Profil koncovej používateľskej stanice Platforma OS Windows

Obsah

1.	Účel d	okumentu	3
2.	Základ	lná úroveň bezpečnosti koncovej stanice	3
3.	Zabez	pečenie základnej úrovne bezpečnosti koncovej stanice	3
	3.1. V	oľba vhodného Operačného systému Windows	4
	3.1.1.	OS Windows 2000	4
	3.1.2.	OS Windows XP	4
	3.1.3.	OS Windows Vista	4
	3.1.4.	OS Windows 7	4
	3.1.5.	OS Windows 8 a 8.1	4
	3.1.6.	Zhrnutie	5
	3.2. В	ezpečná Inštalácia OS Windows	5
	3.2.1.	Postup	5
	3.3. V	oľba silných hesiel	5
	3.3.1.	Nevhodná voľba hesla	5
	3.3.2.	Bezpečnosť hesla	5
	3.3.2.1.	Dĺžka hesla	6
	3.3.2.2.	Použité znaky	6
	3.3.2.3.	Pravidelné menenie hesla	6
	3.3.2.4.	Zložitosť hesla a priestor kľúčov	6
	3.3.2.5.	Generovanie zapamätateľných hesiel	6
	3.3.3.	Obrázkové heslá	6
	3.3.4.	Bezpečné heslo – zhrnutie	7
	3.4. V	ytvorenie a používanie používateľských účtov	7
	3.4.1.	Vytvorenie používateľského účtu	7
	3.4.1.1.	Windows XP	8
	3.4.1.2.	Windows 71	2
	3.5. Ir	nštalácia, konfigurácia a používanie bezpečnostných nástrojov	5
	3.5.1.	Anti-malware riešenie 1	5
	3.5.2.	Firewall	4

Profil koncovej používateľskej stanice – Platforma OS Windows

3.5.2.1	. Odporúčané nastavenia25
3.5.2.2	. Windows Firewall – OS Windows XP 25
3.5.2.3	. Windows Firewall – OS Windows 7
3.5.3.	Komplexné riešenie
3.6.	Pravidelná aktualizácia použitého softvéru
3.6.1.	Operačný systém
3.6.2.	Prehliadač dokumentov pdf
3.6.3.	Java
3.6.4.	Webový prehliadač
3.6.4.1	Mozilla Firefox
3.7.	Inštalácia a konfigurácia nástrojov na rodičovskú kontrolu
3.7.1.	Popis
3.7.2.	Nastavenia funkcie Rodičovská kontrola 42
3.7.3.	Nastavenie konkrétne časové obmedzenie používania PC 44
3.7.4.	Obmedzenie spúšťania programov 44
3.7.5.	Obmedzenie spúšťania hier 46
3.7.6.	Ovládacie prvky
3.7.7.	Webový filter
3.7.7.1	. Kurupira Web Filter
3.7.7.2	Súbor hosts
4. Bezj	pečné používanie PC
5. Zhrr	nutie
5.1.	Používateľské účty
5.2.	Inštalácia programov
5.3.	Tvorba a uchovávanie hesiel
5.4.	Použitie anti-malwarového riešenia
5.5.	Použitie brány firewallu
5.6.	Aktualizácie systému a aplikácií 59
5.7.	Používanie počítača
5.8.	Používanie Internetu

1. Účel dokumentu

Tento dokument vznikol za účelom špecifikácie základných bezpečnostných opatrení pre koncovú stanicu s nainštalovaným systémom na platforme Windows v domácom prostredí. Dokument definuje základnú úroveň bezpečnosti počítača a opatrenia, ktoré je potrebné aplikovať na dosiahnutie tejto úrovne.

Súčasne dokument definuje spôsob ochrany detí prostredníctvom rodičovskej kontroly.

2. Základná úroveň bezpečnosti koncovej stanice

Najskôr si zadefinujeme základnú úroveň bezpečnosti počítača na platforme Windows, ktorú sa budeme snažiť v ďalších častiach dokumentu dosiahnuť pomocou konfiguračných nastavení a odporúčaných postupov ako pracovať s počítačom. Základná úroveň bezpečnosti počítača na platforme Windows musí spĺňať nasledovné body:

- Počítač je chránený pred štandardnými formami škodlivého kódu.
- Počítač umožňuje komunikáciu iba na povolené služby.
- Počítač má aktuálny, výrobcom podporovaný softvér a to najmä:
 - o Operačný systém
 - o Kancelárske balíky
 - Frameworky Java a .NET
 - o Prehliadače PDF
 - Audio a video prehrávače
- V počítači sa nachádza iba legálny softvér a obsah z dôveryhodných zdrojov.
- Používateľ na počítači vykonáva činnosť pod neprivilegovaným účtom.
- Používateľ na počítači pozorne pristupuje k elektronickej pošte, webovým stránkam a obsahu získanému z prostredia Internetu.

V kontexte ochrany maloletého používateľa (dieťaťa) musí ešte základná úroveň bezpečnosti na počítači na platforme Windows spĺňať nasledovný bod:

- Počítač je kontrolovaný administrátorom (rodičom) z hľadiska:
 - Prístupu dieťaťa k počítaču(prihlásenia sa).
 - Prístupu dieťaťa iba k vhodnému obsahu na Internete.
 - Prístupu dieťaťa k vhodným aplikáciám a službám.
 - Kontrola činnosti dieťaťa na počítači.

3. Zabezpečenie základnej úrovne bezpečnosti počítača

Na zabezpečenie základnej úrovne bezpečnosti počítača na platforme Windows, ktorú sme spomenuli vyššie, je potrebné zaistiť nasledovné skutočnosti:

- 1. Voľba vhodného operačného systému Windows
- 2. Bezpečná inštalácia OS Windows
- 3. Voľba silných hesiel
- 4. Vytvorenie a používanie neprivilegovaných účtov
- 5. Inštalácia, konfigurácia a používanie bezpečnostných nástrojov:
 - a. Firewall
 - b. Antimalware riešenie

6. Pravidelná aktualizácia softvéru

V prípade ak počítač používa aj dieťa je potrebné zabezpečiť:

7. Inštalácia a konfigurácia nástrojov na rodičovskú kontrolu

3.1. Voľba vhodného Operačného systému Windows

Táto časť je venovaná voľbe vhodnej verzie OS Windows vzhľadom na jeho aktuálnosť a dĺžku trvania jeho podpory zo strany jeho výrobcu – spoločnosti Microsoft.

Nepodporované operačné systémy obsahujú neopravené bezpečnostné problémy, ktoré sú zneužívané škodlivým kódom a útočníkmi pri kompromitácií a zneužití počítača.

3.1.1. OS Windows 2000

Nástupca OS Windows NT 4.0. Bol orientovaný hlavne na nasadenie v organizáciách. Podpora OS Windows 2000 bola oficiálne ukončená už 13.7.2010.

3.1.2. OS Windows XP

Nástupca Windows 2000 pre sieť bežných pracovných staníc (desktop). Spoločnosť Microsoft dňa 8.4.2014 oficiálne končí podporu pre operačný systém Windows XP. Po tomto dátume už nebude možné získať potrebné aktualizácie pre Windows XP, ani rozšírenú podporu, nakoľko plná technická podpora pre Windows XP skončila už v roku 2009. Ďalej sa predpokladá nárast dopytu po exploitoch (škodlivý kód využívajúci zraniteľnosť) pre tento operačný systém. Tieto exploity budú využívať novoobjavené, prípadne aj staršie, ešte neopravené, bezpečnostné zraniteľnosti Windows XP, operačného systému spoločnosti Microsoft, ktoré už ale nebudú patrične ošetrené. Inými slovami, používatelia budú vystavení riziku zneužívania bezpečnostných chýb vo Windows XP.

Spoločnosť Microsoft v tejto súvislosti odporúča prechod na nástupcov operačného systému Windows XP. Konkrétne ide o OS Windows Vista, Windows 7 a Windows 8, resp. OS Windows 8.1.

3.1.3. OS Windows Vista

Nástupca Windows XP. Má mnoho nových funkcií a tiež zmenené grafické rozhranie nazvané Aero, s množstvom bezpečnostných vylepšení a prepracované protokoly počítačových sietí. Oficiálne zverejnená platnosť predĺženej podpory zo strany spoločnosti Microsoft pre OS Windows Vista je 11.4.2017, začiatočný dátum životného cyklu je 25.1.2007.

3.1.4. **OS Windows 7**

Nástupca Windows Vista. Je modernejší a jeho cieľom je zosúladenie s existujúcimi ovládačmi zariadení, aplikácií a hardvéru. Oficiálne zverejnená platnosť predĺženej podpory zo strany spoločnosti Microsoft pre OS Windows 7 je 15.1.2020, začiatočný dátum životného cyklu je 22.10.2009.

3.1.5. **OS Windows 8 a 8.1**

Nástupca Windows 7. Oba sú založené na používateľskom rozhraní Modern User Interface (Metro). Oficiálne zverejnená platnosť predĺženej podpory zo strany spoločnosti Microsoft pre OS Windows 8 je 10.1.2023, začiatočný dátum životného cyklu je 31.10.2012 pre OS Windows 8 a 13.11.2013 pre OS Windows 8.1.

3.1.6. Zhrnutie

Vzhľadom na vyššie uvedené odporúčame používať **iba aktuálne podporované verzie OS**, teda **Windows Vista**, **Windows 7** a **8**, resp. **8.1**. Pokiaľ je to možné, tak odporúčame používať 64 bitovú architektúru vzhľadom na vyššiu úroveň bezpečnosti v rámci jadra OS.

3.2. Bezpečná Inštalácia OS Windows

Z pohľadu všeobecnej bezpečnosti **neodporúčame** inštalovať ľubovoľnú verziu OS Windows inak ako originál spoločnosti Microsoft a jej zmluvných partnerov. <u>Pri použití inštalačného média</u> <u>z neznámeho zdroja je nutné predpokladať jeho kompromitáciu</u>. Teda samotná inštalácia už môže v sebe obsahovať vírus.

Poznámka

Toto opatrenie je potrebné iba pre počítače, ktoré nie sú dodávané s predinštalovaným operačným systémom. Pri predinštalovanom operačnom systéme je namiesto tohto kroku krátka konfigurácia pri prvom spustení počítača.

3.2.1. Postup

Riaďte sa pokynmi sprievodcu. Odporúčame vždy vykonať tzv. čistú inštaláciu, tj. inštalácia s vymazaním a opätovným vytvorením systémovej partície a jej následným sformátovaním do formátu NTFS. Počas inštalácie bude potrebné zadanie používateľského mena a hesla. Odporúčame však zadať používateľské meno bez diakritiky. Dôvodom sú aplikácie, ktoré nedokážu korektne pracovať s používateľským menom, ktoré obsahuje diakritiku. **Používateľské heslo musí byť bezpečné**. Podrobný spôsob tvorby bezpečného hesla je uvedený v ďalšej časti.

Po inštalácií a prvotnom spustení sa OS Windows nakonfiguruje. Pokiaľ nebol správne rozpoznaný nejaký komponent inštalovaný v PC, je nutné následne doinštalovať jeho ovládače pomocou k nemu priloženého média, prípadne stiahnutím aktuálnej verzie zo stránky výrobcu daného komponentu.

3.3. Voľba silných hesiel

Základným bezpečnostným prvkom je kvalitné heslo. Voľba dostatočne bezpečného a kvalitného hesla je veľmi dôležitá, preto tejto problematike budeme venovať nasledujúce riadky. V moderných mobilných zariadeniach je možné použiť za účelom prihlásenia sa aj biometrické údaje vo forme odtlačkov prstov.

3.3.1. Nevhodná voľba hesla

Medzi nevhodne zvolené heslá môžeme zaradiť každé heslo, ktoré je odvoditeľné z dostupných informácií o osobe, ktorá dané heslo používa. Za nevhodne zvolené heslo môžeme považovať napr. vlastné meno, meno člena rodiny, dátum narodenia, telefónne číslo, atď.

Rovnako je ako heslo nevhodné použiť slovníkové slovo. Napr.: administrátor, Bratislava a podobne.

Na Internete je možné vyhľadať si aj zoznam najpoužívanejších hesiel. Ak je novozvolené heslo na tomto zozname, tak ho nemožno považovať za bezpečné.

3.3.2. Bezpečnosť hesla

Aby bolo možné považovať heslo za bezpečné, tak musí spĺňať parametre ako sú dostatočná dĺžka, dostatočná veľkosť použitej znakovej sady a dostatočná zložitosť. Všetky tieto parametre sú vysvetlené ďalej v texte.

3.3.2.1. Dĺžka hesla

Minimálna dĺžka hesla by mala byť aspoň 9 znakov. Čím dlhšie heslo, tým ťažšie sa pamätá a teda by malo byť aj bezpečnejšie. Bohužiaľ ale samotná dĺžka hesla ešte nezaručuje jeho bezpečnosť, napr. 16 znakové heslo v tvare AAA....AAA nie je bezpečné.

3.3.2.2. Použité znaky

Použité znaky, ktoré môže obsahovať samotné heslo, tvoria znakové sady, ako napr. číslice, anglická znaková sada alebo slovenská znaková sada. Inými slovami hovoríme o abecedách. Špeciálnou sadou, resp. skupinou, sú špeciálne znaky ,?.:"§!/()=;+/*-&*<>\|_`'@#\$%^.

3.3.2.3. Pravidelné menenie hesla

S bezpečnosťou hesla je spojená aj jeho pravidelná zmena. V prípade prihlasovacích hesiel k používateľskému účtu je vhodné takéto heslá obmieňať aspoň raz za 12 mesiacov, pričom je dôležité, aby sa novovytvorené heslo nepoužívalo už v minulosti. Inými slovami, je zakaždým potrebné vytvoriť heslo nové.

3.3.2.4. Zložitosť hesla a priestor kľúčov

Zložitosť samotného hesla je určená hlavne veľkosťou príslušného priestoru kľúčov. Priestor kľúčov je počet všetkých kľúčov (hesiel), ktoré sa dajú vytvoriť z danej znakovej sady a majú vopred určenú maximálnu dĺžku. Priestor kľúčov sa dá ľahko matematicky vypočítať ako veľkosť použitej znakovej sady plus 1 a to celé umocnené na maximálnu dĺžku hesla.

Zložitosť hesla je potom daná použitím dostatočne veľkého priestoru kľúčov, pričom si zvolíme maximálnu dĺžku hesla a nepoužijeme žiadnu z *postupnosti rozloženia znakov na klávesnici*. Pod pojmom *postupnosť rozloženia znakov na klávesnici* je myslený sled znakov na klávesnici v rade, napr. qwertzuiop (qwertyuiop), asdfghjkl, yxcvbnm (zxcvbnm), a 1234567890, prípadne niektorá jeho časť.

Inými slovami, heslo bude mať dobrú zložitosť ak použijeme malé aj veľké písmena spolu s číslicami a špeciálnymi znakmi. Napr.: *kHz34#@oRT8*=%*.

3.3.2.5. Generovanie zapamätateľ ných hesiel

V praxi často používanou metódou na generovanie zapamätateľných hesiel je metóda odvádzania a substitúcie. Metóda spočíva v tom, že používateľ si vymyslí vetu, napr.: *"Keď budem mať 20 rokov, tak navštívim exotickú krajinu."*, z tejto vety použije všetky začiatočné písmena. Takto získame podklad pre heslo *"Kbm2rtnek"*. Následne zameníme znaky napr. takto: $A \rightarrow 4$, $a \rightarrow @$, $E \rightarrow 3$, $e \rightarrow 3$, $S \rightarrow $$, $s \rightarrow $$, $T \rightarrow 7$, $t \rightarrow 7$, $O \rightarrow 0$, $o \rightarrow 0$, $L \rightarrow !$, $l \rightarrow 1$, $i \rightarrow 1$. Takto získame heslo *"Kbm2r7n3k"*. Ak by sa nám výsledne heslo nezdalo dostatočne silné, tak môžeme pridať ďalšie špeciálne znaky, napr. *#* na začiatok hesla a ? na koniec. Výsledné heslo teda nadobudne podobu *"#Kbm2r7n3k?"*.

3.3.3. Obrázkové heslá

OS Windows 8 a 8.1 obsahujú možnosť použitia tzv. obrázkových hesiel. Ide o alternatívny spôsob prihlasovania sa. Používateľovi je umožnené prihlásiť sa pomocou troch dotykových gest na používateľom zvolenom obrázku. Používateľ si za každé gesto môže vybrať bod v ľubovoľnom mieste obrázku, úsečku spájajúcu dva body alebo kružnicu. Používatelia si zväčša vyberajú významné body na obrázkoch, čo značne redukuje celkový priestor kľúčov, v tomto prípade množstvo gest.

Teda iba na základe daného obrázku je možné určiť použité gesto. OS Windows našťastie limituje maximálny počet chybných prihlásení obrázkovým heslom na 5. Ak sa tento limit vyčerpá, tak je používateľ vyzvaný na prihlásenie sa klasickým heslom.

Preto neodporúčame používanie obrázkových hesiel pre ich pomerne nízku bezpečnosť.

3.3.4. Bezpečné heslo – zhrnutie

Za bezpečné heslo považujeme teda heslo, ktoré spĺňa nasledujúce podmienky:

- Je dlhé aspoň 12 znakov.
- Obsahuje malé a veľké písmená abecedy, čísla a špeciálne znaky (z každej množiny aspoň jeden výskyt).
- Nie je to slovníkové slovo alebo výraz.
- Nie je asociovateľné s užívateľom.
- Nie je staršie ako jeden rok.

V prípade ak existuje podozrenie na kompromitáciu hesla je nutné vykonať zmenu hesla okamžite, teda kontaktovať v tejto veci administrátora počítača a udalosť nahlásiť aj ako bezpečnostný incident správcovi služby, ku ktorej bolo možné kompromitovaným heslom pristupovať.

3.4. Vytvorenie a používanie používateľ ských účtov

Dôležitým krokom po samotnej inštalácii OS Windows je vytvorenie štandardného (bežného, neprivilegovaného) používateľského účtu, nakoľko používateľ vytvorený počas inštalácie je automaticky priradený do skupiny administrátorov.

Bežný používateľský účet, na ktorý sa bude používateľ PC prihlasovať v rámci bežnej práce s počítačom, je jedným z hlavných bezpečnostných prvkov v OS Windows. Tento účet má slúžiť čisto pre potreby bežnej práce s PC, teda pomocou tohto účtu nebude možné inštalovať ďalšie programy, ani meniť systémové nastavania.

Takéto opatrenie slúži na obmedzenie šírenia škodlivého kódu v prípade infikovania PC. Pre potreby zmeny systémových nastavení alebo inštalácie prídavného softwaru je nutné používať administrátorsky účet, napr. ten, ktorý bol vytvorený v rámci samotnej inštalácie OS.

Pri bežnej práci nikdy nepoužívajte administrátorský účet.

3.4.1. Vytvorenie používateľského účtu

Na vytvorenie alebo úpravu používateľských účtov sú potrebné administrátorské oprávnenia.

Rozhranie umožňujúce vytvorenie nového používateľského účtu (kontá), prípadne jeho úpravu, je dostupné pomocou *Ovládacieho panelu (Control Panel)* a položky *Používateľské kontá (User Accounts)*.

3.4.1.1. Windows XP

Úvodná obrazovka ponúka okrem možnosti vytvorenia nového používateľského účtu, aj možnosti úpravy používateľského účtu a zmenu spôsobu prihlasovania a odhlasovania sa používateľov.



Ikony s menami používateľov v spodnej časti úvodnej obrazovky umožňujú priamy prístup k správe konkrétneho používateľa.

Z úvodnej obrazovky je potrebné zvoliť *Vytvoriť nové konto (Create a new account)*. Na nasledujúcej obrazovke je potrebné vyplniť meno pre nového používateľa.

😫 User Accounts		
Ġ Back 💮 🔮 Home		
	Name the new account: MovePousivate This name will appear on the Welcome screen and on the Start menu.	Liext > Cancel

Ako ďalšie je potrebné zvoliť typ používateľského účtu, presnejšie jeho úroveň oprávnení. V prípade vytvárania administrátorského účtu je potrebné zvoliť voľbu *Správca počítača (Computer administrator)*. V prípade vytvárania bežného účtu je potrebné zvoliť voľbu *S obmedzeným prístupom (Limited)*, ako vidíme na obrázku nižšie.



Na vytvorenie nového používateľského účtu je potrebné stlačiť tlačidlo Vytvoriť účet (Create Account).

Na nasledovnom obrázku je možné vidieť novú ikonu pre nového používateľa.



Po kliknutí na túto ikonu sa otvorí okno s možnosťami správy tohto používateľského účtu. Teraz je potrebné vytvoriť pre používateľa nové heslo pomocou voľby *Vytvoriť heslo (Create a password)*. Odporúčame sa riadiť podľa informácií uvedených vyššie v časti venovanej heslám.



Na vytvorenie nového hesla pre zvoleného používateľa je potrebné nové heslo zadať dvakrát, aby sa vylúčila možnosť preklepu v danom hesle. Následne je vyžadovaná fráza, prípadne slovo, ktoré pripomenie používateľovi jeho heslo. Odporúčame do tohto poľa zadať formuláciu "Kontaktujte svojho administrátora!!!".



Heslo pre používateľský účet bude vytvorené po stlačení tlačidla Vytvoriť heslo (Create password).

Ak chceme používateľský účet zmazať, tak je potrebné zvoliť v správe tohto účtu voľbu Zmazať konto (Delete the account). Následne sa zobrazí obrazovka s možnosťou buď zmazania alebo ponechania súborov tohto používateľského účtu.



Na ďalšej obrazovke je vyžadované už iba potvrdenie zmazania používateľského účtu, ktoré sa potvrdí voľbou *Zmazať konto (Delete Account)*.



3.4.1.2. Windows 7

Úvodná obrazovka ponúka, na rozdiel od Windows XP, priamo správu prihláseného používateľa. Pre správu iných používateľských účtov je teda potrebné zvoliť voľbu *Spravovať iné konto (Manage another account)*, kde sa zobrazí prehľadové okno so všetkými používateľskými účtami.





Ikony s menami používateľov umožňujú priamy prístup k správe konkrétneho používateľa. Na vytvorenie nového používateľského účtu je potrebné zvoliť voľbu *Vytvoriť nové konto (Create a new account)*.



Na nasledujúcej obrazovke je potrebné vyplniť meno pre nového používateľa a zvoliť typ používateľského účtu, presnejšie jeho úroveň oprávnení. V prípade vytvárania administrátorského účtu je potrebné zvoliť voľbu *Správca (Administrator)*. V prípade vytvárania bežného účtu je potrebné zvoliť voľbu *Štandardný používateľ (Standard user)* ako je možné vidieť na obrázku vyššie. Na vytvorenie nového používateľského účtu je potrebné stlačiť tlačidlo *Vytvoriť účet (Create Account)*.

Na nasledovnom obrázku je možné vidieť novú ikonu pre nového používateľa v prehľade používateľský účtov.



Po kliknutí na túto ikonu sa otvorí okno s možnosťami správy tohto používateľského účtu. Teraz je potrebné vytvoriť pre používateľa nové heslo pomocou voľby *Vytvoriť heslo (Create a password)*. Odporúčame sa riadiť podľa informácií uvedených vyššie v časti venovanej heslám.

🕒 💭 🖉 « Manage Accounts 🕨 Change an Account	▼ 49	Search Control Panel	Q
Make changes to NovyPouzivatel's account			
Change the account name			
Create a password		NovyPouzivatel	
Change the picture		Standard user	
Set up Parental Controls			
Change the account type			
Delete the account			
Manage another account			

				x
🕞 🗸 🥵 « Change an Account 🕨 Cr	eate Password	🗸 🍫 Search Contro	l Panel	\$
Create a password for Novy	/Pouzivatel's account			
NovyPouzivatel Standard user				
You are creating a password for Nov	yPouzivatel.			
If you do this, NovyPouzivatel will	lose all EFS-encrypted files, perso	nal certificates and sto	red passwords	
To avoid losing data in the future, as	:s. sk NovvPouzivatel to make a passw	ord reset floppy disk.		
	······			
New password				
Confirm new password				
If the password contains capital lette How to create a strong password	ers, they must be typed the same wa	ay every time.		
Tune a near used bint				
Type a password hint				
What is a password hint?	everyone who uses this computer.			
· · · · F				
		Create password	Cancel	

Na vytvorenie nového hesla pre zvoleného používateľa je potrebné nové heslo zadať dvakrát, aby sa vylúčila možnosť preklepu v danom hesle. Následne je vyžadovaná fráza, prípadne slovo, ktoré pripomenie používateľovi jeho heslo. Odporúčame do tohto poľa zadať formuláciu "Kontaktujte svojho administrátora!!!".

Heslo pre používateľský účet bude vytvorené po stlačení tlačidla Vytvoriť heslo (Create password).

3.5. Inštalácia, konfigurácia a používanie bezpečnostných nástrojov

Medzi nutnú softwarovú výbavu každého počítača patrí anti-malwarové riešenie a firewall. Táto softwarová výbava tvorí základný stavebný kameň bezpečnosti počítača.

3.5.1. Anti-malware riešenie

Anti-malware riešenie slúži na identifikáciu a prípadne odstránenie škodlivého kódu. Jeho základnou úlohou je prevencia, teda zabránenie infikovania PC. Dôležitou vlastnosťou je ochrana v reálnom čase, označovaná aj ako real-time ochrana (*Real-time Shield, Real-time Protection*), prípadne rezidentná ochrana.

Ako vhodné neplatené anti-malware riešenia spomenieme Avast!, Avira, AVG, Spyware Terminator, Spybot a Ad-Aware, prípadne Windows Defender (pre Windows 7 a vyššie verzie).

Ako ďalší príklad vhodného neplateného anti-malware riešenie spomenieme Microsoft Security Essentials, ktoré poskytuje funkcionalitu anti-malware riešenia, hoci je ho možné zaradiť medzi komplexné riešenia, ktoré sú spomínané v ďalšej časti.

Za vhodné platené alternatívy považujeme napríklad Kaspersky Anti-Virus, ESET NOD32 Antivirus a McAfee AntiVirus Plus.

3.5.1.1. Používanie anti-malware riešenia

• Inštalácia:

Anti-malwarové riešenie je potrebné inštalovať hneď po nainštalovaní operačného systému. Ak to nie je možné, je potrebné ho inštalovať v najskoršom možnom čase.

• Aktualizácia:

Aktualizujte pravidelne databázu signatúr škodlivého kódu. Ideálnym intervalom aktualizácie je jeden deň pri počítači pripojenom k Internetu a jeden týždeň pri počítači nepripojenom do Internetu.

• Rezidentná ochrana:

V anti-malwarovom riešení je potrebné povoliť rezidentnú ochranu systému (ochrana počítača počas bežnej prevádzky).

• Kontrola systému

Systém pravidelne kontrolujte na prítomnosť škodlivého kódu vo forme kontroly všetkých súborov a aj bootovacej partície. Ak je to možné, je potrebné nastaviť túto kontrolu ako automatizovanú. Odporúčaná frekvencia úplnej kontroly je jeden mesiac.

Pred spustením alebo skopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory skontrolovať anti-malwarovým riešením. Uvedená voľba sa najčastejšie nachádza v kontextovom menu súborov (po kliknutí pravého tlačidla myši na súbor).

3.5.1.2. Microsoft Security Essentials

Ako bolo spomenuté vyššie, Microsoft Security Essentials je neplatené anti-malware riešenie.

• Inštalácia

Riaďte sa pokynmi sprievodcu. Nižšie uvedená obrázková dokumentácia znázorňuje celý priebeh inštalácie.

Microsoft Security Essenti	ials
	Víta vás Sprievodca inštaláciou aplikácie Microsoft Security Essentials
Microsoft Security Essentials	Aplikácia Security Essentials pomáha zlepšiť zabezpečenie a výkon počítača. Aplikácia Security Essentials sa neustále dopĺňa o nové funkcie a služby, ktoré môžu vyžadovať odosielanie dodatočných informácií spoločnosti Microsoft. Ďalšie informácie nájdete v dokumente <u>Vyhlásenie o ochrane osobných údajov</u> . Najnovšie aktualizácie sa prevezmú po dokončení inštalácie. Pokračujte kliknutím na tlačidlo Ďalej.
	Ďalej > Zrušiť

Microsoft Security Essentials		
Licenčné podmienky pre softvér Microsoft Secu	rity Essentials	
Pozorne si prečítajte nasledujúce licenčné podmienky pre soft	rér:	
LICENČNÉ PODMIENKY PRE SOFTVÉR A SLU MICROSOFT	JŽBU ONLINE SPOL	LOČNOSTI
MICROSOFT SECURITY ESSENTIALS		
Tieto licenčné podmienky sú zmluvou medzi spolo (alebo podľa miesta vášho bydliska jednou z jej afi Vzťahujú sa na softvér menovaný vyššie vrátane n	čnosťou Microsoft Co ácií) a vami. Prečítajt nédií (ak existujú), na	orporation e si ich. ktorých ste ho ▼
Kliknutím na tlačidlo Súhlasím vyjadrujete svoj súhlas s licenčr pre softvér.	ými podmienkami	Tlačiť
Vyhlásenie o ochrane osobných údajov	Súhlasím	Nesúhlasím

Microsoft Security Essentials
Zapojiť sa do programu zvyšovania spokojnosti zákazníkov
Môžete sa zapojiť do programu zvyšovania spokojnosti zákazníkov a odosielaním informácií o používaní aplikácie Security Essentials pomôcť spoločnosti Microsoft zlepšiť tento produkt.
Zhromaždené informácie sa nepoužijú na vašu identifikáciu ani na vaše kontaktovanie a z tohto programu môžete kedykoľvek vystúpiť.
Ďalšie informácie o programe zvyšovania spokojnosti zákazníkov
Prehlásenie o ochrane osobných údajov
🔘 Zapojiť sa do programu zvyšovania spokojnosti zákazníkov
Momentálne sa nechcem zapojiť do programu
< Späť Ďalej > Zrušiť

Microsoft Security Essentials	
Optimalizovať zabezpečenie	
Ak chcete optimalizovať ochranu počítača, mali by ste používať bránu firewall. Ak brána firew nie je zapnutá, aplikácia Security Essentials môže počas tejto inštalácie zapnúť bránu Windows Firewall.	all s
🕼 Ak nie je zapnutá žiadna brána firewall, zapnúť bránu Windows Firewall (odporúča sa)	
Tento softvér obsahuje funkciu, ktorá môže určité súbory identifikovať ako podozrivé. Ak vyberiete túto možnosť, súbory alebo informácie o nich sa môžu automaticky odoslať do spoločnosti Microsoft na ďalšiu analýzu. Spoločnosť Microsoft používa tieto súbory a informá na identifikáciu nového malvéru a vylepšenie ochrany.	icie
Zapnúť automatické odosielanie vzoriek.	
< Späť Ďalej >	Zrušiť

Microsoft Security Essentials
Inštalácia aplikácie Microsoft Security Essentials je pripravená
Ak sú v počítači nainštalované iné antivírusové programy alebo programy na ochranu pred spyware, môžu spôsobiť konflikt s aplikáciou Security Essentials a zabrániť jej správnemu fungovaniu. Prítomnosť viacerých antivírusových programov alebo programov na ochranu pred spyware môže tiež spôsobiť vážne problémy s výkonom počítača.
Pred spustením tohto sprievodcu odporúčame odstrániť všetky ostatné antivírusové programy a programy na ochranu pred spyware.
Ako odinštalovať ostatné antivírusové programy a programy na ochranu pred spyware?
Inštalácia > Zrušiť

🚠 Microso	Microsoft Security Essentials			
Inštal	ácia aplikácie Microsoft Security Essentials			
đ	Počkajte, kým sprievodca nainštaluje aplikáciu Security Essentials do počítača. Môže to trvať niekoľko minút.			
	Stav: Inštaluje sa Security Essentials			
	Zrušiť			

Microsoft Security Essent	tials
	Dokončenie práce Sprievodcu inštaláciou aplikácie Microsoft Security Essentials
Microsoft	Sprievodca inštaláciou aplikácie Security Essentials sa úspešne dokončil.
Security Essentials	Dokončite inštaláciu kliknutím na tlačidlo Dokončiť. Aplikácia Security Essentials sa spustí automaticky a skontroluje najnovšie definície vírusov a spyware.
	Skontrolovať počítač kvôli možným hrozbám po získaní najnovších aktualizácií.
	Dokončiť

• Aplikácia

Úvodná obrazovka aplikácie je zobrazená na obrázku 1. Sú na nej zobrazené informácie o aktuálnom stave real-time ochrany a aktuálnosti databázy signatúr (*Definície vírusov a spywaru*). Z úvodnej obrazovky je možné priamo spustiť kontrolu počítača.

Medzi možnosti kontroly patrí rýchly test. Ten kontroluje pamäť počítača a základné adresáre operačného systému.

Aspoň raz mesačne odporúčame vykonať *Úplnú kontrolu počítača*, ktorá skontroluje celý počítač. Priebeh kontroly pri tomto nastavení je zobrazený na obrázku **2**.

Poslednou možnosťou je tzv. *Vlastná kontrola*, ktorá ponúkne používateľovi možnosť zvoliť si adresáre, prípadne aj celé diskové partície, ktoré sa následne budú kontrolovať. – Obrázok 3.

Domov Aktualizovať História Nastavenie	Pomocník
Počítač sa monitoruje a je chránený.	Možnosti kontroly:
 Ochrana v reálnom čase: Zapnutá Definície vírusov a spywaru: Aktuálne 	Skontrolovať teraz
Podrobnosti kontroly Plánovaná kontrola: Denne okolo 16:00 (Rýchla kontrola) Zmeniť plá	in kontroly

Obrázok 1

Microsoft Security Essentials		
Stav počítača: Chránený		
Domov Aktualizovať	História Nastavenie	🥐 Pomocník 👻
Kontroluje sa počítač Môže to trvať istý čas v z	ávislosti od vybratého typu kontroly.	
Typ kontroly:	Úplná kontrola	
Začiatok:	22:19	
Uplynulý čas:	00:00:04	
Skontrolované položky:	581	
Položka:	C:\Program Files (x86)\Adobe\Reader 10.0\Reader\Locale\cs_CZ\DVA.CZE	

Obrázok 2

Microsoft Security Essentials	×
Vyberte jednotky a priečinky, ktoré chcete skontrolovať: Local Disk (C:) Local Disk (E:) Local Disk (E:) BD-ROM Drive (G:) 	

Dôležitá je pravidelná aktualizácia nielen samotnej aplikácie, ale aj databázy signatúr. Táto aktualizácia prebieha automaticky, ale je možné ju manuálne vynútiť na záložke *Aktualizovať* a to voľbou *Aktualizovať* - Obrázok 4.

Microsofi Stav po	t Security Essentials čítača: Chránený		
Domo	ov Aktualizovať História	Nastavenie	🧿 Pomocník 🔻
	Definície vírusov a spyware: Aktuálr	ne	
	Z dôvodu ochrany počítača sa automat	icky aktualizujú definície vírusov	a spyware.
	Definície vytvorené: Naposledy aktualizované definície: Verzia definícií vírusov: Verzia definícií spywaru:	6.1.2014 o12:37 6.1.2014 o21:00 1.165.1271.0 1.165.1271.0	Akt <u>u</u> alizovať
0	Viete, že		
	Definície vírusov, spyware a ostatného m nechcený softvér v počítači. Tieto definície sa aktualizujú automaticky tlačidlo Aktualizovať.	alvéru sú súbory, pomocou ktor y. Najnovšie aktualizácie však mô	ých sa identifikuje škodlivý alebo potenciálne)žete získať v ľubovoľnom čase kliknutím na

Obrázok 4

Záložka *Nastavenia* umožňuje nastaviť *Plánovanú kontrolu, Predvolené akcie,* real-time ochranu a mnoho ďalších nastavení. Kontrolu počítača je možné vykonávať plánovane, kde je možné zvoliť nielen kedy sa bude kontrola vykonávať, ale je možné zvoliť aj jej úroveň – Obrázok 5.

V nastaveniach *Predvolených akcií* je možné upraviť nastavenia akcií, ktoré sa vykonajú, v závislosti od úrovne hrozby, ktorá bola detegovaná – Obrázok 6.

Ako je uvedené vyššie, z pohľadu bezpečnosti počítača je dôležité, aby bola zapnutá real-time ochrana – Obrázok 7.

V nastaveniach *Rozšírené* je dôležité mať aktívne voľby *Kontrolovať archívne súbory* a *Kontrolovať vymeniteľné jednotky* – Obrázok 8.

Microsoft Security Essentials	
Stav počítača: Chránený	
Domov Aktualizovať Hi Plánovaná kontrola Predvolené akcie Ochrana v reálnom čase Ochrana v reálnom čase Vylúčené súbory a umiestnenia Vylúčené typy súborov Vylúčené procesy Rozšírené Komunita MAPS	tória Nastavenie Image: Spustiť plánovanú kontrolu v počítači (odporúča sa) Image: Spustiť plánovanú kontrolu v počítači (odporúča sa) Image: Spusteri mage:

Obrázok 5

Microsoft Security Essentials		
Stav počítača: Chránený		
Domov Aktualizovať	História Nastavenie	🖓 Pomocník 🔻
Plánovaná kontrola Predvolené akcie Ochrana v reálnom čase Vylúčené súbory a umiestnenia Vylúčené typy súborov Vylúčené procesy Rozšírené Komunita MAPS	Vyberte akciu, ktorá sa má pri hrozby s nasledujúcimi úrovň <u>Čo sú úrovne výstrah a čo tre</u> Závažná dôležitosť výstrah Odporúčaná akcia Vysoká dôležitosť výstrahy Odporúčaná akcia Stredná dôležitosť výstrahy: Odporúčaná akcia Nízka dôležitosť výstrahy: Odporúčaná akcia	edvolene zobraziť alebo použiť, keď sa zistia potenciálne ami výstrah. <u>ba robiť?</u> y: v: v: v: v: v: v: v: v: v: v: v: v: v:
		Uložiť zmeny <u>Z</u>rušiť

Microsoft Security Essentials			
Stav počítača: Chránený			
Domov Aktualizovať Plánovaná kontrola Predvolené akcie Ochrana v reálnom čase	História Nastavenie	n ča <u>s</u> e (odporúča sa) s sa zobrazí upozornenie, keď sa škodlivý alebo iný	Pomocník ▼
Vylúčené súbory a umiestnenia Vylúčené typy súborov Vylúčené procesy Rozšírené Komunita MAPS	nechceny softver pokusi n	ainstaiovat sam seba do vasno pocitaca alebo sa v	nom spusut.
		Uožiť zmeny	<u>Z</u> rušiť

Microsoft Security Essentials Stav počítača: Chránený		x
Domov Aktualizovať	História Nastavenie ? Pomocník	c 🔻
Plánovaná kontrola Predvolené akcie Ochrana v reálnom čase Vylúčené súbory a umiestnenia Vylúčené typy súborov Vylúčené procesy Rozšírené Komunita MAPS	 Kontrolovať archívne súbory Umožňuje zahrnúť archívne súbory, ako sú napríklad súbory .zip alebo .cab. Kontrolovať vymeniteľné jednotky: Počas úplnej kontroly umožňuje zahrnúť vymeniteľné jednotky, ako napríklad USB kľúče. Vytvoriť bod obnovenia systému Umožňuje pred odstránením alebo spustením zistených položiek alebo ich presunutím do karantény vytvoriť v počítači bod obnovenia systému. Povoliť všetkým používateľom zobraziť všetky výsledky histórie Všetkým používateľom tohto počítača sa povolí zobrazenie všetkých zistených položiek na karte História. (Týmto spôsobom sa zobrazia položky, ktoré sú v záujme ochrany osobných údajov používateľov zvyčajne skryté.) Odstrániť súbory v karanténe po: Súbory v karanténe zostanú zakázané, kým ich nepovolíte alebo neodstránite. 	
	Image: Construction of the second	

3.5.2. Firewall

Firewall, resp. brána firewall, je v prípade PC softwarové zariadenie (aplikácia), ktoré slúži k riadeniu sieťovej prevádzky. Zjednodušene sa dá definovať ako kontrolný bod definujúci pravidlá pre komunikáciu medzi vonkajšou sieťou, napr. LAN alebo sieť Internet, a samotným PC.

Samotný OS Windows v sebe obsahuje funkcionalitu firewallu. Ak sa tento firewall správne nakonfiguruje, tak plne postačuje pre bežné PC.

Za vhodné neplatené firewall riešenie považujeme napríklad Windows Firewall, Comodo Free Firewall, TinyWall a ZoneAlarm Free Firewall.

Odporúčame, aby ste používali firewall s nasledovnými nastaveniami:

- Funkcionalita firewallu je zapnutá pre všetky sieťové pripojenia.
- Firewall blokuje všetky prichádzajúce pripojenia s výnimkou tých, ktoré sú zadané ako povolené. To znamená, že sú zadané ako výnimky v pravidlách firewallu.
- Funkcionalita firewall je zapnutá pre všetky druhy sietí (súkromné, verejné alebo doménové).

3.5.2.1. Odporúčané nastavenia

Pre zvýšenie zabezpečenia OS Windows je možné zakázať všetky prichádzajúce spojenia ako je odporúčané vyššie, ale aj všetky odchádzajúce spojenia. V prípade blokovania všetkých odchádzajúcich spojení je ale dôležité pridať výnimku pre každú službu, ktorú chceme používať. Napríklad pre základnú prácu s webovým prehliadačom je nutné povoliť prehliadaču používanie portov 80, a 443 spolu s protokolom TCP a portu 53 spolu s protokolom UDP smerom z koncovej stanice do siete Internet.

Poznámka

Windows Firewall implementovaný v OS Windows XP nedokáže blokovať odchádzajúce spojenia.

3.5.2.2. Windows Firewall – OS Windows XP

Nastavenie Windows Firewallu je dostupné pomocou *Ovládacieho panelu (Control Panel)* a položky *Brána firewall systému Windows (Windows Firewall)*.

Na nasledovnom obrázku 9 je zobrazené úvodne okno s informáciou o aktuálnom stave firewallu. V tomto prípade je firewall aktívny.





V záložke *Výnimky (Exceptions)* je zoznam povolených programov. V prípade ak firewall nie je aktívny, je táto informácia na tejto záložke uvedená, podobne ako na obrázku 10.

😺 Brána fi	rewall sy	stému Windows	×
Všeobecné	Výnimky	Spresnenie	
Brána firev správca po	vall systému očítača.	Windows Firewall je vypnutá. Tieto nastavenia riadi váš	
Programy a	a služby:		
	Notes		
Pomo Systé ✓ Vzdia ↓ Vind ↓ Vind ∠dieľ	c na dial ku m UPnP lená pracov ows Remote ows Remote anie súboro	ná plocha e Management e Management - Compatibility Mode (HTTP-In) v a tlačiarní	
Pri <u>d</u> ať pr	ogram	Pridať po <u>r</u> t Upr <u>a</u> víť <u>O</u> dstrániť]
✓ Zobraz	ť upozorner	nie, keď brána firewall systému Windows zablokuje prograr	n
<u>Aké sú rizi</u>	(á povoleni)	a výnimiek?	
		OK Zrušiť	

Overenie, či je funkcionalita firewallu zapnutá pre všetky sieťové pripojenia, je možné vykonať na záložke *Spresnenie (Advanced)* – Obrázok 11. Štandardne sú uvedené položky ako *Lokálne pripojenie (Local Area Connection)* a *Bezdrátové pripojenie (Wireless Network Connection),* prípadne aj *Pripojenie 1394 (1394 Connection),* ak počítač disponuje týmto rozhraním.

šeobecné Výriniky Spresnenie Nastavenie sieťového pripojenia Brána firewall systému Windows je zapnutá pre pipojenia vybrané nižšie. Al chcete pridď výriniky pre samostatné pripojenie, vyberte dané pripojenie a kliknite na takidilo Nastavenie: Image: Strategy st	Frána firewall systému Windows	
Nastavenie sieťového pripojenia Brána firewall systému Windows je zapnutá pre pripojenia vybrané nižšie. Al chcete pridať vybiniky pre samostatné pripojenie, vyberte dané pripojenie a kliknite na tlačidlo Nastavenie. Image: Status i stat	eobecné Výnimky Spresnenie	
Brána firewall systému Windows je zaprutá pre pripojenia vybrané nižšie. Al chote pridať výriniky pre samostatné pripojenie, vybenté dané pripojenie a kliknite na tladičilol Nastavenie: Image: Status pri samostatné pripojenie, vybenté dané pripojenie a kliknite na tladičilol Nastavenie. Image: Status pripojenie Image: Status pri pripojenie <td>Nastavenie sieťového pripojenia</td> <td></td>	Nastavenie sieťového pripojenia	
Veckálne pripojenie Nagtavenie Pripojenie 1334 Nagtavenie Zapisovanie do denníka zabezpečenia Za Za účelom riešenia problémov môžete vytvoriť súbor denníka. Nastavenie Protokol ICMP Prostredníctvom protokolu ICMP (Internet Control Message Protocol) môžu počítače v sieti zdieľať informácie o chybách a stave. Nastavenie Predvolené nastavenia Ak chcete obnovíť všetky predvolené nastavenia brávy firewall systému Windows, kliknite na tlačidlo Obnovíť predvolené. Dnoviť predvolené	Brána firewall systému Windows je zapnutá pre pripoji chcete pridať výnimky pre samostatné pripojenie, vyb kliknite na tlačidlo Nastavenie:	enia vybrané nižšie. Ak arte dané pripojenie a
Zapisovanie do denníka zabezpečenia Za účelom riešenia problémov môžete vytvoriť súbor denníka. Protokol ICMP Prostredníctvom protokolu ICMP (Internet Control Message Protocol) môžu počítače v sieti zdieľať informácie o chybách a stave. Predvolené nastavenia Ak chcete obnovíť všetky predvolené nastavenia brávy firewall systému Windows, kliknite na tlačidlo Øbnovíť predvolené.	☑ Lokálne pripojenie ☑ Pripojenie 1394	Na <u>s</u> tavenie
Protokol ICMP Prostední ctvom protokolu ICMP (Internet Control Message Protocol) môžu počítače v sieti zdieľať informácie o chybách a stave. Predvolené nastavenia Ak chcete obnoviť všetky predvolené nastavenia brány firewall systému Windows, kliknite na tlačidlo Obnoviť predvolené.	Zapisovanie do denníka zabezpečenia Za účelom riešenia problémov môžete vytvoriť súbor denníka.	N <u>a</u> stavenie
Prostredníctvom protokolu ICMP (Internet Control Message Protocol) môžu počítače v sieti zdieľať informácie o chybách a stave. Predvolené nastavenia Ak chcete obnovíť všetky predvolené nastavenia brány firewall systému Windows, kliknite na tlačidlo Obnovíť predvolené.	Protokol ICMP	
Predvolené nastavenia Ak chcete obnoviť všetky predvolené nastavenia brány firewall systému Windows, kliknite na tlačidlo Obnoviť predvolené.	Prostredníctvom protokolu ICMP (Internet Control Message Protocol) môžu počítače v sieti zdieľať informácie o chybách a stave.	<u>N</u> astavenie
Ak chcete obnoviť všetky predvolené nastavenia brány firewall systému Windows, kliknite na tlačidlo Obnoviť predvolené.	Predvolené nastavenia	
	Ak chcete obnoviť všetky predvolené nastavenia brány firewall systému Windows, kliknite na tlačidlo Obnoviť predvolené.	Obnoviť predvolené

Obrázok 11

Nastavenie samotných pravidiel pre Windows Firewall sa deje v záložke *Výnimky* (Obrázok 10), a to pomocou volieb *Pridať program … (Add Program …)* (Obrázok 12) a *Pridať port … (Add port …)*, prípadne *Upraviť … (Edit …)* (Obrázok 13).

Pridanie programu	×
Ak chcete povolíť komunikáciu s programom jeho pridaním do zoznamu Výnimky, vybette daný program, alebo kliknutím na tlačidlo Vyhľadávať vyhľadajte program, ktorý sa v zozname nenachádza. <u>P</u> rogramy:	
😰 7-Zip File Manager	^
Roadcom Advanced Control Suite 2	
🚔 Canon MF Network Scan Utility	≣
A Sector	
ESET Smart Security	-
ESET SysInspector	
Jahren Blauer	
A InterActual Player	
Martine Actual Hayer Onlinstall	
	<u>×</u>
Cesta: C:\Program Files\7-Zip\7zFM.exe Prehľadáva	r
Zmeniť rozsah OK Zrušiť	

Obrázok 12

V prípade *Pridania programu* (Obrázok 12) je danej aplikácií povolené plné spojenie. To znamená, že aplikácia má povolené používať oba protokoly TCP a UDP a s nimi všetky dostupné porty.

V prípade *Pridania portu,* resp. *Upraviť* (Obrázok 13) je možné špecifikovať konkrétny port a k nemu prislúchajúci protokol (TCP alebo UDP)

Pridanie portu 🔀	Upraviť port 🛛 🔀
Tieto nastavenia použite na otvorenie portu prostredníctvom brány firewall systému Windows. Číslo portu a protokol nájdete v dokumentácii k programu alebo službe, ktorú chcete používať.	Tieto nastavenia použite na otvorenie portu prostredníctvom brány firewall systému Windows. Číslo portu a protokol nájdete v dokumentácii k programu alebo službe, ktorú chcete používať.
Meno:	Meno: Windows Remote Management
Číglo portu:	Číglo portu: 5985
⊙ ICP O UDP	⊙ ICP O UDP
Aké sú riziká otvorenia portu? Zmeniť rozsah OK Zrušiť	Aké sú riziká otvorenia portu? Zmeniť rozsah OK Zrušť

^	L	- 4 -			4.7
U	n	ca:	70	IK.	1.5
~		-			

Ako nastaviť odporúčané nastavenia vo Windows Firewall

Ako ukážkový príklad zvolíme vlastnú aplikáciu *Explor*, ktorá plní funkciu jednoduchého webového servera na portoch 80 a 443 s protokolom TCP, teda pre jej správnu funkčnosť potrebuje prijímať spojenia.

- 1. Je potrebné byť prihlásený ako administrátor.
- 2. Teraz je potrebné spustiť konfiguračné rozhranie pre nastavenie Windows Firewallu, ktoré je dostupné pomocou *Ovládacieho panelu (Control Panel)* a položky *Brána firewall systému Windows (Windows Firewall)*.
- 3. Je potrebné skontrolovať používanie firewallu (Obrázok 9).

- 4. Teraz je potrebné pridať výnimku pre aplikáciu (Obrázok 10).
- 5. Pomocou voľby *Pridať program … (Add Program …)* (Obrázok 12) vyberieme požadovanú aplikáciu webového prehliadača, v tomto prípade aplikáciu *Explor*, a voľbu potvrdíme tlačidlom *OK*.

Pridanie programu	×
Ak chcete povoliť komunikáciu s programom jeho pridaním do zoznamu Výnimky, vyberte daný program, alebo kliknutím na tlačidlo Vyhľadávať vyhľadajte program, ktorý sa v zozname nenachádza. <u>P</u> rogramy:	
SESET SysRescue	^
🖤 Explor	
🚑 FreeCell	
A InterActual Player	
🕎 InterActual Player Uninstall	
🧶 Internetová dáma	
Internetové piky	
Internetové reversi	
Internetové srdcia	
🧭 Internetový backgammon	
Kartová hra Srdcia	~
Cesta: C:\explore.exe Prehľadávať	
Zmeniť rozsah OK Zrušiť	

6. Následne označíme novovytvorenú výnimku a zvolíme voľbu Upraviť ... (Edit ...).

🖗 Brána firewall systému Windows 🛛 🛛 🔀				
Všeobecné Výnimky Spresnenie				
Brána firewall systému Windows je vypnutá. Váš počítač je vystavený nebezpečenstvu útokov a prienikov z vonkajších zdrojov, ako je napríklad Internet. Odporúčame, aby ste klikli na kartu Všeobecné a vybrali nastavenie Zapnuté.				
Programy a služby:				
Názov				
 Explor Lotus Notes Network Diagnostics for Windows XP Pomoc na diaľku Systém UPnP Vzdialená pracovná plocha Windows Remote Management Windows Remote Management - Compatibility Mode (HTTP-In) Zdieľanie súborov a tlačiarní 				
Pridať program Pridať port Upraviť Odstrániť Zobraziť upozornenie, keď brána firewall systému Windows zablokuje program Aké sú riziká povolenia výnimiek?				

Výsledkom bude nasledovné okno.

Úргаvа ргоз	yramu 🔀			
Komunikáciu s týmto programom môžete povoliť pre každý počítač, vrátane počítačov na Internete, alebo len pre počítače v sieti.				
Meno:	💙 Explor			
Cesta:	C:\explor.exe			
Zmeniť rozsal	n OK Zrušiť			

Takto je v nastaveniach Windows Firewall povolená aplikácia Explor.

Ak je žiaduce povolenie iba portu 443, tak je postup nasledovný:

- V 5. kroku sa nezvolí voľba *Pridať program … (Add Program …)*, ale zvolí sa voľba *Pridať port … (Add port …)* (Obrázok 5).
- Zadá sa nové meno Explor port 443 a taktiež sa zadá číslo portu 443 a ako protokol sa zvolí TCP.

Pridanie portu 🔀				
Tieto nastavenia použite na otvorenie portu prostredníctvom brány firewall systému Windows. Číslo portu a protokol nájdete v dokumentácii k programu alebo službe, ktorú chcete používať.				
<u>M</u> eno:	Explor - port 443			
Čí <u>s</u> lo portu:	443			
<u>Aké sú riziká otvorenia portu?</u>				
Zmeniť rozsah	OK Zrušiť			

Takto je v nastaveniach Windows Firewall povolený port 443 s protokolom TCP. Obdobne sa postupuje aj v prípade iného portu , napr. portu 80 a protokolu TCP.

Aplikácia Explor teraz môže prijímať prichádzajúce spojenia. Celkový výsledok by mal byť nasledovný:

🐱 Brána firewall systému Windows 🛛	×			
Všeobecné Výnimky Spresnenie				
Brána firewall systému Windows je vypnutá. Váš počítač je vystavený nebezpečenstvu útokov a prienikov z vonkajších zdrojov, ako je napríklad Internet. Odporúčame, aby ste klikli na kartu Všeobecné a vybrali nastavenie Zapnuté.				
Programy a služby:				
Názov				
Explor - port 443				
Lotus Notes				
Pomoc na diaľku				
□ Systém UPnP				
✓ Vzdialená pracovná plocha				
Windows Remote Management				
Windows Remote Management - Compatibility Mode (HTTP-In)				
∐∠dielanie suborov a (laciarni				
Pridať program) Pridať po <u>r</u> t Upr <u>a</u> viť <u>O</u> dstrániť				
☑ Zobraziť upozornenie, keď brána firewall systému Windows zablokuje program				
<u>Aké sú riziká povolenia výnimiek?</u>				
OK Zrušiť				

3.5.2.3. Windows Firewall – OS Windows 7

Nastavenie Windows Firewallu je dostupné pomocou *Ovládacieho panelu (Control Panel)* a položky *Brána firewall systému Windows (Windows Firewall)*.

Na nasledovnom obrázku je zobrazené úvodne okno s informáciou o aktuálnom stave firewallu. V tomto prípade je firewall aktívny pre všetky siete.



Nastavenie firewallu je možné zmeniť pomocou voľby v ľavom menu *Zapnúť alebo vypnúť bránu Windows Firewall (Turn Windows Firewall on or off)*, kde sa následne zobrazí nasledovná obrazovka.

🕒 🗢 📾 « Wir	ndows Firewall Customize Settings	٩
Custor You can What are Home o	mize settings for each type of network modify the firewall settings for each type of network location that you use. e network locations? or work (private) network location settings Turn on Windows Firewall Block all incoming connections, including those in the list of allowed programs Votify me when Windows Firewall blocks a new program Turn off Windows Firewall (not recommended)	
Public n	network location settings	
0	Turn on Windows Firewall Block all incoming connections, including those in the list of allowed programs Image: Notify me when Windows Firewall blocks a new program	
Ø	Turn off Windows Firewall (not recommended)	
	OK Cancel]

Pomocou voľby Povolenie komunikácie programu prostredníctvom brány Windows Firewall (Allow a program or feature through Windows Firewall) je možné povoliť, prípadne blokovať, aplikácie a služby na firewalle. Na nasledovnom obrázku je znázornené toto rozhranie s prehľadom povolených aplikácií a služieb.

	-	-	_ D X
🚱 🕞 🗢 🔐 « All Control Panel Items 🔸 Windows Firewall 🕨 Allowed Programs	👻 🐓 Search	Control Panel	م
Allow programs to communicate through Windows P To add, change, or remove allowed programs and ports, click Change What are the risks of allowing a program to communicate? Allowed programs and features: Name BranchCache - Content Retrieval (Uses HTTP) BranchCache - Hosted Cache Client (Uses HTTPS) BranchCache - Hosted Cache Server (Uses HTTPS) BranchCache - Peer Discovery (Uses WSD) Connect to a Network Projector Core Networking Distributed Transaction Coordinator File and Printer Sharing HASP LLM HomeGroup HP Remote Graphics	irewall e settings. Bench Home/Work (Private)	Public Public Remove	
	ОК	Cancel	

Pomocou voľby *Povoliť iný program … (Allow another program …)* je možné pridať ďalšie pravidlo pre firewall, pomocou výberu konkrétnej aplikácie. V tomto prípade je na obrázku nižšie vybraná opäť aplikácia Internet Explorer.

Add a Program	×	
Select the program you want to add, or click Browse to find one that is no listed, and then click OK.	ot	
Programs:		
🔩 Immunity Debugger	*	
S Intel® Management and Security Status		
🖗 Intel® Matrix Storage Console		
Every KeePass 2	-	
f Microsoft Security Essentials	-	
🥪 Microsoft Silverlight		
Nmap - Zenmap GUI		
Variate VM VirtualBox		
Rageant		
Er Pullingen	Ŧ	
P <u>a</u> th: C:\Program Files\Internet Explorer\jexplore.e Browse		
What are the risks of unblocking a program?		
You can choose which network location types to add this program to.		
Network location types Add Cancel		

Na ďalšom obrázku je zobrazená situácia po stlačení tlačidla *Pridať (Add)*. Teraz je daná aplikácia pridaná do zoznamu povolených programov, kde je možné upraviť jej prístup pre konkrétnu sieť.

🚱 🔵 🗢 🕍 « All Control Panel Items 🕨 Windows Firewall 🕨 Allowed Pro	ograms 👻 4 Search Control Panel 🔎
Allow programs to communicate through Wir	ndows Firewall
To add, change, or remove allowed programs and ports, clic	k Change settings.
What are the risks of allowing a program to communicate?	🛞 Cha <u>ng</u> e settings
Allowed programs and features:	
Name	Home/Work (Private) Public ^
Connect to a Network Projector	
Core Networking	
Distributed Transaction Coordinator	
HP Remote Graphics	
HP Remote Graphics	
HP Remote Graphics	
HP SkyRoom	
Internet Explorer	
iSCSI Service	
	Details Remove
	Allow another program
	OK Cancel

V prípade potreby povolenia, prípadne blokovania, konkrétneho portu je potrebné na úvodnej obrazovke zvoliť voľbu *Rozšírené nastavenie (Advanced settings)*. Následne sa zobrazí nasledovné okno:



Štandardne je všetka odchádzajúca komunikácia povolená. Ak je požadované blokovanie všetkých odchádzajúcich spojení, tak je potrebné zmeniť nastavenie *Outbond connections* na *Blokovanie* (*Block*) pomocou ponuky *Rozšírené nastavenie* (*Advanced settings*) a následne voľby *Windows Firewall Properties*.



Upozornenie

Ak vo Windows Firewall sú zakázané aj všetky odchádzajúce spojenia, tak **pre správnu funkcionalitu je potrebné povoliť všetky porty, na ktorých komunikujú aplikácie, ktoré budeme chcieť používať**, ako napr. anti-malware riešenie, internetový prehliadač, e-mailový klient, prípadne ftp klient a iné.

Ako príklad uvedieme povolenie portu 443. Postup nasledovný:

• Z ľavého menu zvolíme *Pravidlá odchádzajúcej komunikácie (Outbound Rules)* a v pravom menu zvolíme *Nové pravidlo (New rule,)* výsledok by mal byť podobný ako na obrázku, kde zvolíme voľbu *Port*:

New Outbound Rule Wizard	a
Rule Type Select the type of firewall rule to ce	reate.
Steps: Protocol and Ports Action Profile Name	What type of rule would you like to create? Program Rule that controls connections for a program. P rdef Rule that controls connections for a TCP or UDP pot. P rdefined: BranchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. O Lostom Custom rule.
	< Back Next > Cancel

• V nasledujúcom kroku je potrebné zvoliť požadovaný protokol *TCP* a príslušný port *443*.

💣 New Outbound Rule Wizard	1	deline .	x		
Protocol and Ports					
Specify the protocols and ports to	which this rule applies.				
Steps:					
Rule Type	Does this rule apply to TCP or UDF	??			
Protocol and Ports	<u>Т</u> СР				
 Action 	© <u>U</u> DP				
 Profile 					
 Name 	Does this rule apply to all remote po	orts or specific remote ports?			
	All remote ports				
	Specific remote ports:	443			
		Example: 80, 443, 5000-5010			
	Learn more about protocol and por	ts			
		< <u>B</u> ack <u>N</u> ext > Cancel			

• V ďalšom kroku je potrebné nastaviť požadovanú akciu, teda či spojenie bude povolené alebo blokované.

Prev Outbound Rule Wizard	And a second	×			
Action					
Specify the action to be taken whe	n a connection matches the conditions specified in the rule.				
Steps:					
Rule Type	What action should be taken when a connection matches the specified conditions?				
Protocol and Ports	Allow the connection				
Action	This includes connections that are protected with IPsec as well as those are not.				
Profile	Allow the connection if it is secure.				
• Name	 Allow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize Block the connection 	a			

• V predposlednom kroku je potrebné ešte konkretizovať pre aké siete sa má toto pravidlo uplatňovať. Na obrázku sú zvolené všetky siete.

🔗 New Outbound Rule Wizard	d la			
Profile				
Specify the profiles for which this n	ule applies.			
Steps:				
Rule Type	When does this rule apply?			
Protocol and Ports				
Action	Domain			
Profile	Applies when a computer is connected to its coliporate domain.			
Name	Applies when a computer is connected to a private network location			
	Applies when a computer is connected to a public network location.			
	Learn more about profiles			
	< Back Next > Cancel			

• V poslednom kroku je potrebné iba vytvárané pravidlo pomenovať a stlačiť tlačidlo *Dokončiť* (*Finish*). V tomto prípade je pravidlo nazvané *Internet Explorer* – 443.

🔐 New Outbound Rule Wizard		3
Name		
Specify the name and description	this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name		
	Description (optional):	
	< <u>B</u> ack Finish Cancel	

Takto je v nastaveniach Windows Firewall povolený port 443 s protokolom TCP. Obdobne sa postupuje aj v prípade iných portov a protokolov, napr. portu 80 a protokolu TCP.

Výsledok by mal byť nasledovný:

Windows Firewall with Advanced	Security		2	٩	
File Action View Help					
🗢 🔿 🙍 🖬 🗟 🖬					
🔗 Windows Firewall with Advance	Outbound Rules				Actions
Inbound Rules	Name	Group	Profile	~	Outbound Rules
Connection Security Pular	Internet Explorer - 443		All		🐹 New Rule
Monitoring	HP Remote Graphics		All		Eilter by Brofile
p age monitoring	IP Remote Graphics		All .	_	
	🕑 HP Remote Graphics		All	-	Y Filter by State
	🕑 HP SkyRoom		All		Tilter by Group
	BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr	All		View 🕨
	BranchCache Hosted Cache Client (HTT	BranchCache - Hosted Cach	All	-1	Refrech
	BranchCache Hosted Cache Server(HTTP	BranchCache - Hosted Cach	All		
	BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove	All		Export List
	Connect to a Network Projector (TCP-Out)	Connect to a Network Proje	Private		? Help
	Connect to a Network Projector (TCP-Out)	Connect to a Network Proje	Domain		Internet Evolorer - 443
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain		Disable Rule
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private		🔏 Cut
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain		🖹 Сору
	Connect to a Network Projector (WSD-O	Connect to a Network Proje	All		¥ Delete
	Core Networking - DNS (UDP-Out)	Core Networking	All		
	Core Networking - Dynamic Host Config	Core Networking	All		Properties
	Core Networking - Dynamic Host Config	Core Networking	All		Help
	Core Networking - Group Policy (LSASS	Core Networking	Domain		
	Core Networking - Group Policy (NP-Out)	Core Networking	Domain		
	Core Networking - Group Foncy (TCP-O	Core Networking			
	Core Networking - IPHTTPS (TCP-Out)	Core Networking	All		
	Core Networking - IPv6 (IPv6-Out)	Core Networking	All		
	Ocore Networking - Multicast Listener Do	Core Networking	All		
	Ocore Networking - Multicast Listener Ou	Core Networking	All		
	Ore Networking - Multicast Listener Rep	Core Networking	All		
	Ore Networking - Multicast Listener Rep	Core Networking	All		
	Core Networking - Neighbor Discovery A	Core Networking	All		
	Ocore Networking - Neighbor Discovery S	Core Networking	All		
	Ocore Networking - Packet Too Big (ICMP	Core Networking	All -	-	
< III >	•		+		

Upozornenie

V PC postačuje jedna aplikácia starajúca sa o zabezpečenie funkcionality firewallu (okrem firewallu, ktorý je pravdepodobne súčasťou sieťového smerovača). Ak by v počítači existovali viaceré bežiace aplikácie s touto funkcionalitou, tak by to mohlo vyvolať konflikty a problémy.

Poznámka

Pre správne fungovanie zobrazovania webových stránok je potrebné povoliť porty 443/TCP, 80/TCP a 53/UDP.

3.5.3. Komplexné riešenie

Komplexné riešenie je zlúčením anti-malwarového riešenia spolu s ďalšou funkcionalitou. Vo väčšine prípadov poskytujú takéto riešenia aj funkcionalitu firewallu, webového filtra a mnoho inej funkcionality, a to v závislosti od rozsahu licencie pre konkrétny produkt.

Ako vhodné neplatené riešenia spomenieme Microsoft Security Essentials.

Za vhodné platené alternatívy považujeme Kaspersky Internet Security, ESET Smart Security, McAfee Total Protection a Avast! Internet Security.

3.6. Pravidelná aktualizácia použitého softvéru

Každú aplikáciu nainštalovanú v PC je nutné aktualizovať, nielen samotný OS. Sú to práve aplikácie, ktoré najviac infikujú počítač.

3.6.1. Operačný systém

Rozhranie pre aktualizáciu operačného systému *Windows Update* je dostupné pomocou *Ovládacieho panelu (Control Panel)* a položky *Windows Update*.

V tomto rozhraní je možné manuálne skontrolovať dostupnosť nových aktualizácií a to pomocou tlačidla *Vyhľadať aktualizácie*.



V prípade nájdenia dostupných aktualizácií je možné ich stiahnuť a nainštalovať. Ak nie sú dostupné žiadne nové aktualizácie, bude zobrazené nasledovné okno:



Pomocou voľby *Zmeniť nastavenia (Change settnigs)* je možné skontrolovať a prípadne upraviť nastavenie aktualizácií operačného systému. Odporúčané nastavenie je uvedené na obrázku.

Image: Second state of the second
Výber spôsobu, akým má systém Windows inštalovať aktualizácie
Systém Windows môže automaticky zisťovať dostupnosť dôležitých aktualizácií, keď je počítač online, a inštalovať ich na základe týchto nastavení. Keď sú k dispozícii nové aktualizácie, môžete ich nainštalovať aj pred vypnutím počítača.
Aké sú výhody automatickej aktualizácie?
Dôlež <u>i</u> té aktualizácie
🐼 Inštalovať aktualizácie automaticky (odporúča sa) 👻
Inštalovať nové akt <u>u</u> alizácie: každý deň 🔹 <u>o</u> 3:00 👻
Odporúčané aktualizácie
Poskytovať odporúčané aktualizácie rovnakým spôsobom ako dôležité aktualizácie
Kto môže inštalovať aktualizácie
Povoliť všetkým používateľom inštalovať aktualizácie v tomto počítači
Microsoft Update
Poskytovať aktualizácie pre produkty spoločnosti Microsoft a vyhľadávať nový voliteľný softvér spoločnosti Microsoft pri aktualizácii systému Windows
Upozornenia na softvér
🔲 Zobrazovať podrobné oznámenia, keď je k dispozícii nový softvér spoločnosti Microsoft
Poznámka: Služba Windows Update sa môže pred vyhľadávaním ďalších aktualizácií sama automaticky aktualizovať. Prečítajte si <u>prehlásenie spoločnosti Microsoft o používaní osobných údajov online</u> .
🔞 OK Zrušiť

3.6.2. Prehliadač dokumentov pdf

Najznámejším prehliadačom dokumentov pdf je Adobe Acrobat Reader. Vhodnou alternatívou je napr. aplikácia Foxit.

Obe aplikácie kontrolujú dostupnosť novších verzií, pokiaľ to nemajú zakázané vo svojich nastaveniach.

V prípade Adobe Acrobat Readeru je používateľ informovaný o možnosti stiahnutia a nainštalovania aktualizácie upozornením zobrazeným na obrázku.



Inštalácia aktualizácie prebieha obdobne ako inštalácia samotnej aplikácie.

3.6.3. Java

Java je programovací jazyk a výpočtová platforma. Nakoľko existuje veľa aplikácií a webových stránok, ktoré bez nainštalovania Javy nebudú fungovať, tak Java Framework je nutnou súčasťou softwarovej výbavy bežného počítača. Java taktiež upozorňuje na dostupnosť novej aktualizácie.



Inštalácia aktualizácie prebieha podobne ako inštalácia samotného frameworku.

3.6.4. Webový prehliadač

Moderné webové prehliadače používajú filtrovanie webového obsahu pomocou reputačných databáz ako spôsob ochrany používateľa pred webovými stránkami obsahujúcimi škodlivý kód.

Odporúčame používať prehliadače Mozilla Firefox, Google Chrome, Opera a Internet Explorer.

V prípade webových prehliadačov je obzvlášť nutná ich aktualizácia na najnovšiu verziu hneď ako je to možné. Webové prehliadače si samé kontrolujú svoje aktualizácie a keď je dostupná novšia verzia, tak na túto skutočnosť používateľa upozornia a ponúknu mu možnosť aktualizácie.

3.6.4.1. Mozilla Firefox

Aktualizácie je možné taktiež manuálne skontrolovať pomocou položky *O prehliadači Firefox* v menu *Pomocník*. Okno, ktoré sa následne zobrazí je uvedené nižšie.



Následne sa daná aktualizácia stiahne, nainštaluje a následne sa prehliadač reštartuje.

Nastavanie aktualizácie prehliadača je možné zmeniť v *Možnostiach* prehliadača sekcia *Spresnenie*, na záložke *Aktualizácie*. Na obrázku je vidieť odporúčané nastavenie.

Možnosti							
		Ţ		OP		Ó	
Všeobecné Karty Obsah Aplikácie Súkromie Bezpečnosť Synchronizácia Spresnenie Všeobecné Sieť Aktualizácie Šifrovanie Aktualizácie prehliadača Firefox Aktualizácie prehliadača Firefox Automaticky inštalovať aktualizácie (odporúčané z dôvodu zvýšenej bezpečnosti) Upozorniť, ak by nainštalovanie zakázalo niektoré doplnky Vyhľadávať aktualizácie, ale poskytnúť možnosť zvoliť, či sa nainštalujú Nevyhľadávať aktualizácie (neodporúča sa z dôvodu zníženej bezpečnosti) 							
Zobraziť <u>h</u> istóriu aktualizácií Na inštaláciu aktuali <u>z</u> ácií používať službu na pozadí Automaticky aktualizovať: Vyhľadávacie moduly							
				(ОК	Zrušiť	<u>Pomocník</u>

3.7. Inštalácia a konfigurácia nástrojov na rodičovskú kontrolu

V časti Používateľské účty sme popísali ako rozdeliť používateľov na dve skupiny a to na administrátorov a bežných používateľov. V tejto časti sa budeme venovať ďalšiemu obmedzeniu používateľských oprávnení.

3.7.1. Popis

Rodičovská kontrola (Parental controls) je funkcia, ktorá umožňuje administrátorovi (napr. rodičovi) nastaviť limity pre používanie počítača. Umožňuje napr. nastaviť čas, ktorý používateľ (napr. dieťa) môže stráviť pri PC. Ďalej umožňuje nastaviť skupinu programov (napr. hry), ktorú môže daný používateľ spúšťať (teda používať). Svoje uplatnenie môže nájsť aj v rámci rôznych aplikácií, ktoré túto funkciu podporujú. Medzi takéto aplikácie patrí Windows Media Center, kde je umožnené zablokovať prístup k nežiaducemu televíznemu vysielaniu a filmom.

Keď sa pomocou rodičovskej kontroly blokuje prístup k určitému programu alebo hre, zobrazí sa upozornenie, že program je zablokovaný. Používateľ môže kliknúť na odkaz v upozornení a požiadať o povolenie na prístup k programu alebo hre. Prístup môže byť následne povolený administrátorom (rodičom) a to zadaním požadovaných informácií.

Upozornenie

Ak je počítač pripojený k doméne, rodičovská kontrola nie je k dispozícii. Rodičovskú kontrolu je možné používať iba pre štandardné používateľské kontá. Funkcia rodičovskej kontroly je dostupná v OS Windows Vista a vyššie.

3.7.2. Nastavenia funkcie Rodičovská kontrola

Pre zmenu nastavení Rodičovskej kontroly je potrebné byť prihlásený ako používateľ s administrátorskými oprávneniami. Konfiguračné rozhranie pre nastavenie Rodičovskej kontroly je dostupné pomocou *Ovládacieho panelu (Control Panel)* a položky *Rodičovská kontrola (Parental Control)*.

Ako prvý krok je potrebné zvoliť používateľský účet, pre ktorý chceme Rodičovskú kontrolu nastaviť, prípadne upraviť. Po výbere štandardného používateľského konta by malo byť zobrazené okno podobné tomu na obrázku 14 uvedenom nižšie. Po zapnutí rodičovskej kontroly by malo okno nadobudnúť podobu ako na obrázku 15.

Teraz je možné meniť jednotlivé nastavenia Rodičovskej kontroly kliknutím na príslušné prepojenia.



Obrázok 14



Obrázok 15

3.7.3. Nastavenie konkrétne časové obmedzenie používania PC

Nastavením časových obmedzení je možné určiť, kedy má vybraný používateľ povolené prihlásiť sa do svojho používateľského účtu. Časové obmedzenia zabraňuje používateľovi prihlásiť sa do počítača počas určených hodín. Takéto časové obmedzenie je možné nastaviť pre každý deň v týždni zvlášť. Napr. na obrázku 16 je zobrazené nastavenie, ktoré umožňuje byť používateľovi prihlásený od 16:00 do 19:00 počas pracovných dní a od 13:00 do 19:00 počas víkendu.

Samotné nastavenie časového rozvrhu sa deje za pomoci vyznačovania časového harmonogramu pomocou myši.





Upozornenie

Keď je používateľ prihlásený v čase, keď sa skončí vyhradený čas na prihlásenie sa, používateľ bude automaticky odhlásený.

3.7.4. Obmedzenie spúšťania programov

Pomocou tohto nastavania je možné riadiť prístup k aplikáciám, napr. aj hrám, ale v prípade hier odporúčame využiť aj funkciu Obmedzenia spúšťania hier, ktorá je popísaná nižšie. Po kliknutí na voľbu *Povolenie a blokovanie konkrétnych programov* je možné zvoliť povolenie všetkých programov alebo len programov, ktoré administrátor povolí, ako je uvedené na obrázku nižšie.



Následne sa po zvolení druhej možnosti načíta zoznam programov, kde je možné pomocou voľby *Prehľadávať …* pridať nový program do tohto zoznamu.

🗢 🌆 🛠 Kontrola noužívateľ	ov 🕨 Obmedzenia anlikácií	- 40	Prehľadávať: Ovládací pa	nel
		• • 7	Prentodovot. Ovladaci pa	//CL
Ktoré programy môže O Používateľ UpdatusUser Používateľ UpdatusUser	používateľ UpdatusUser použív r môže používať všetky programy r môže používať len programy, ktoré pove	ať? blím		
Vyberte programy, ktoré moži	no používať:			_
Súbor	Popis	Názov produ	uktu	-
C:\Program Files (x86)\Code	eMeter\Runtime\bin			^ -
🔲 💷 cmu32.exe	CodeMeter Universal Support Tool	<neznáme></neznáme>		
🔲 😋 CodeMeter.exe	CodeMeter Runtime Server	<neznáme></neznáme>		
🔲 😋 CodeMeterCC.exe	CodeMeter Control Center	<neznáme></neznáme>		
C:\Program Files (x86)\Com	nmon Files\InstallShield\Driver\7\Intel 32			^
🔲 🚰 IDriver.exe	InstallDriver Module	InstallDriver	Module	
C:\Program Files (x86)\Com	nmon Files\InstallShield\Professional\Run	Time\11\00\Ir	ntel32	
ISBEW64.exe	InstallShield (R) 64-bit Setup Engine	InstallShield	(R)	
🔲 💷 DotNetInstaller.exe	DotNetInstaller	<neznáme></neznáme>	•	
C:\Program Files (x86)\Com	nmon Files\microsoft shared\DW			~
🔲 📬 DW20.EXE	Microsoft Application Error Repor	<neznáme></neznáme>		
DWTRIG20.EXE	Watson Subscriber for SENS Netw	<neznáme></neznáme>		
C:\Program Files (x86)\Com	nmon Files\microsoft shared\EQUATION			<u>^</u> -
Pridať program do zozna	mu: Prehľadávať	V	ybrať všetky Zrušiť v	ýber
				.214

Pre tento účel sme zvolili inštalačnú aplikáciu ovládačov grafickej karty (*setup.exe*). Po nájdení konkrétneho programu napr. s príponou *exe* a potvrdení sa zobrazí nižšie uvedené okno.



Po jeho potvrdení sa následne aktualizuje zoznam aplikácií a pribudne v ňom nová položka.

a first her			_ D X
🚱 🕞 🗢 🌆 « Kontrola použí	vateľov 🕨 Obmedzenia aplikácií	👻 🐓 Prehľadávať: Ovládac	í panel 🔎
Ktoré programy m	Ôže používateľ UpdatusUser použív IsUser môže používať všetky programy IsUser môže používať len programy, ktoré pov	rať? olím	
Vyberte programy, ktoré	možno používať:		
Súbor	Popis	Názov produktu	^
C:\NVIDIA\DisplayDriv	er\314.07\Win8_WinVista_Win7_64\Internation	al	· ·
🗹 🃦 setup.exe	NVIDIA Install Application	NVIDIA Install Application	
C:\Program Files (x86)	\CodeMeter\Runtime\bin		~
🔲 💷 cmu32.exe	CodeMeter Universal Support Tool	<neznáme></neznáme>	
🔲 😋 CodeMeter.exe	CodeMeter Runtime Server	<neznáme></neznáme>	
CodeMeterCC.exe	e CodeMeter Control Center	<neznáme></neznáme>	
C:\Program Files (x86)	\Common Files\InstallShield\Driver\7\Intel 32		- ^
🔲 💒 IDriver.exe	InstallDriver Module	InstallDriver Module	
C:\Program Files (x86)	\Common Files\InstallShield\Professional\Run	Time\11\00\Intel32	- ^
ISBEW64.exe	InstallShield (R) 64-bit Setup Engine	InstallShield (R)	
🔲 💷 DotNetInstaller.ex	e DotNetInstaller	<neznáme></neznáme>	
C:\Program Files (x86)	\Common Files\microsoft shared\DW		- ^
🔲 🛸 DW20.EXE	Microsoft Application Error Repor	<neznáme></neznáme>	-
Pridať program do :	zoznamu: Prehľadávať	Vybrať všetky Zruš	šiť výber
		ОК	Zrušiť

3.7.5. Obmedzenie spúšťania hier

Pomocou tohto nastavania je možné riadiť prístup k hrám na základe výberu určitej úrovne hodnotenia a to na základe vhodnosti pre určitú vekovú kategóriu. Ďalej je možné vybrať typy obsahu, ktoré bude blokované. Nakoniec je možné priamo povoliť alebo blokovať konkrétne hry.

Základné nastavenie je zobrazené na obrázku 17. Toto nastavenie povoľuje používateľovi hrať hry. Maximálne povolené hodnotenie hier je nastavené na úroveň 18+, vrátane možnosti hrať hry, ktoré takéto hodnotenie nemajú.





Obrázok 18 znázorňuje príklad nastavenia obmedzení pre vekovú skupinu do 16 rokov s tým, že chceme blokovať všetok nežiaduci obsah.

Obrázok 19 znázorňuje výsledné nastavenia pre zvolené používateľské konto.

Pomocou funkcie Rodičovská kontrola je možné riadiť, ktoré hry má vybraný používateľ (napr. dieťa) povolené spúšťať (hrať) v rámci svojho používateľského účtu.

Nastavenie obsahuje nasledovné voľby:

- Všetky hry
- Konkrétne hry podľa vlastného uváženia
- Konkrétne hry na základe hodnotenia ich vhodnosti pre určitú vekovú kategóriu
- Konkrétne hry na základe hodnotenia ich obsahu

Bližšie informácie sú k dispozícií na adrese http://windows.microsoft.com/sk-sk/windows7/choosewhich-games-children-can-play, kde je postupnosť krokov ako jednotlivé voľby nastaviť.



				x
🚱 🕞 🗢 🌆 « Rodičovská 🕨 Kontrola používateľov	▼ 4 ₇	Prehľadávať: Ovl	ádací panel	Q
				0
Nastavenie spôsobu, akým môže používateľ Upda	itusUser p	oužívať počít	ač	
Rodičovská kontrola:	Aktuálne na	astavenia:		
Sapnutá, presadiť aktuálne nastavenie			or	
🔘 Vypnuté		Štandardný p	oužívateľ	
Nastavenie systému Windows		Chránené hes	lom	
Časové obmedzenia Kontrola používanja počítaža používateľom Updaturiljser	Časové o	bmedzenia:	Zapnuté	
	Hodnote	nie hier:	Maximálne 12+	
 Hry Kontrola hier podľa hodnotenia, obsahu alebo názvu 	Obmedze	enie programov:	Vypnuté	
Povolenie a blokovanie konkrétnych programov Povolenie a blokovanie programov v počítači				
			0	к

Upozornenie

Ak však počítač hru nerozpozná, rodičovská kontrola ju nezablokuje. V tomto prípade je potrebné nezablokovanú hru manuálne pridať do zoznamu blokovaných programov.

3.7.6. Ovládacie prvky

Okrem základných ovládacích prvkov, ktoré poskytuje systém Windows, môžme nainštalovať ďalšie ovládacie prvky aj od iných poskytovateľov služieb. Tieto ovládacie prvky je možné používať v rámci funkcie Rodičovská kontrola na spravovanie spôsobu, akým bežný používateľ využíva počítač. Napríklad napriek tomu, že filtrovanie webového obsahu a protokolovanie aktivity nie sú súčasťou inštalovanej verzie systému Windows, je možné tieto ďalšie ovládacie prvky nainštalovať prostredníctvom iného poskytovateľa služieb.

3.7.7. Webový filter

Filtrovanie webového obsahu je účinným spôsobom ako znížiť riziko infikovania počítača a zároveň vo veľkej miere obmedziť používateľa v prístupe k webovému obsahu, ktorý administrátor považuje za nevhodný pre používateľov všeobecne. Moderné webové filtre umožňujú filtrovať obsah webových stránok na základe ich obsahu, napr. obsah pre dospelých, drogy, alkohol alebo hazardné hry. Umožňujú definovať nielen zakázaný obsah (Blacklist Filtering), ale tiež iba povolený obsah (Whitelist Filtering). Preto môžme webový filter využiť ako prostriedok na kontrolu dostupnosti obsahu pre maloletého používateľa a implementovať tak rodičovskú kontrolu nad webovým obsahom a webovými službami.

Upozornenie

Filtrovanie webového obsahu, resp. obmedzenie dostupnosti niektorých webových stránok, je len doplnkom k zvýšeniu bezpečnosti počítača.

Ako vhodné neplatené riešenia poskytujúce funkcionalitu webového filtra spomenieme službu OpenDNS Basic, Kurupira Web Filter a K9 Web Protection.

3.7.7.1. Kurupira Web Filter

Jedná sa o aplikáciu poskytujúcu funkcionalitu rodičovskej kontroly, v rámci ktorej obsahuje aj webový filter.

Po samotnej inštalácií aplikácia si sama vyžiada zadanie hesla a e-mailového účtu. Tieto údaje sú následne vyžadované pri zmene nastavení tejto aplikácie. Následne je oznámené uloženie zadaného hesla. (Obrázok 20)

Set your password		
Password:	Email: (in order to recover a lost password)	🔥 Kurupira.Net
Confirm Password:	Confirm Email:	Password saved!
	<u> </u>	ОК

Obrázok 20



Obrázok 21

Obrázok 21 znázorňuje úvodne okno samotnej aplikácie. Hlavnými položkami v ľavej časti sú *Web, Applications* a *Settings*. Aplikácia sama umožňuje taktiež generovať *Správy (Reports)* a *Prehľady prístupov (History)*.



Položka Web umožňuje nastavenia webového filtra - Obrázok 22.

Obrázok 22

V rámci položky *Web* je možné nastavovať nielen samotný webový filter, ale tiež upravovať zoznam blokovaných webových stránok a zoznam povolených webových stránok, nastavovať časový harmonogram povolenia a blokovania prístupu k webovým stránkam, prípadne nastaviť čas, kedy bude aplikácia webového filtra vypnutá, a blokovanie sociálnych sietí a aplikácií určených na komunikáciu (IM – Instant messaging) - Obrázky 24 až 27. Obrázok 23 zobrazuje aktuálne nastavenie webového filtra.

Kurupira Web Filte	r 1.0.33	?
	UTUPICA WEB FILTER	SAFETY IN THE
	Web filter Web filter Automatically block inappropriate websites (artificial intelligence active) Prevent access ONLY to websites registered as blocked	Blocked websites
Web	Grant access DNLY for those websites registered as allowed Grant access to all websites, just keep tracking Exceptions	Allowed websites
Applications	Exceptions control how applications and websites run with Kurupira Web Filter. Add a applic to work without the Kurupira's intervention.	cation or website exception to allow it
Settings	NOTE: you don't need to set a list of blocked websites to enjoy the Kurupira's protection. The the great majority of the cases. Anyhow, you can add websites to the database. Also, access screen to download websites lists from our server. You can make an exception for a given web	Kurupira's artificial intelligence handles the Updates feature on Kurupira's home bsite, just register it as Allowed.
	Cano	Save settings

Obrázok 23

Kurupira Web Filte	r 1.0.33
	YOUR SAFETY IN THE DIGITAL JUNGLE
	Web Address: Action: Add to database
Web	No data found
Applications	
10	K Remove ALL listed from database
	Import websites list
Cattioner	entry. This action will edit the BLOCKED websites list.
Settings	
	Download websites list

Obrázok 24

Kurupira Web Filte	YOUR SAFETY IN THE DIGITAL JUNGLE
Web Web	ALLOWED websites list Web Address: Action: Add to database
Settings	Import websites list Add or remove websites listed in a text file. Use paragraph to delimit a new entry. This action will edit the ALLOWED websites list.
₽ ♠	Website exception

Vytvorené vlastné zoznamy povolených a zakázaných webových stránok je potom možné v prípade potreby aj exportovať.

Kurupira Web Filte)k		FIL	O) TER				R				JR	SAF	ET	Y	P X
		sun	mon	tue	wed	thu	fri	sat		sun	mon	tue	wed	thu	fri	sat		O Allow access
A COLORAD	00:00								12:00								_	O Division
	01:30								12:30									Block access
	01:30								13:30									👝 Disable Kurupira
	02:00								14:00									(sleep mode)
Web	02:30								14:30									Disable blocking
web	03:00								15:00									networking
	03:30								15:30									websites
	04:00								16:00									
	04:30								16:30									Allow all
	05:00								17:00									Block all
	05:30								17:30									
	06:00								18:30									Time allowance
Applications	07:00								19:00									03:00 per day
	07:30								19:30									(hh:mm)
	08:00								20:00									
1000	08:30								20:30									Block all windows
	09:00								21:00									
	09:30								21:30									Canaal
	10:00								22:00									Laricei
Settings	10:30								22:30									
	11:00								23:00									Save settings
	11:30								23:30					1				

Kurupira Web Filte	1.0.33
	YOUR SAFETY IN THE DIGITAL JUNGLE M and Social network Block access to Windows Live Messenger, AIM, Gtalk and similar (including the web versions) Block access to Skype
Web	Block access to the following social networking websites:
	TWITTER ORKUT MYSPACE YOUTUBE GOOGLE PLUS
Applications	BEBO HI5 SONICO
Settings	
	Cancel Save settings

Obrázok 27

Položka Applications umožňuje správu inštalovaných aplikácií - Obrázok 28.

Podobne ako v prípade webových stránok je možné vytvárať zoznam povolených aplikácií a zoznam zakázaných aplikácií. Aplikácia Kurupira Web Filter umožňuje aj zachytávať pracovnú plochu (screenshot) do formy obrázku, ktorý je následne možné nájsť v *Captured screens* – Obrázky 30 až 31.

Obrázok 29 znázorňuje aktuálne nastavenie aplikačného filtra.



Kurupira Web Filter	YOUR SAFETY IN THE DIGITAL JUNGLE
Web	Application filter Application for a streen shot every: I minute Application for a streen shot every: I minute
Applications	Always Between 00:00 and 23:59 The window title contains the word or expression: Add Remove
Settings	Cancel Save settings

Obrázok 29

Kurupira Web Filte	r 1.0.33
	UTUPITO WEB FILTER VOUR SAFETY IN THE DIGITAL JUNGLE
Web	BLOCKED applications list Window title: Action: Add to database Click for options No data found
Applications	Remove ALL listed from database Remove the selected records from database Import applications list Add or remove applications listed in a text file. Use paragraph to delimit a new entry. This action will edit the BLOCKED applications list.
	EALLOWED applications list ESet the applications filtering

Kurupira Web Filter	1.0.33 YOUR SAFETY IN THE DIGITAL JUNGLE
Web	ALLOWED applications list Window title: Action: Add to database No data found
Settings	Import applications list Add or remove applications listed in a text file. Use paragraph to delimit a new entry. This action will edit the ALLOWED applications list.
	BLOCKED applications list

Obrázok 31

Položka Settings umožňuje meniť nastavenia samotnej aplikácie - Obrázok 22. V rámci nastavení je možné zmeniť heslo, zmeniť e-mail a jazyk. Aktuálne sú v ponuke jazykov dostupné nemčina, angličtina, taliančina a portugalčina.

V prípade e-mailovej notifikácie sú zaujímavé voľby ako zasielanie správy v prípade prístupu na blokovanú stránku (*Whenever there is a website blockage*), spustenie blokovanej aplikácie (*Whenever there is a application blockage*), zhotovenie snímky pracovnej plochy (*Whenever Kurupira takes a screenshot*), prípadne keď je aplikácia Kurupira vypnutá (*Whenever the Kurupira is disabled*) alebo v presne určení čas (*Once a day at*).

Kurupira Web Filter 1	.0.33			? ×
	Drupira WEB FILTER	No and the second secon	YOUR SAFE DIGITAL	TY IN THE
Web	Password Current password: New password: Confirmation: Email notification Set your email account	Genera Hid Shr Get Keep H Place o	I le tray icon (stealth mode) ow Kurupira Toolbar : date/time from an Internet time serve istory data for 1 days of use: HOME	M T
Applications	Whenever there is a website block Whenever there is a application blo Whenever Kurupira takes a screen Kurupira takes a screen	age ockage shot	Whenever the Kurupira is disa Once a day at	bled
Settings	Choose the Kurupira language: English Deutsch English English	· (i) About	Up to challenge to translate Kuru Cancel	pira for a new language? <u>Click here.</u> Save settings
	1 Italiano	-		

Obrázok 32

V prípade zavretia aplikácie (minimalizácie) a jej následného zobrazenia sa je potrebné zadanie bezpečnostného hesla – Obrázok 33.

Kurupira.net - Login
Password:
Forgot your password? Cancel <u>O</u> K

Obrázok 33

3.7.7.2. Súbor hosts

Operačný systém Windows sám poskytuje možnosť ako vytvoriť v rámci samého seba webový filter. Ide ale o plne manuálne a zdĺhavé riešenie. OS Windows obsahuje súbor *hosts*, ktorý je umiestnený v adresári *Windows/System32/drivers/etc*. Ide o súbor obsahujúci záznamy o doménach a k ním priradených IP adresách. Ak je vo webovom prehliadači zadaný nejaký názov webovej stránky (nejaká doména), tak sa pre tento názov (túto doménu) vyhľadá zodpovedajúca IP adresa príslušného webového servera. Službu takéhoto prekladu poskytujú DNS servery (Domain Name System Servers). Operačný systém sa ale najskôr pozrie do súboru *hosts* a ak tam požadovaný záznam nenájde, tak sa pokúsi osloviť DNS servery, ktoré má nastavené, so snahou získať požadovanú IP adresu.

Problémom pri použití tohto webového filtra je nevyhnutnosť zadať všetky konkrétne názvy blokovaných stránok (domén) a ako IP adresu uviesť IP adresu 127.0.0.1.

Upozornenie

Na modifikáciu súboru hosts sú potrebné administrátorské oprávnenia.

4. Bezpečné používanie PC

Najslabším článkom v celej reťazi bezpečnostných prvkov z pohľadu počítačovej bezpečnosti je človek, teda používateľ. V reálnom svete a aj v tom virtuálnom by sa mal uvedomelý používateľ PC riadiť nasledovným heslom: "*Nič nie je zadarmo!*"

Toto heslo sa viaže nielen na používanie nelegálne získaných aplikácií a platných licenčných kľúčov, ale týka sa aj nelegálne získaných autorských diel (hudba, pozadia na pracovnú plochu a fotky) a obchádzania platených služieb prostredníctvom iných webových stránok.

V prípade nelegálne získaných aplikácií a platných licenčných kľúčov (vo forme záplaty - patchu) si používateľ sám inštaluje do svojho počítača aplikáciu modifikovanú neznámou treťou stranou. Tieto modifikácie v sebe často nesú škodlivý kód.

Nelegálne získané autorské diele nesú v sebe taktiež riziko infikovania PC. Škodlivý kód môže byť súčasťou mp3 skladby rovnako ako aj krásneho obrázka dažďového pralesa určeného ako obrázok na pracovnú plochu.

Návšteva webovej stránky je taktiež potenciálne nebezpečná. Preto by uvedomelý používateľ nemal klikať na každý URL odkaz, ktorý sa mu zobrazí či už na webovej stránke alebo ako súčasť e-mailu.

V prípade e-mailovej komunikácie je veľkou hrozbou tzv. phishing, kde hlavným cieľom je vylákanie prihlasovacích údajov od príjemcu takéhoto e-mailu.

Výsledkom vyššie uvedeného konania môže byť skutočnosť, že počítač sa stane napr. súčasťou siete botnet, ktorý sa ako súčasť takejto siete môže podieľať na riadenom útoku na iné siete. Ďalej môže byť takýto počítač využívaný ako C&C server (riadiaci server botnetu), dátový sklad pre nevhodný obsah (napr. detskú pornografiu) alebo prípadne môže šíriť nevyžiadanú poštu (SPAM).

Rovnako dôležité je uchovávanie hesiel. V tomto smere odporúčame aplikácie ako napr. KeePass alebo Password Saver.

V neposlednom rade je dôležité pravidelne vykonávanie zálohovania dôležitých súborov a dokumentov nachádzajúcich sa v počítači na sekundárny disk alebo externé úložné médium.

5. Zhrnutie

V tejto časti zhrnieme odporúčané postupy pre zníženie pravdepodobnosti výskytu alebo dopadov niektorých bežných rizík na počítače.

5.1. Používateľské účty

- 1. Je nutné používať výhradne účet pre bežného používateľa a iba v nutnom prípade použiť administrátorsky účet.
- 2. Používať samostatný používateľský účet na využívanie služieb ako je napr. Internet Banking a podobne.

5.2. Inštalácia programov

- Je potrebné inštalovať a používať iba legálne aplikácie, ktoré sú získané iba z dôveryhodného zdroja. V prípade, že na stránke výrobcu je aj kontrolný súčet je odporúčané tento kontrolný súčet overiť.
- 2. Rozšírenia do internetového prehliadača je vhodné inštalovať iba z dôveryhodných zdrojov.

5.3. Tvorba a uchovávanie hesiel

- Heslá nesmú byť uchovávané v elektronickej alebo papierovej podobe v nechránenom priestore. Ideálne je potrebné ich uchovávať iba v pamäti používateľa alebo v špecializovanom programovom vybavení, určenom pre tento účel.
- 2. Heslá nesmú byť rovnaké pre rôzne účty.
- 3. Heslá je potrebné vytvárať dostatočne komplexné, aby sa pravdepodobnosť úspechu útokov hádaním alebo hrubou silou minimalizovala. Treba používať malé a veľké písmená, čísla, diakritiku a ostatné tlačiteľné znaky.
- 4. Dĺžka hesla by mala mať aspoň 9 znakov.
- 5. Heslá nesmú byť asociovateľné s používateľom, nesmú mať slovníkový význam a nesmú byť vytvorené miernou modifikáciou predchádzajúcich typov.
- 6. Heslá je potrebné pravidelne meniť.
- 7. Heslá do dôležitých účtov je potrebné meniť aspoň raz za 12 mesiacov.
- 8. Heslá do menej dôležitých účtov je potrebné meniť aspoň raz za 2 roky.
- 9. V prípade, že existuje podozrenie na odhalenie hesla je nutné okamžite heslo zmeniť, teda kontaktovať v tejto veci administrátora počítača a udalosť nahlásiť aj ako bezpečnostný incident správcovi služby, ku ktorej bolo možné odhaleným heslom pristupovať.

5.4. Použitie anti-malwarového riešenia

- 1. Anti-malwarové riešenie inštalujte hneď po nainštalovaní operačného systému. Ak to nie je možné, je potrebné ho inštalovať v najskoršom možnom čase.
- Je potrebné aktualizovať pravidelne anti-malwarovú databázu signatúr. Ideálnym intervalom aktualizácie je jeden deň pri počítači pripojenom k Internetu a jeden týždeň pri počítači nepripojenom do Internetu.
- 3. V anti-malwarovom riešení je potrebné povoliť rezidentnú ochranu.

5.4.1. Kontrola systému

 Systém je potrebné pravidelne kontrolovať na prítomnosť škodlivého kódu vo forme prehliadky všetkých súborov a aj bootovacej partície. Ak je to možné, tak je treba nastaviť túto kontrolu ako automatizovanú. Odporúčaná frekvencia úplnej kontroly je jeden mesiac. 2. Pred spustením alebo skopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory skontrolovať anti-malwarovým riešením.

5.5. Použitie brány firewallu

- 1. Firewall je potrebné nainštalovať skôr ako je počítač pripojený k sieti.
- 2. Je potrebné ho pravidelne aktualizovať, ideálnym intervalom aktualizácie je jeden deň.

5.5.1. Nastavenie

- 1. Všetko je potrebné zakázať a povoľujú sa iba potrebné služby.
- 2. Ak počítač neslúži ako server alebo na zdieľanie priečinkov alebo tlačiarní, je vhodné zakázať akúkoľvek iniciáciu spojenia zo siete.
- 3. V prípade, že firewall umožňuje učenie sa prostredníctvom interakcie s používateľom, je potrebné povoľovať pri tejto interakcii iba také akcie, ktoré používateľ sám spustil a povoľovať spojenie do Internetu iba dôveryhodným aplikáciám.
- 4. Pre jednotlivé firewally je potrebné si prečítať odporúčanú konfiguráciu firewallu od výrobcu alebo "best practises" pre daný firewall z dôveryhodného zdroja a na základe týchto zdrojov firewall nastaviť.

5.6. Aktualizácie systému a aplikácií

- 1. Operačný systém by mal byť podporovaný výrobcom a v aktuálnej verzii.
- 2. Operačný systém je potrebné pravidelne aktualizovať. Ak to systém umožňuje je potrebné nastaviť automatické aktualizácie operačného systému.
- 3. Nainštalované aplikácie je potrebné pravidelne aktualizovať. Ak to aplikácia umožňuje je potrebné ju nastaviť na automatické inštalovanie aktualizácie, prípadne nastaviť zobrazovania upozornenia na novú aktualizáciu.
- 4. Je potrebné pravidelne aktualizovať aj doplnky aplikácií (plugins, kodeky audio a video formátov).

5.7. Používanie počítača

5.7.1. Prihlasovanie sa

- 1. Do počítača je potrebné vždy nastaviť prístupové heslo.
- 2. Pri odchode od počítača je potrebné vždy počítač zamknúť alebo odhlásiť sa.
- 3. Šetrič obrazovky je potrebné nastaviť tak, aby pri jeho vypnutí bolo potrebné heslo.
- 4. Heslo nesmie byť zapísané nikde v okolí počítača, teda nie na viditeľnom alebo ani menej viditeľnom mieste.

5.7.2. Šifrovanie

- 1. Všetky citlivé dáta v počítači je potrebné uchovávať iba v šifrovanej podobe.
- 2. Vhodným riešením je použitie šifrovaného disku, ako napr. softvérové nástroje TrueCrypt a BitLocker.

5.7.3. Zálohovanie

- Všetky dôležité dáta je potrebné si zálohovať mimo počítača pravidelne v šifrovanej podobe. Odporúčaný interval zálohovania je jeden mesiac pri menej dôležitých dátach, týždeň pri dôležitých dátach a každý deň pri veľmi dôležitých a kritických dátach.
- 2. Zálohované dáta je potrebné pravidelne kontrolovať, či záloha prebehla v poriadku. Odporúčaný interval kontroly záloh je jeden mesiac.

5.8. Používanie Internetu

- Svoje heslá a prihlasovacie údaje nikdy nikam neposielajte e-mailom, chatom, ani iným spôsobom. V prípade, že prišla požiadavka aj zo zdanlivo dôveryhodného zdroja je potrebné túto požiadavku odmietnuť a nahlásiť ju zodpovedajúcim miestam ako bezpečnostný incident. Platí to zvlášť pre dôležité účty ako sú Internet Banking alebo účet do pracovnej stanice.
- 2. Pri prístupe na zabezpečené stránky prostredníctvom protokolu https je potrebné vždy overiť certifikát.
- 3. Pred registráciou na stránku je potrebné si dôkladne prečítať podmienky používania.
- 4. Pri odchode zo stránky je vždy potrebné odhlásiť sa z danej stránky.
- 5. Je vysoko odporúčané nešíriť reťazové e-maily a neoverené varovania prostredníctvom e-mailu.
- 6. Je vysoko odporúčaná opatrnosť na stránkach, ktoré ohlasujú výhry. Je veľká pravdepodobnosť, že tu existuje snaha o podvod.
- 7. Nikde na Internete by sa nemalo zadávať číslo platobnej karty, ani ďalšie údaje obsiahnuté na tejto karte, okrem prípadov, keď ňou chce používateľ platiť. Aj v tomto prípade je ale potrebná opatrnosť a využívanie služieb iba dôveryhodných elektronických obchodov.
- Je vysoko odporúčané zvýšiť opatrnosť pri používaní neznámych anti-malwarových aplikácií.
 Môže sa jednať o falošný anti-malwarový program s cieľom napadnúť Vaše zariadenie.
- 9. Po ukončení práce s prehliadačom je vhodné vymazať históriu, uložené dočasné súbory a *cookies*.