Operační systémy Windows 2

Klíčové pojmy:

- Navigace v prostředí Windows
- Příkazový řádek CLI a PowerShell
- Jádro operačního systému
- Serverové aplikace
- Nástroje ochrany osobních údajů ve Windows
- Windows Hello
- Šifrování zařízení (BitLocker)
- Ochrana osobních údajů při online aktivitách
- Správa diagnostických dat

Navigace v prostředí Windows

Navigace v prostředí Windows je proces, kterým uživatelé interagují s grafickým uživatelským rozhraním (GUI) operačního systému Windows. Windows poskytuje přehledné uživatelské rozhraní, které usnadňuje používání aplikací, správu souborů a přístup k systémovým funkcím.

Klíčové prvky navigace:

1. Pracovní plocha (Desktop):
    - Pracovní plocha je hlavní obrazovkou, kde jsou umístěny ikony aplikací, složek a souborů. Je výchozím bodem pro interakci s operačním systémem.
2. Nabídka Start:
    - Nabídka Start je centrální místo pro přístup k aplikacím, souborům a systémovým nástrojům. Uživatelé mohou také vyhledávat aplikace a nastavení pomocí vyhledávacího pole v nabídce Start.
3. Průzkumník souborů:
    - Průzkumník souborů umožňuje procházet souborový systém Windows, vytvářet složky, přejmenovávat soubory a kopírovat nebo přesouvat data. Obsahuje také nástroje pro práci s externími disky a síťovými jednotkami.
4. Hlavní panel (Taskbar):
    - Hlavní panel obsahuje zástupce často používaných aplikací a spuštěných programů. Uživatelé mohou rychle přepínat mezi aplikacemi a monitorovat systémové upozornění, jako jsou síťová připojení nebo stav baterie.
5. Centrum akcí:
    - Centrum akcí slouží ke správě notifikací a rychlému přístupu k důležitým nastavením systému, jako jsou síť, obrazovka a aktualizace.

Příkazový řádek CLI a PowerShell

Příkazový řádek (CLI) a PowerShell jsou dvě rozhraní pro práci s příkazovými řádky v systému Windows. Poskytují možnost automatizovat úlohy, spravovat systémové prostředky a provádět pokročilé operace, které nejsou vždy dostupné prostřednictvím GUI.

Příkazový řádek CLI (Command Line Interface):

- **CLI** je tradiční textové rozhraní pro zadávání příkazů. Jeho hlavní funkcí je správa systému a spouštění programů pomocí jednoduchých příkazů. CLI se často používá pro rychlé administrativní úlohy, jako je kopírování souborů, vytváření adresářů nebo úprava síťových nastavení.
- **Použití**: Pomocí příkazů jako `dir`, `cd`, `copy` a `ipconfig` mohou uživatelé procházet adresářovou strukturu, kopírovat soubory nebo zobrazit konfiguraci sítě.

PowerShell:

- **PowerShell** je pokročilejší nástroj než tradiční příkazový řádek. Je navržen pro správu systémových prostředků a automatizaci složitých úloh. PowerShell využívá **cmdlety** (jednoduché příkazy) a podporuje skriptování, což umožňuje provádět složité operace s minimem příkazů.
- **Použití**: PowerShell umožňuje spravovat soubory, procesy, síťová připojení a mnoho dalších aspektů systému. Lze také používat PowerShell skripty k automatizaci opakovaných úkolů, jako je hromadné vytváření uživatelských účtů nebo konfigurace systému. Příkazy jako `Get-Process`, `Get-Help` nebo `Set-ExecutionPolicy` poskytují přímý přístup k systémovým funkcím.
- **Existují dvě prostředí**: PowerShell a PowerShellISE:

Funkce	PowerShell	PowerShell ISE
Typ prostředí	Příkazový řádek (CLI)	Grafické rozhraní (GUI)
Zvýraznění syntaxe	Ne	Ano
Ladění skriptů	Základní, přes výstupy	Pokročilé, s body přerušení
Automatické doplňování	Částečné	Plné automatické doplňování příkazů
Více skriptovacích oken	Ne	Ano
Multiplatformní podpora	Ano (v moderních verzích)	Ne (dostupné pouze na Windows)

Spuštění příkazového řádku CLI a PowerShell

- Spuštění příkazového řádku (CLI):
  - Z nabídky Start: Otevřete nabídku Start a napište „cmd“. Klikněte na Příkazový řádek.
  - Klávesová zkratka: Stiskněte Windows + R, napište cmd a stiskněte Enter.
- Spuštění PowerShell:
  - Z nabídky Start: Otevřete nabídku Start a napište „PowerShell“. Klikněte na Windows PowerShell.
  - Klávesová zkratka: Stiskněte Windows + X a vyberte Windows PowerShell (Terminál) nebo Windows PowerShell (Admin) (Terminál (správce)).

Jádro operačního systému

Jádro (kernel) je centrální součást operačního systému, která zajišťuje základní komunikaci mezi hardwarem a softwarem. V systému Windows se používá jádro zvané Windows NT kernel, které poskytuje stabilní a bezpečné prostředí pro běh aplikací a správu systémových prostředků.

Funkce jádra:

1. **Správa paměti**: Jádro řídí, jak je operační paměť přidělována jednotlivým aplikacím, a zajišťuje, aby různé procesy nezasahovaly do paměti jiných procesů.
2. **Správa procesů**: Jádro kontroluje, které procesy běží, a zajišťuje jejich přepínání (multitasking) a synchronizaci.
3. **Správa vstupů/výstupů**: Jádro zajišťuje komunikaci mezi aplikacemi a hardwarovými zařízeními, jako jsou pevné disky, síťové karty nebo vstupní zařízení (klávesnice, myš).
4. **Bezpečnost**: Jádro implementuje bezpečnostní model, který kontroluje přístupy uživatelů a procesů k systémovým zdrojům.

Serverové aplikace

Systémy Windows jsou široce používány také v prostředí serverů, kde zajišťují provoz klíčových firemních služeb a aplikací. Windows Server je speciální edice Windows navržená pro servery a podnikové prostředí.

Nejpoužívanější role Windows Serveru:

1. **Active Directory Domain Services (AD DS):**

   Active Directory je hierarchická adresářová služba, která spravuje uživatele, skupiny, počítače a další síťové objekty. AD DS je zodpovědná za autentizaci a autorizaci uživatelů v síti.

   Použití: Správa domény, uživatelských účtů, skupinových zásad a ověřování v rámci sítě.

   Pozn.:

Funkce	Autentizace	Autorizace
Účel	Ověřit identitu uživatele	Umožnit nebo omezit přístup k prostředkům
Proces	Zjistí, kdo uživatel je	Určuje, co uživatel může dělat
Příklad	Zadání uživatelského jména a hesla	Povolení přístupu ke specifickým souborům
Kdy probíhá	První krok v procesu přístupu	Probíhá až po úspěšné autentizaci
Výstup	Ověření identity	Přiřazení úrovně přístupu nebo oprávnění

2. **DHCP Server:**

   Dynamic Host Configuration Protocol (DHCP) server přiděluje IP adresy zařízením v síti automaticky, což usnadňuje správu sítě.

   Použití: Automatické přidělování IP adres, správa rozsahů a přidělení síťových parametrů.

3. **DNS Server:**

   Domain Name System (DNS) server zajišťuje překlad názvů domén na IP adresy, což umožňuje komunikaci na internetu i v lokálních sítích.

   Použití: Překlad názvů domén (např. www.example.com) na IP adresy (např. 192.168.1.1).

4. **File and Storage Services:**

   Tento server spravuje sdílení souborů a přístup k úložištím. Může poskytovat prostor pro ukládání souborů, správu oprávnění a replikaci dat.

   Použití: Centrální úložiště pro uživatele a aplikace, správa sdílených složek a přístupových práv.

5. **Hyper-V:**

   Hyper-V je virtualizační technologie integrovaná v systému Windows Server, která umožňuje spouštět virtuální stroje na fyzickém serveru.

   Použití: Nasazení a správa virtuálních strojů, vytvoření testovacích nebo produkčních prostředí bez potřeby dalšího hardwaru.

6. **Webový server (IIS):**

   Internet Information Services (IIS) je role webového serveru, která umožňuje hostování webových aplikací a stránek.

   Použití: Hostování webových stránek a aplikací na platformě Windows, podpora ASP.NET a dalších technologií.

7. **Remote Desktop Services (RDS):**

   RDS umožňuje uživatelům vzdálený přístup k aplikacím a plochám běžícím na serveru. Podporuje víceuživatelský přístup k aplikacím.

   Použití: Vzdálený přístup k aplikacím, pracovním stanicím a serverům pro zaměstnance.

Nástroje ochrany osobních údajů ve Windows

Ochrana osobních údajů je v dnešní době kritickým aspektem každého operačního systému, včetně `Windows`**.** Microsoft v průběhu let implementoval řadu nástrojů a funkcí do Windows 10 a Windows 11, které umožňují uživatelům kontrolovat, jak jsou jejich data shromažďována, ukládána a sdílena. Tyto nástroje se zaměřují na zajištění bezpečnosti dat, ochranu osobních údajů a minimalizaci sběru informací bez souhlasu uživatele.

Nastavení ochrany osobních údajů v systému Windows

Windows poskytuje **centrum nastavení ochrany osobních údajů**, kde mohou uživatelé konfigurovat širokou škálu možností souvisejících s ochranou dat a soukromí. Tato nastavení lze najít v aplikaci **Nastavení** pod záložkou **Soukromí a zabezpečení**.

Klíčové oblasti ochrany osobních údajů:

- **Obecná nastavení ochrany soukromí**: Tato sekce obsahuje přepínače, které umožňují uživatelům rozhodnout, zda mohou aplikace sledovat a využívat jejich reklamní ID, jestli mohou být shromažďovány informace o aktivitě uživatele a zda může Windows zobrazovat přizpůsobené návrhy.

- **Oprávnění aplikací**: Uživatelé mohou spravovat, jaké aplikace mají přístup k citlivým údajům, jako je kamera, mikrofon, poloha, kontakty, soubory nebo jiné osobní informace. Každou aplikaci lze individuálně povolit nebo zakázat pro přístup k těmto zdrojům.
- **Poloha**: Ovládá, které aplikace mohou přistupovat k údajům o poloze zařízení. Uživatelé mohou také vypnout sledování polohy a vymazat historii polohy.
- **Kamera a mikrofon**: Uživatelé mají možnost spravovat, které aplikace mají přístup ke kameře a mikrofonu. Je možné povolit nebo zakázat přístup pro jednotlivé aplikace.
- **Historie aktivit**: Windows 10 a Windows 11 shromažďují historii aktivit, což umožňuje přístup k nedávno používaným souborům, aplikacím nebo webovým stránkám. Uživatelé mohou tuto funkci deaktivovat nebo odstranit historii aktivit uloženou v cloudu.

Windows Hello

Windows Hello je biometrický autentizační systém, který umožňuje přihlašování pomocí **rozpoznání obličeje**, **otisku prstu** nebo **PIN kódu**. Tento systém poskytuje bezpečnější a pohodlnější přístup k zařízení, protože minimalizuje riziko krádeže hesel.

- **Ochrana osobních údajů**: Windows Hello ukládá biometrické údaje přímo v zařízení, nikoliv na cloudových serverech. To zajišťuje, že citlivé osobní údaje zůstanou bezpečně v počítači a nebudou vystaveny riziku narušení bezpečnosti v síťovém prostředí.

Přihlašování pomocí rozpoznání obličeje

Rozpoznávání obličeje je metoda, která využívá **biometrické údaje** ke zjištění identity uživatele. Využívá se pokročilých senzorů, jako jsou **infračervené kamery** a **systémy pro hloubkovou analýzu**, aby vytvořily detailní mapu obličeje uživatele.

Jak to funguje:

Registrace obličeje: Při nastavování rozpoznání obličeje si systém vezme detailní snímek obličeje uživatele pomocí infračervené kamery. Vytvoří **biometrický profil**, který zachytí důležité rysy, jako jsou vzdálenosti mezi očima, nosem a ústy, a ukládá je jako šifrovanou reprezentaci obličeje.

Ověřování identity: Když se uživatel pokusí přihlásit, infračervená kamera snímá obličej a porovná jej s uloženým biometrickým profilem. Pokud se rysy obličeje shodují, uživatel je přihlášen.

Bezpečnostní mechanismy:

- **Infračervené světlo**: Tato technologie umožňuje přihlašování za různých světelných podmínek, včetně tmy, a poskytuje ochranu proti pokusům o přihlášení pomocí fotografie.
- **3D rozpoznávání**: Systémy, které podporují rozpoznávání hloubky, používají **3D mapu obličeje**, což zvyšuje bezpečnost proti falšování (například pokusy o oklamání systému pomocí 2D fotografie).

Zabezpečení dat: Biometrický profil není nikdy ukládán jako fotografie, ale jako **matematická reprezentace** obličeje, která je **zašifrovaná** a uložena pouze v lokálním zařízení. Tyto údaje nejsou odesílány ani uloženy v cloudu.

Přihlašování pomocí otisku prstu

Otisk prstu je jedním z nejběžnějších biometrických autentizačních mechanismů. Základní myšlenkou je, že **otisk prstu** je jedinečný pro každého člověka, což umožňuje bezpečnou a rychlou identifikaci.

Jak to funguje:

Registrace otisku prstu: Při nastavení otisku prstu uživatel položí prst na snímač (čtečku). Tento snímač skenuje otisk prstu a vytvoří biometrický profil na základě charakteristik, jako jsou minutiae (konkrétní detaily v otisku prstu, jako je umístění hřebínků a údolíček).

Ověřování identity: Když uživatel znovu položí prst na čtečku, snímač zachytí aktuální obraz otisku a porovná jej s uloženým biometrickým profilem. Pokud se otisk shoduje, uživatel je přihlášen.

Zabezpečení dat: Stejně jako u rozpoznání obličeje, údaje o otisku prstu jsou ukládány v podobě matematického modelu a jsou zašifrovány. Nejsou uchovávány v podobě obrazu otisku prstu a nejsou odesílány na vzdálené servery.

Kapacitní snímače: Moderní čtečky otisků prstů využívají kapacitní snímače, které měří elektrické vlastnosti kůže, aby zlepšily přesnost skenování a odolnost proti podvodům (například pomocí umělých otisků prstů).

Přihlašování pomocí PIN kódu

PIN (Personal Identification Number) je číselný kód, který je přidělen nebo nastaven uživatelem pro přístup do zařízení. Přihlašování pomocí **PIN kódu** je považováno za bezpečnější alternativu k heslům.

Jak to funguje:

Registrace PIN kódu: Uživatel nastaví PIN kód, což je obvykle čtyřmístné nebo vícečíslicové číslo, které je použito pro přístup k jeho zařízení. PIN je spojen výhradně s konkrétním zařízením.

Ověřování identity: Když se uživatel pokusí přihlásit, zadá PIN, který systém porovná s uloženou hodnotou. Pokud se hodnoty shodují, uživatel získá přístup.

Bezpečnostní vlastnosti PIN kódu:

Lokální úložiště: PIN není uložen v cloudu ani přenášen po síti. Je uchováván pouze na daném zařízení a je chráněn šifrováním.

Specifické zařízení: Na rozdíl od hesla, které může být použito na více zařízeních a online účtech, PIN kód je platný pouze pro konkrétní zařízení. Pokud by někdo získal přístup k PINu, bez fyzického zařízení by byl tento kód k ničemu.

Možnost nastavení delších PINů: Uživatelé mohou zvolit delší a složitější PINy (např. šestimístné, osmimístné) pro vyšší úroveň zabezpečení.

Další ochrany: PIN kód může být chráněn dalšími bezpečnostními mechanismy, jako jsou limity pokusů o zadání. Při opakovaném zadání nesprávného PINu může být zařízení zablokováno.

Šifrování zařízení (BitLocker)

BitLocker je nástroj pro **šifrování disků**, který zajišťuje, že data uložená na zařízení jsou chráněna před neoprávněným přístupem. Pokud je BitLocker aktivován, všechna data na disku jsou šifrována, což znamená, že i v případě krádeže zařízení nebude útočník schopen data přečíst bez správného dešifrovacího klíče.

- **BitLocker To Go**: Poskytuje možnost šifrování dat na **externích úložných zařízeních** (např. USB disky), čímž chrání přenosná data před ztrátou nebo krádeží.
- **Ochrana před offline útoky**: BitLocker chrání data i v případě, že je disk vyjmut a vložen do jiného zařízení.
- Šifrování jednotky pomocí služby BitLocker není k dispozici na zařízeních s operačním systémem Windows 11 Home a Windows 10 Home.

Ochrana osobních údajů při online aktivitách

Microsoft Edge, výchozí webový prohlížeč Windows, obsahuje několik nástrojů na ochranu osobních údajů při prohlížení internetu.

- **Blokování sledovacích prvků**: Microsoft Edge obsahuje **funkce pro blokování sledování** (tracking prevention), které zabraňují webovým stránkám a inzerentům sledovat aktivitu uživatele na internetu a shromažďovat osobní údaje. Uživatelé si mohou vybrat úroveň ochrany (základní, vyvážená nebo přísná).
- **Režim InPrivate**: Tento režim zabraňuje ukládání historie prohlížení, souborů cookie a dat formulářů. Je vhodný pro zajištění většího soukromí při prohlížení internetu.

Windows Defender SmartScreen

Windows Defender SmartScreen chrání uživatele před potenciálně nebezpečnými webovými stránkami, aplikacemi a soubory, které mohou obsahovat malware nebo jiné bezpečnostní hrozby. Tento nástroj kontroluje stahované soubory a navštěvované weby v reálném čase, aby minimalizoval riziko nakažení malwarem.

- **Ochrana před phishingem**: SmartScreen upozorní uživatele, pokud navštíví podezřelou webovou stránku nebo kliknou na potenciálně nebezpečný odkaz, který by mohl být součástí phishingového útoku.
- **Kontrola aplikací a stahování**: Při stahování aplikací z internetu kontroluje SmartScreen jejich důvěryhodnost a blokuje potenciálně nebezpečné nebo neznámé programy.

Režim Ochrany proti sledování **(Tracking Prevention)**

Režim ochrany proti sledování, který je k dispozici v prohlížeči Microsoft Edge, blokuje webové stránky a třetí strany před sledováním aktivity uživatelů na internetu. Tato funkce přispívá k ochraně osobních údajů tím, že omezuje sledovací technologie, jako jsou soubory cookie a skripty používané pro cílenou reklamu.

Kontrola soukromí v cloudu a službách Microsoftu

Windows je úzce propojen se službami Microsoftu, jako je **OneDrive**, **Cortana** a **Microsoft Account**. Uživatelé mají přístup k nástrojům, které jim umožňují spravovat data sdílená s těmito službami.

- **Cortana a ochrana soukromí**: **Cortana**, hlasová asistentka ve Windows, může shromažďovat osobní údaje, jako jsou vyhledávací dotazy a údaje o poloze. Uživatelé mohou omezit, co Cortana sleduje a zpracovává, nebo ji úplně deaktivovat.

- **OneDrive**: Data uložená v **OneDrive** jsou šifrována během přenosu i v klidovém stavu. Uživatelé mají možnost spravovat, kdo má přístup k jejich souborům, a nastavit sdílení souborů pouze s důvěryhodnými osobami.

Windows Defender Antivirus

Windows Defender Antivirus je integrované řešení pro ochranu před malwarem, které je součástí Windows. Zajišťuje ochranu před viry, spywarem, ransomwarem a dalšími hrozbami v reálném čase.

- **Ochrana soukromí**: Windows Defender monitoruje zařízení a blokuje potenciálně nebezpečné aplikace nebo webové stránky, aniž by odesílal osobní údaje uživatele na externí servery. Uživatelé mají možnost rozhodnout, jaká data o bezpečnostních událostech budou sdílena s Microsoftem.

Ochrana soukromí dětí a rodin

Windows nabízí nástroje pro rodičovskou kontrolu, které umožňují rodičům sledovat a omezovat aktivity svých dětí na počítači.

- **Microsoft Family Safety**: Tento nástroj poskytuje rodičům přehled o tom, jak jejich děti používají zařízení, kolik času tráví u obrazovky a jaké aplikace používají. Rodiče mohou nastavit časové limity, blokovat nevhodné aplikace nebo webové stránky a získat zprávy o aktivitách dětí.

Správa diagnostických dat

Windows shromažďuje diagnostická data, která pomáhají Microsoftu identifikovat problémy se systémem a zlepšovat jeho fungování. Uživatelé mají možnost spravovat, jaká diagnostická data jsou odesílána Microsoftu:

- **Základní diagnostika**: Omezuje množství odesílaných dat na minimum (zahrnuje informace potřebné k identifikaci základních problémů).
- **Úplná diagnostika**: Obsahuje podrobnější data o fungování systému a aplikací. Uživatelé mohou vypnout některé z těchto funkcí, pokud chtějí minimalizovat sdílení osobních údajů.

Odkazy:

Microsoft.com

Wikipedia

Cisco Linux Essentials

Root.cz

Chatgpt