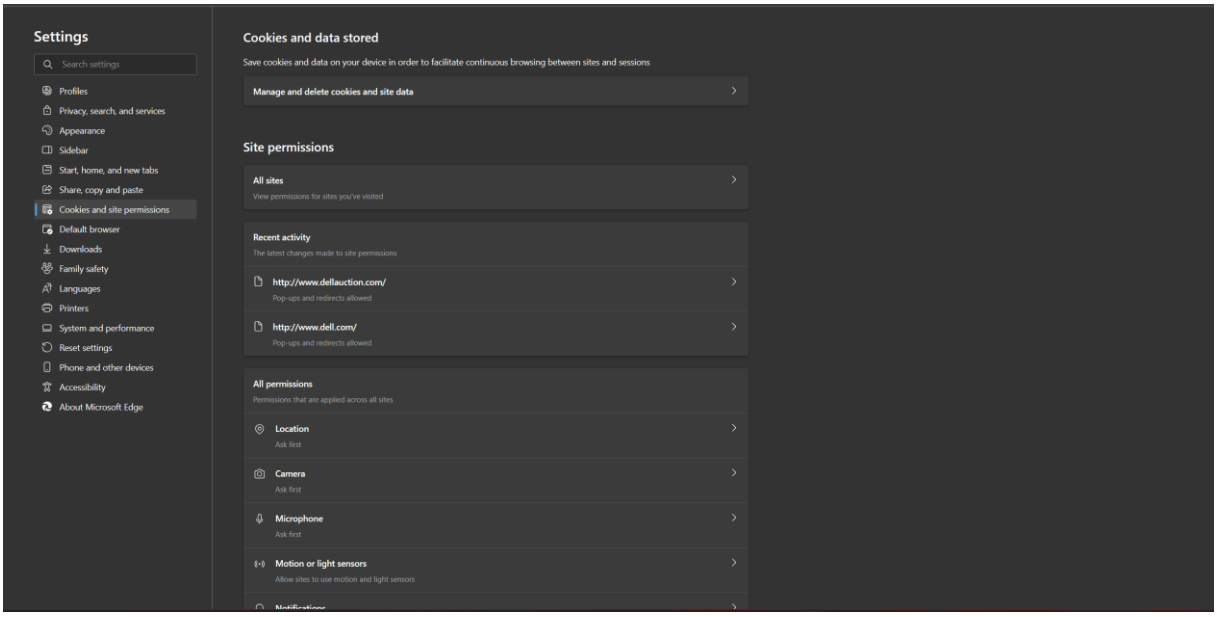
Zakázanie automatického spustenia USB zariadení zabezpečí izoláciu škodlivého SW pre prípad pripojenia infikovaného USB zariadenia. SW sa spustí až po interakcii používateľa.

1. Otvoríme nastavenia *Bluetooth & devices*
2. Klikneme na položku *AutoPlay*
3. Vypneme nastavenie *Use AutoPlay for all media and devices*

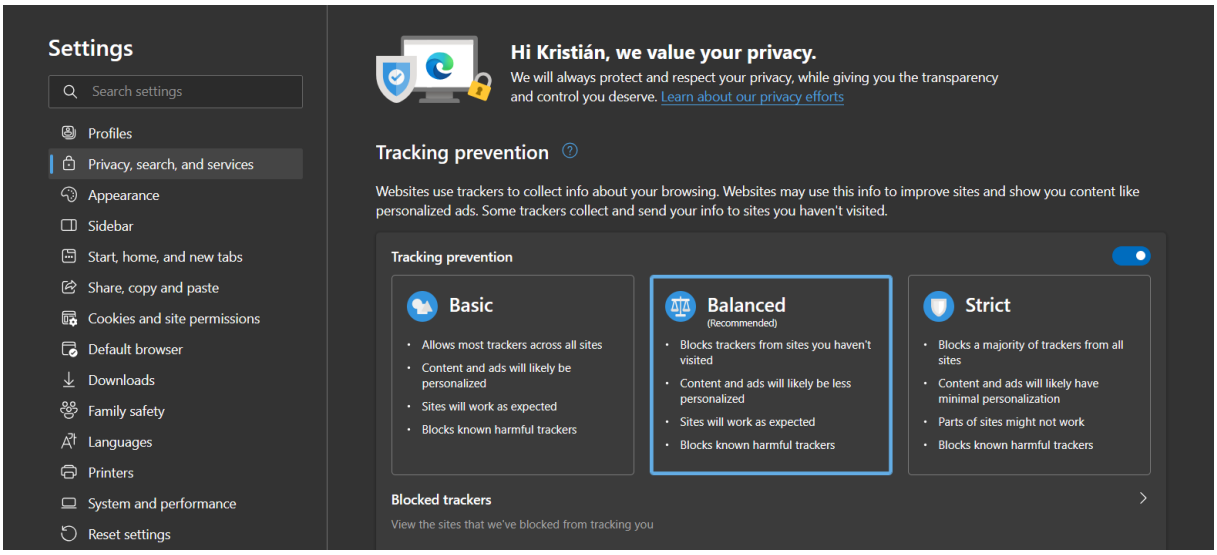
11. Zabezpečenie webového prehliadača

Nakoľko je webový prehliadač bránou do internetu, tak je aj najčastejšie vystavovaný externým vplyvom. Z tohto dôvodu je jeho zabezpečenie mimoriadne dôležité. V rámci tohto manuálu si spomenieme prehliadač Microsoft Edge.

1. Aktualizácia: rovnako ako pri iných aplikáciách, tak aj tu platí dôležitosť aktualizácií a implementácie bezpečnostných záplat
2. Používanie rozšírení: používanie a implementácia rozšírení len z dôveryhodných zdrojov
3. Používanie netriviálnych hesiel/správcu hesiel (neukladajte heslá do prehliadača, využívajte služby na to určené, napríklad KeePass (offline), Bitwarden (online), a podobne)
4. Zmena nastavení kamery, mikrofónu, a pod., nakoľko tieto nastavenia nie sú preberané zo systému Windows



5. Zmena nastavení ochrany osobných údajov na základe množstva dát, ktoré chceme prehliadaču poskytnúť.



12. Povolenia Privacy & security

Nastavenia *Privacy & security* obsahujú množstvo povolení, ktoré je možné v prípade neoprávneného prístupu k zariadeniu zneužiť. Preto je potrebné určiť, ktoré aplikácie majú prístup k jednotlivým zdrojom (kamera, poloha, mikrofón, kalendár a pod.).

1. Otvoríme nastavenia *Privacy & security*
2. Prejdeme do sekcie *App permissions* a vyberieme príslušný zdroj
3. Vypneme prístup pre špecifickú aplikáciu, resp. pre zariadenie ako také

13. Reportovací systém

Využívanie reportovacieho systému rozširuje databázu *Windows Error Reporting server*. Tá nám následne pomáha rýchlejšie riešiť incidenty, prípadne predchádzať problémom. Povolenie reportov je možné aplikovaním nastavení Group policy pomocou Local Group Policy Editor *Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds*: nastavenie *Allow Telemetry* na povolené.

V rámci telemetrie je vhodné držať sa postupov uvedených v:
https://www.csirt.gov.sk/wp-content/uploads/2021/08/MS_Telemetria_1.06.pdf

14. Kontrola automaticky spúšťaných aplikácií

Automatické spúšťanie aplikácií pri štarte poskytuje priestor pre zneužitie zraniteľných aplikácií bez vedomia používateľa. Preto je dôležité kontrolovať, ktoré aplikácie disponujú právami na automatické spustenie.

1. Otvoríme nastavenia *Apps*
2. Prejdeme do sekcie *Startup*
3. Vypneme automatické zapnutie pre neželané aplikácie