ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

CSIRT.SK
Microsoft Windows Telemetria
Odporúčanie

TLP: White

Vypracoval: CSIRT.SK

Čo je to Microsoft Windows Telemetria?

Telemetria v systémoch Windows je nástroj, ktorým spoločnosť Microsoft získava potrebné údaje zo zariadení. Patria sem napríklad údaje: systém Windows, programy systému Windows, programy tretích strán, ale aj dáta z hardvérových zariadení a periférií, ktoré boli alebo sú k systému pripojené.

Taktiež zahŕňa údaje o ich fungovaní a správaní v rámci systému Windows. Telemetria je teda nástroj, ktorý zbiera potrebné údaje a informácie o používaní systému, ako samotným užívateľom systému Windows, tak aj zariadeniam k nemu pripojených, vrátane periférnych a samotného hardvéru pracovných staníc. Obsahuje tiež údaje na zlepšenie kvality používania služieb systému Windows, ktoré pomáhajú Microsoftu zlepšovať použiteľnosť systému v závislosti od správania používateľa alebo hardvérového zariadenia, aby sa dosiahla čo najvyššia kvalita a optimalizácia v rámci prostredia Windows.

Načo využíva spoločnosť Microsoft údaje Windows Telemetrie?

- Automatická kontrola aktualizácii systému Windows na pozadí
- Monitoring štandardného zabezpečenia, výkonu a spoľahlivosti systému Windows
- Zlepšovanie použiteľnosti systému Windows na základe používania užívateľom
- Pochopenie, ako používateľ využíva alebo nevyužíva systém Windows a jeho súčasti
- Monitorovanie správania hardvéru a periférií, ktoré boli použité alebo sa aktuálne používajú v rámci systému
- Monitoring aplikácii vrátane aplikácií tretích strán, ktoré sú nainštalované v systéme, ich správanie a využívanie prostriedkov systému
- Monitoring informácií o spoľahlivosti alebo zlyhaní ovládačov zariadení v systéme
- Monitoring a škálovanie Cloudovej služby Cortana, informácie o používaní tejto služby
- Monitoring využívania a prispôsobovania ponuky Štart systému Windows používateľmi

Je všeobecne známe, že spoločnosť Microsoft využíva tieto dáta na identifikáciu problémov so zabezpečením, spoľahlivosťou a zlyhaním v systémoch Windows. Na základe týchto dát analyzuje problémy, čím môže zlepšovať kvalitu systému Windows. Telemetria tak pomáha v rozhodnutiach o budúcich zmenách a vývoji systému Windows. Inak povedané, Windows telemetria umožňuje každému používateľovi mať ako keby hlas pri vytváraní budúcich verzií systému Windows. Na základe toho vy poskytujete rýchlu spätnú väzbu Microsoftu a ten môže v krátkom čase na ňu reagovať, napríklad definovaním nových funkcií systému alebo zlepšovaním kvality používania Windows.

Treba poznamenať, že zber dát pomocou telemetrie používania nie je špecifický len pre spoločnosť Microsoft. V súčasnosti tento zber dát aplikujú aj iné spoločnosti v rámci IT segmentu.

Spoločnosť Microsoft rozdeľuje zbierané dáta na **telemetrické** a **funkčné**.

Funkčné dáta sú dáta, ktoré si vymieňajú aplikácie a komponenty systému Windows za účelom poskytovania informácií alebo funkcií používateľovi, ktoré požaduje. Základným príkladom je lokalizačná služba Microsoft (údaje o polohe), ktorej informácie potrebuje napríklad služba **Počasie** na zobrazenie aktuálneho počasia, prípadne služba **Lokálne správy**, na poskytnutie týchto informácii pre presnú lokalitu, kde sa práve nachádzate. Funkčné dáta je možno úplne zablokovať napríklad vypnutím služby údaje o polohe. Samozrejme úplné vypnutie funkčných dát vypne funkčnosť aplikácií, ktoré sú na nich závislé.

Telemetrické dáta sa nedajú úplne vypnúť, ale len v závislosti od používanej edície sa dajú minimalizovať na úroveň **Security** resp. **Basic**. Je odporúčané prepnutie telemetrie na čo možno najnižšiu úroveň.

Dôležité: Windows Telemetria sa vzťahuje len na súčasti systému Windows, Windows Server, System Center a aplikácie, ktoré používajú súčasti **Windows User Experience.** Aktuálne (Windows 10 – 1903, Windows Server 2019 a nižšie vydania) je možné nastaviť úroveň telemetrie nasledovne:

- Pre edíciu Windows 10 Enterprise a Education – **maximálna úroveň 0 Security**
- Pre edície Windows 10 Pro a nižšie – **maximálna úroveň 1 Basic**

Všetky dáta zhromažďované a prenášané pomocou telemetrie sú Microsoftom automaticky šifrované cez SSL a presúvané do Microsoftu cez Microsoft Data Management Service. Prenos týchto dát prebieha pravidelne, vždy keď je zariadené pripojené k internetu.

Telemetrické dáta, ktoré sú zasielané do Microsoftu sú uchovávané v skrytom priečinku umiestnené **C:\ProgramData\Microsoft\Diagnosis**. Tieto dáta sú však šifrované no je možné k nim získať prístup.

Prehľad úrovní Telemetrie

Security (úroveň 0) – Poskytujú sa len nevyhnutné údaje potrebné na zabezpečenie a ochranu systému Windows. Medzi tie patrí napríklad:

- Informácie o operačnom systéme (Verzia, Aktualizácie)
- ID zariadenia (HW Info)
- Trieda zariadenia (Server/Desktop/Notebook)
- Správa skenovaní prostredníctvom nástroja na odstránenie škodlivého kódu (MSRT)
- Ak sa používa, tak údaje z Windows Defendera a Firewall hlásenia

Basic (úroveň 1) – Poskytuje všetky dáta z úrovne 0 a naviac podrobnosti o stave aplikácií ich zmenách, koľko pamäte a času procesora použili. Údaje o kompatibilite a iné:

- Verzia programu Internet Explorer
- Atribúty zariadení, batérie, sieťové napríklad počet sieťových adaptérov alebo MAC adresa
- Atribúty procesora a pamäte, ako je počet jadier, veľkosť pamäte, alebo architektúra
- Atribúty ukladania, ako je počet pevných diskov, typ diskov a veľkosť
- Atribúty operačného systému, ako napríklad vydanie systému Windows a stav virtualizácie
- Atribúty virtualizácie, ako napríklad Host Operating System alebo podpora SLAT
- Informácie o Microsoft Store zahŕňajú počet stiahnutých aplikácií, inštalácie a aktualizácie
- Zoznam nainštalovaných aplikácií vrátane názvov aplikácií, informácií o vydavateľovi, verzií
- Údaje o spúšťaní, používaní, zameraní aplikácií a ako dlho sú jednotlivé aplikácie otvorené
- Systémové údaje, ktoré spoločnosť Microsoft používa na určenie, či zariadenie spĺňa minimálne požiadavky na aktualizáciu na nasledujúcu verziu systému Windows. Zahŕňa informácie o procesore a systéme BIOS.
- Zoznam prídavných zariadení, ako sú tlačiarne alebo externé pevné disky. Informácie o kompatibilite tiež určujú, či sú kompatibilné s ďalšou verziou systému Windows.
- Údaje o nainštalovaných ovládačoch vrátane toho, či sú kompatibilné s ďalšou verziou systému Windows

Enhanced (úroveň 2) - Poskytuje všetky dáta úrovne 0, 1 a ešte zahŕňa údaje, ktoré popisujú užívateľský komfort v operačnom systéme a pri používaní aplikácií. Vďaka týmto dátam Microsoft môže vylepšovať a určovať lepšie smer pre budúce aktualizácie a vylepšenia systému.

- Udalosti operačného systému (Event Log) vrátane sieťovania, Hyper-V, Cortana, disky a ukladanie, súborový systém
- Udalosti aplikácií operačného systému a nástrojov na správu od spoločnosti Microsoft, ktoré sa prevzali z Microsoft Store alebo sa predinštalovali s operačným systémom (napríklad Microsoft Edge, Mail alebo Photos)
- Udalosti pre špecifické zariadenia napríklad Surface Hub alebo Microsoft HoloLens
- Zoznam zlyhaní a pádov operačného systému

Full (úroveň 3) – Ide o predvolené (default) nastavenie systému Windows pre všetky edície ktoré nie sú Enterprise, Education a Server. Poskytuje všetky dáta úrovne 0,1,2 a naviac napríklad:

- Použitie aplikácií, spustenie a dĺžka trvania spustenia každej aplikácie
- Používanie prehliadačov vrátane histórie prehliadania a hľadaných výrazov
- Rozšírené hlásenia chýb, ako napríklad stav pamäte zariadenia, kedy došlo k zlyhaniu systému, alebo aplikácie
- Stav a zaznamenávanie informácií o operačnom systéme
- Ďalšie údaje o zariadeniach, informácie o konektivite a konfiguračné údaje nad rámec toho, čo sa už zhromažďuje na úrovni 1

Servery slúžiace na zber telemetrie:

- Informácie o používateľských skúsenostiach a telemetria - v10.vortex-win.data.microsoft.com a settings-win.data.microsoft.com
- Hlásenie chýb systému Windows - watson.telemetry.microsoft.com
- Online analýza zlyhaní - oca.telemetry.microsoft.com
- Aplikácia OneDrive pre systém Windows 10 - vortex.data.microsoft.com/collect/v1

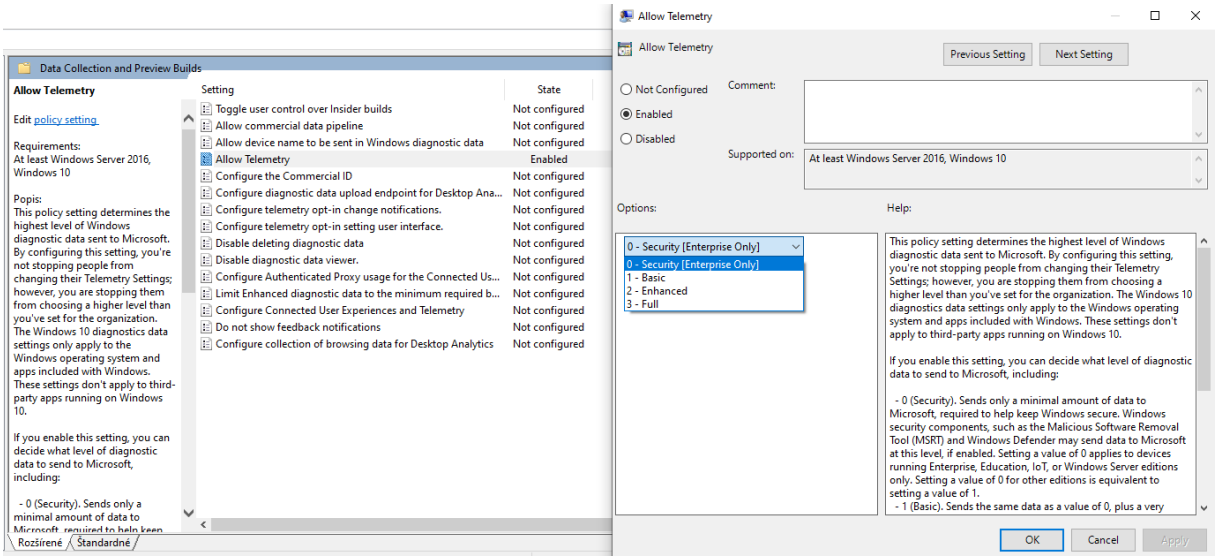
Konfigurácia Telemetrie

Cez nastavenia v systéme:

- Na otvorenie aplikácie Nastavenia použite klávesovú skratku Windows + tlačidlo i
- Prejdite na položku Ochrana osobných údajov > diagnostika a pripomienky
- Vyhľadajte časť Diagnostika - „Vyberte, koľko údajov odošlete spoločnosti Microsoft“
- Máte možnosť prepínať medzi: základné (úroveň 1) a úplné (úroveň 3)

Cez nastavenie Lokálnych alebo Skupinových politík (GPO/LGPO):

- Použite tlačidlo Windows + tlačidlo R a zadajte gpedit.msc. Potom stlačte Enter
- Použite štruktúru priečinkov vľavo a prejdite na Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds
- Dvakrát kliknite na „Allow Telemetry“.
- Nastavte politiku na možnosť Povolené (Enabled)
- Vyberte jednu z dostupných úrovní (Security-0, Basic-1, Enhanced-2, Full-3).
- Najnižšia úroveň, ktorú môžete nastaviť v edíciách systému Windows 10 Home a Pro, je Basic (úroveň 1)



Cez nastavenie Windows Registry

- Použite tlačidlo Windows + tlačidlo R a zadajte regedit.exe. Potom stlačte Enter
- Prejdite vľavo na nasledujúci kľúč:
  KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataCollection
- Kliknite pravým tlačidlom myši na DataCollection a vyberte New > Dword (32-bit) Value
- Pomenujte ho AllowTelemetry
- Dvakrát kliknite na AllowTelemetry a nastavte jej hodnotu podľa toho, ktorú chcete 0,1,2,3
- Opäť platí, že Security sa automaticky zmení na Basic v edíciách Windows 10 Home a Pro.
- Potom počítač reštartujte.

Akákoľvek zmena v nastaveniach telemetrie je vykonávaná na vlastné riziko užívateľa. Avšak ani zmena nastavenia na **úroveň 0 – Security** by nemala spôsobovať užívateľom komplikácie pri používaní systému Windows v rámci ich štandardného používania. V prípade akýchkoľvek problémov v stabilite systému po nastavení telemetrie, je kedykoľvek možné jej nastavenie vrátiť na pôvodnú úroveň.