Operační systémy Windows 6.2

Funkce zabezpečení ve Windows – přehled

Systém Windows obsahuje řadu integrovaných funkcí, které chrání počítač před viry, malwarem a dalšími hrozbami. O některých z nejdůležitějších funkcí se můžete dozvědět více níže.

6.2.1 Windows defender antivirus

Popis:

- **Windows Defender Antivirus** je vestavěné antivirové řešení ve Windows 10 a Windows 11, které poskytuje ochranu v reálném čase proti virům, malwaru a dalším škodlivým softwarům.
- Automaticky skenuje soubory a aplikace při jejich spuštění nebo přístupu k nim.

Klíčové Funkce:

- Ochrana v reálném čase: Neustálé monitorování systému pro detekci hrozeb.
- Cloudová ochrana: Využívá cloudové služby pro rychlejší detekci nových hrozeb.
- Automatické aktualizace: Pravidelně aktualizuje definice virů a malwaru.

Možnosti Nastavení:

- Uživatelé mohou naplánovat pravidelné skenování, vyloučit určité soubory nebo složky a konfigurovat úroveň ochrany.

6.2.2 Windows Firewall

Popis:

- **Windows Firewall** je integrovaný firewall, který pomáhá zabránit neoprávněnému přístupu k systému přes síť nebo internet.

Klíčové Funkce:

- Filtrace příchozího a odchozího provozu: Kontroluje data vstupující a opouštějící systém na základě předdefinovaných pravidel.
- Profily síťových umístění: Umožňuje nastavit různé úrovně zabezpečení pro soukromé, veřejné a doménové sítě.
- Pokročilá konfigurace: Umožňuje vytvářet vlastní pravidla pro konkrétní aplikace a porty.

Možnosti Nastavení:

- Přístupné přes Windows Security nebo Windows Defender Firewall s pokročilým zabezpečením pro detailní konfiguraci.

6.2.3 User Account Control (UAC)

Popis:

- **User Account Control** je bezpečnostní funkce, která pomáhá zabránit neautorizovaným změnám systému tím, že vyžaduje potvrzení nebo administrátorská oprávnění pro určité akce.

Klíčové Funkce:

- Prevence nežádoucích změn: Upozorňuje uživatele, když aplikace nebo procesy chtějí provést změny vyžadující vyšší oprávnění.
- Ochrana proti malware: Snižuje riziko, že malware získá administrátorská práva bez vědomí uživatele.

Možnosti Nastavení:

- Uživatelé mohou upravit úroveň UAC v Nastavení > Účty > Možnosti přihlášení nebo přes Ovládací panely.

6.2.4 BitLocker Drive Encryption

Popis:

- **BitLocker** je funkce pro šifrování celých disků, která chrání data před neoprávněným přístupem v případě ztráty nebo krádeže zařízení.

Klíčové Funkce:

- Šifrování disků: Umožňuje šifrovat systémové i datové disky.
- TPM integrace: Využívá Trusted Platform Module (TPM) pro bezpečné ukládání šifrovacích klíčů.
- BitLocker to go: Šifrování externích disků a USB flash disků.

Možnosti Nastavení:

- Přístupné přes Ovládací panely > Šifrování jednotky BitLocker.
- Umožňuje zálohovat obnovovací klíče a nastavit metody ověřování (PIN, heslo).

6.2.5 Windows Hello

Popis:

- **Windows Hello** nabízí biometrické přihlášení pomocí otisku prstu, rozpoznání obličeje nebo oční duhovky, poskytující rychlý a bezpečný přístup k zařízení.

Klíčové Funkce:

- Biometrická autentizace: Nahrazuje tradiční hesla bezpečnějšími metodami.
- Komfort a rychlost: Umožňuje rychlé přihlášení bez potřeby pamatovat si hesla.

Možnosti Nastavení:

- Nastavení v Nastavení > Účty > Možnosti přihlášení.
- Vyžaduje kompatibilní hardware (např. kamera s podporou IR pro rozpoznání obličeje).

6.2.6 Secure Boot

Popis:

- **Secure Boot** je bezpečnostní standard UEFI, který pomáhá zajistit, že počítač spustí pouze důvěryhodný software při startu systému.

Klíčové Funkce:

- Ochrana před malware při startu: Zabraňuje načtení škodlivého kódu při bootování.
- Digitální podepisování: Vyžaduje, aby firmware a ovladače byly digitálně podepsány.

Možnosti Nastavení:

- Konfigurace přes BIOS/UEFI nastavení systému.

6.2.7 Windows Defender Application Guard

Popis:

- **Application Guard** izoluje nedůvěryhodné webové stránky a aplikace v bezpečném kontejneru, aby zabránil ohrožení systému.

Klíčové Funkce:

- Izolace: spouští Edge nebo aplikace v izolovaném prostředí pomocí virtualizace.
- Ochrana před útoky: Zabraňuje škodlivému kódu z izolovaného prostředí ovlivnit hostitelský systém.

Možnosti Nastavení:

- Dostupné v edicích Windows 10/11 Pro a Enterprise.
- Lze povolit přes Windows Features nebo pomocí Group Policy.

6.2.8 Windows Defender Credential Guard

Popis:

- **Credential Guard** chrání odcizení přihlašovacích údajů tím, že ukládá pověřovací informace ve virtualizovaném prostředí.

Klíčové Funkce:

- Ochrana pověřovacích údajů: Izoluje LSA (Local Security Authority) procesy, aby zabránil útokům jako Pass-the-Hash.
- Virtualizace: využívá Hyper-V pro vytvoření bezpečného prostředí.

Možnosti Nastavení:

- Vyžaduje Windows 10/11 Enterprise a podporu virtualizace v hardware.
- Konfigurace přes Group Policy nebo Registry Editor.

6.2.9 Windows Defender Exploit Guard

Popis:

- **Exploit Guard** poskytuje sadu funkcí pro prevenci exploitů, omezení přístupu a kontrolu chování aplikací.

Klíčové Funkce:

- Attack surface reduction: Omezování oblastí, kde mohou být systémy napadeny.
- Network protection: Blokuje nebezpečné odchozí připojení.
- Controlled folder access: Chrání soubory a složky před neoprávněnými změnami.

Možnosti Nastavení:

- Konfigurace přes Windows Security > Virus & threat protection > Manage settings.
- Pokročilá nastavení pomocí Group Policy nebo System Center Configuration Manager.

6.2.10 Windows Defender SmartScreen

Popis:

- **SmartScreen** filtruje škodlivé webové stránky a stahované soubory, aby chránil uživatele před phishingem a malwarem.

Klíčové Funkce:

- Webová ochrana: Varuje před nebezpečnými weby v prohlížeči Microsoft Edge.
- Ochrana při stahování: Blokuje potenciálně škodlivé soubory.

Možnosti Nastavení:

- Nastavení v Windows Security > App & browser control.
- Uživatelé mohou povolit, zakázat nebo upravit úroveň varování.

6.2.11 Windows Update

Popis:

- **Windows Update** zajišťuje, že systém je aktuální s nejnovějšími aktualizacemi zabezpečení a opravami.

Klíčové Funkce:

- Automatické aktualizace: Pravidelné stahování a instalace aktualizací.

- Možnosti odložení: Umožňuje podnikům kontrolovat nasazení aktualizací.

Možnosti Nastavení:

- Nastavení v Nastavení > Aktualizace a zabezpečení > Windows Update.
- Pokročilá správa pomocí Windows Server Update Services (WSUS) nebo Microsoft Endpoint Configuration Manager.

6.2.12 Windows Sandbox

Popis:

- **Windows Sandbox** je lehké desktopové prostředí, kde lze bezpečně spouštět nedůvěryhodné aplikace bez ovlivnění hostitelského systému.

Klíčové Funkce:

- Izolované prostředí: Každé spuštění je čistá instalace Windows.
- Automatické odstranění: Po zavření Sandboxu se veškerý obsah trvale odstraní.

Možnosti Nastavení:

- Dostupné v edicích Windows 10/11 Pro a Enterprise.
- Lze povolit přes Windows Features.

6.2.13 Skupinové Politiky a Active Directory

Popis:

- **Skupinové politiky** umožňují správcům centrálně spravovat a konfigurovat nastavení systému a zabezpečení na úrovni uživatelů a počítačů v síti.

Klíčové Funkce:

- Centrální správa: Aplikace politik na organizační jednotky (OUs) v Active Directory.
- Bezpečnostní nastavení: Konfigurace hesel, přístupových práv, nastavení firewallu atd.

Možnosti Nastavení:

- Správa přes Group Policy Management Console (GPMC).
- Umožňuje detailní kontrolu nad téměř všemi aspekty systému.

6.2.14 Windows Information Protection

Popis:

- **Windows Information Protection (WIP)** chrání firemní data před neúmyslným únikem na osobní zařízení nebo aplikace.

Klíčové Funkce:

- Oddělení dat: Odděluje firemní a osobní data na stejném zařízení.
- Kontrola přístupu: Definuje, které aplikace mohou přistupovat k firemním datům.
- Šifrování: Automaticky šifruje firemní data.

Možnosti Nastavení:

- Konfigurace pomocí Intune, System Center Configuration Manager nebo Group Policy.

6.2.15 Microsoft Defender for Endpoint

Popis:

- **Microsoft Defender for Endpoint** je podnikové řešení pro ochranu koncových bodů, které poskytuje pokročilou ochranu před hrozbami, detekci a reakci.

Klíčové Funkce:

- Endpoint Detection and Response (EDR): Detekuje a reaguje na pokročilé hrozby.
- Threat & Vulnerability Management: Identifikuje a opravuje zranitelnosti.
- Automatizovaná Reakce: Automatizuje reakce na bezpečnostní incidenty.

Možnosti Nastavení:

- Spravováno přes Microsoft 365 Defender portál.
- Vyžaduje předplatné Microsoft 365 E5 nebo samostatné licence.

6.2.16 Device Guard

Popis:

- **Device Guard** je sada funkcí, které pomáhají chránit zařízení před spuštěním nedůvěryhodného kódu.

Klíčové Funkce:

- Code Integrity Policies: Umožňuje pouze spuštění důvěryhodného kódu.
- Virtualization-Based Security: Využívá virtualizaci pro ochranu kritických procesů.

Možnosti Nastavení:

- Konfigurace přes Group Policy a PowerShell.
- Vyžaduje kompatibilní hardware a Windows 10/11 Enterprise.

6.2.17 Další Bezpečnostní Funkce

- **AppLocker**: Umožňuje kontrolovat, které aplikace a soubory mohou být spuštěny.
- **Controlled Folder Access**: Chrání důležité složky před neoprávněnými změnami, zejména před ransomwarem.

- **Windows Defender Firewall s pokročilým zabezpečením**: Poskytuje detailní nastavení pravidel firewallu a IPSec.
- **Encrypting File System (EFS)**: Umožňuje šifrovat jednotlivé soubory a složky.
- **Credential Manager**: Bezpečně ukládá přihlašovací údaje a hesla.
- **Dynamic Lock**: Automaticky uzamkne počítač, když se uživatel vzdálí (např. pomocí Bluetooth spárovaného zařízení).

Odkazy:

https://edu.gcfglobal.org/en/windows10/security-and-maintenance/1/

https://support.microsoft.com/en-us/windows/manage-updates-in-windows-643e9ea7-3cf6-7da6-a25c-95d4f7f099fe#WindowsVersion=Windows_10

https://www.computerworld.cz/clanky/jak-chytre-spravovat-aktualizace-windows-10/

https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/select-types-of-rules-to-create

https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/configure?tabs=intune

chatgpt.com