EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE
it akadémia

Modul 12: Bezpečnosť pri využívaní IKT

Škodlivý softvér (malware)

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
www.itakademia.sk
ITMS2014+: 312011F057

2 Škodlivý softvér (malware)

2.1 Typy a metodiky

2.1.1 Čo je škodlivý softvér (malware), rôzne spôsoby skrývania sa škodlivého softvéru (trójsky kôň, rootkit, backdoor)

Malware (z anglického malicious software - škodlivý softvér) je všeobecné označenie pre škodlivý softvéru akéhokoľvek typu, ktoré väčšinou bežia na počítači bez vedomia (a súhlasu) majiteľa počítača. Patria sem napr. vírusy, červy, trójske kone, spyware, adware, ransomware, keylogger, backdoor, rootkit, dialer, spammer. Majú rôzne funkcie, spôsoby šírenia a skrývania sa - malware využíva rôzne spôsoby maskovania aby nebol predčasne odhalený a mohol vykonať svoju úlohu.

Trójsky kôň je škodlivý softvér, ktorý sa maskuje za užitočný. Nerozmnožuje sa. Väčšinou si ho používateľ stiahne alebo nainštaluje dobrovoľne ako užitočný program. Počas jeho používania program okrem užitočných vecí začne vykonávať aj iné, škodlivé činnosti.

Rootkit je sada aplikácií, ktoré maskujú prítomnosť malwaru v počítači. Rootkit upravuje operačný systém (skrýva adresáre, API volania, procesy, sieťové spojenia alebo systémové služby) tak, aby prítomnosť malwaru nebolo možné odhaliť bežnými prostriedkami.

Backdoor (z angličtiny zadné vrátka) je v informatike názov metódy, ktorá umožňuje obísť štandardnú autentifikáciu, ktorá bráni používateľovi neoprávnene využívať počítačový systém. Backdoor je väčšinou zámerne implementovaná funkcia programátorom systému. Môže byť využívaný na legitímnu činnosť (napr. pre servisný účel), ale veľmi často býva zneužitý útočníkmi (a malwarom) na vykonávanie činností, na ktoré nemajú v systéme oprávnenie.

2.1.2 Nákazlivý malware (vírusy, červy)

Vírus je časť kódu, ktorý nefunguje samostatne, ale pripája sa k iným programom a rozmnožuje sa do ďalších programov. Patria tu aj škodlivé makrá v dokumentoch.

Červ je samostatný program, ktorý sa rozširuje rôznymi komunikačnými kanálmi (napr. cez backdoor alebo cez e-maily) do ďalších počítačov.

2.1.3 Formy odcudzenia údajov, typy škodlivého softvéru zameraného na dosiahnutie priameho zisku (adware, ransomware, spyware, botnet, keylogger, dialler)

Adware (z anglického advertising-supported software – reklamou podporovaný softvér) program, ktorý zobrazuje nevyžiadanú reklamu. Väčšinou nie sú priamo nebezpečné, bývajú súčasťou nejakej bezplatne použiteľnej aplikácie a prinášajú takto autorovi aplikácie zisk.

Ransomware (z anglického ransom software – softvér na výkupné) zneprístupní informácie na napadnutom počítači (často ich zašifrovaním) a od používateľa požaduje zaplatenie výkupného za opätovné sprístupnenie (dešifrovanie) informácií.

Spyware z anglického spy software - špionážny softvér) kradne a odosiela rôzne (aj citlivé) informácie z napadnutého počítača útočníkovi.

Botnet (z anglického robots network – sieť robotov) je sieť počítačov infikovaných malwarom, ktorý je riadený z nejakého centra. Takto infikovaný počítač bez vedomia používateľa vykonáva rôzne koordinované činnosti, napr. rozosiela nevyžiadanú poštu alebo realizuje útok na niektoré služby s cieľom vyradiť ju s činnosti. Útočník sám nemusí využívať botnet, môže prístup k nemu predávať iným záujemcom za účelom zisku.

Keylogger (z anglického keystroke logger – zaznamenávač stlačení kláves) je špeciálny typ spyware, ktorý sleduje a ukladá (odosiela) stláčanie jednotlivých kláves - dá sa takto použiť na odchytenie hesla.

Dialer (z anglického dialer – "vytáčač") program, ktorý vytáča audiotextové číslo cez modem alebo softvér na telefonovanie, nebezpečné môžu byť nové klony na mobily.

2.2 Ochrana

2.2.1 Princípy fungovania antivírusového softvéru a jeho obmedzenia

Na ochrane počítača proti malware sa podieľajú tri základné komponenty.

Prvou je samotný operačný systém a jeho nastavenia pre používateľov, ktorý môže eliminovať väčšinu malware. Napr. ak používateľ nemá administrátorské práva, program, ktorý spustí, nemôže zapisovať do oblastí, kde je uložený operačný systém. Dôležitá je pravidelná aktualizácia operačného systému (a aplikačného softvéru), ktorou sa odstraňujú priebežne objavované bezpečnostné diery.

Druhou je samotný používateľ, ktorý by sa mal správať obozretne a neotvárať súbory a nespúšťať programy z pochybných zdrojov.

Treťou je antivírusový softvér, ktorý má úlohu odhaliť a zneškodniť malware, ktorý neeliminoval operačný systém a omylom alebo úmyselne ho aktivoval používateľ. Treba si uvedomiť, že antivírus už z princípu nemôže byť dokonalý a je to len doplnkom k prvým dvom spomenutým komponentom ochrany počítača. Antivírus pre odhaľovanie malwaru využíva niekoľko spôsobov:

- rezidentná ochrana súborového systému (kontroluje súbory pri spúšťaní, otváraní, ukladaní),
- ochrana prístupu na web (kontroluje obsah údajov preberaných z webu, najmä aktívne prvky ako skripty a pod.),
- ochrana elektronickej pošty (kontroluje obsah správ, najmä príloh, prijímanej aj odosielanej pošty),

- kontrola vymeniteľných médií (optické nosiče, USB kľúče, pamäťové karty a pod.),
- kontrola na vyžiadanie.

Antivírusový softvér využíva v princípe dve techniky na detekciu škodlivého softvéru:

- rozpoznávanie vzoriek známeho malware, ktoré má uložené vo vírusovej databáze,
- rozpoznávanie podozrivých aktivít v systéme, na ktoré používa rôzne heuristické metódy a je účinné aj proti neznámemu malware, ale môže spôsobiť falošné poplachy.

2.2.2 Nutnosť inštalácie antivírusového softvéru na počítači a zariadeniach

Antivírusový program nedokáže zo zle nastaveného alebo deravého operačného systému vytvoriť bezpečný systém - je to však užitočný doplnkový komponent ochrany, obzvlášť ak hovoríme o bežných používateľoch počítača.

Treba mať totiž na zreteli, že pri práci s počítačom sťahujeme a spúšťame programy aj bez toho, že by sme si to priamo uvedomili (napríklad v podobe makier kancelárskeho balíka, skriptov webových stránok a podobne). Nie vždy máme tiež možnosť overiť integritu a zdroj týchto programov a preto je vhodné mať antivírusový program nainštalovaný, spustený a aktualizovaný.

Aktualizovaná vírusová databáza je u antivírusového programu kľúčový prvok, pretože antivírus bez aktualizácií stráca na efektívnosti detekcie malwaru.

2.2.3 Dôležitosť pravidelnej aktualizácie softvéru (antivírusový program, webový prehliadač, zásuvné moduly, štandardné aplikácie, operačný systém)

Je samozrejmé, že často softvér obsahuje chyby. Neplatí to o všetkých chybách, ale množstvo z týchto chýb je možné zneužiť pre nejaký typ útoku alebo prieniku do počítačového systému (jedná sa o tzv. bezpečnostné chyby). Jedným zo základných kameňov počítačovej bezpečnosti sú aktualizácie softvéru, ktorými sa k používateľom dostávajú opravy známych chýb - a to nielen bezpečnostných (opravy bezpečnostných chýb sa dostávajú k používateľom spravidla s vyššou prioritou a nazývame ich bezpečnostné záplaty/opravy/aktualizácie).

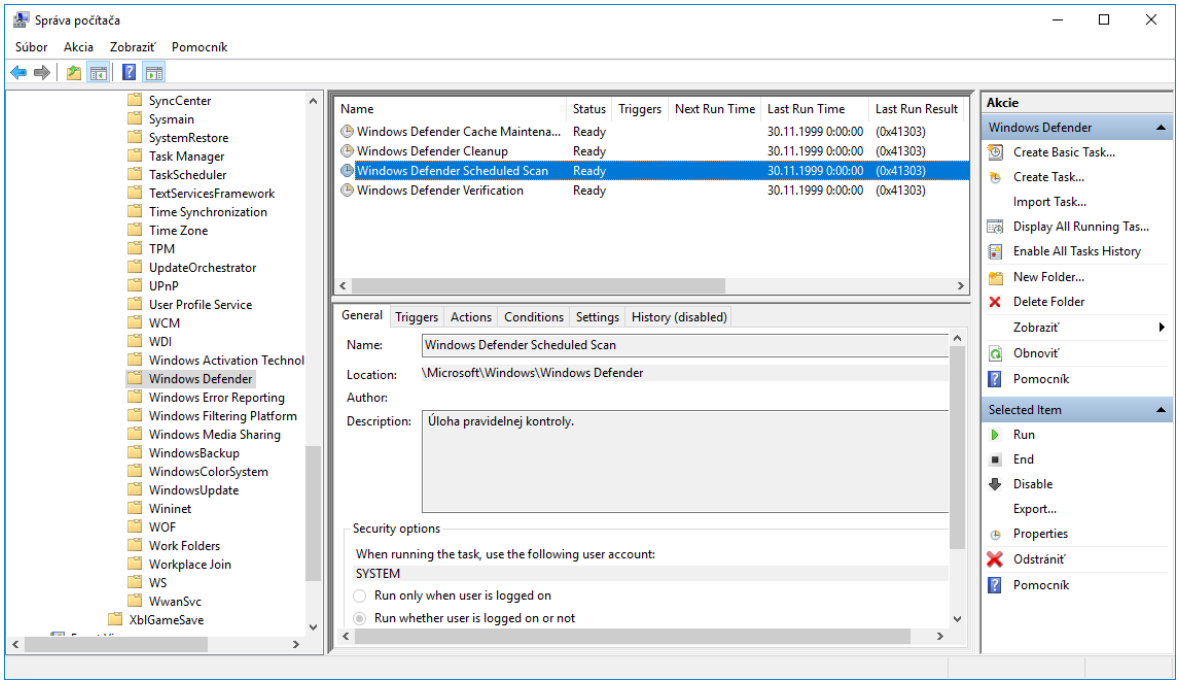
Aj keď nemožno pochybovať o tom, že všetky bezpečnostné opravy sú dôležité, aktualizácie niektorého softwaru v počítači je ešte kritickejšie. Jedná sa hlavne o aktualizácie operačného systému, webového prehliadača a antivírusového programu.

2.2.4 Kontrola konkrétnej pamäťovej jednotky, priečinka alebo súboru pomocou antivírusového softvéru. Naplánovanie kontroly s využitím antivírusového programu

Kedykoľvek si môžeme skontrolovať konkrétny súbor, priečinok, alebo pamäťovú jednotku pomocou antivírusového softvéru priamo cez program Prieskumník. Klikneme

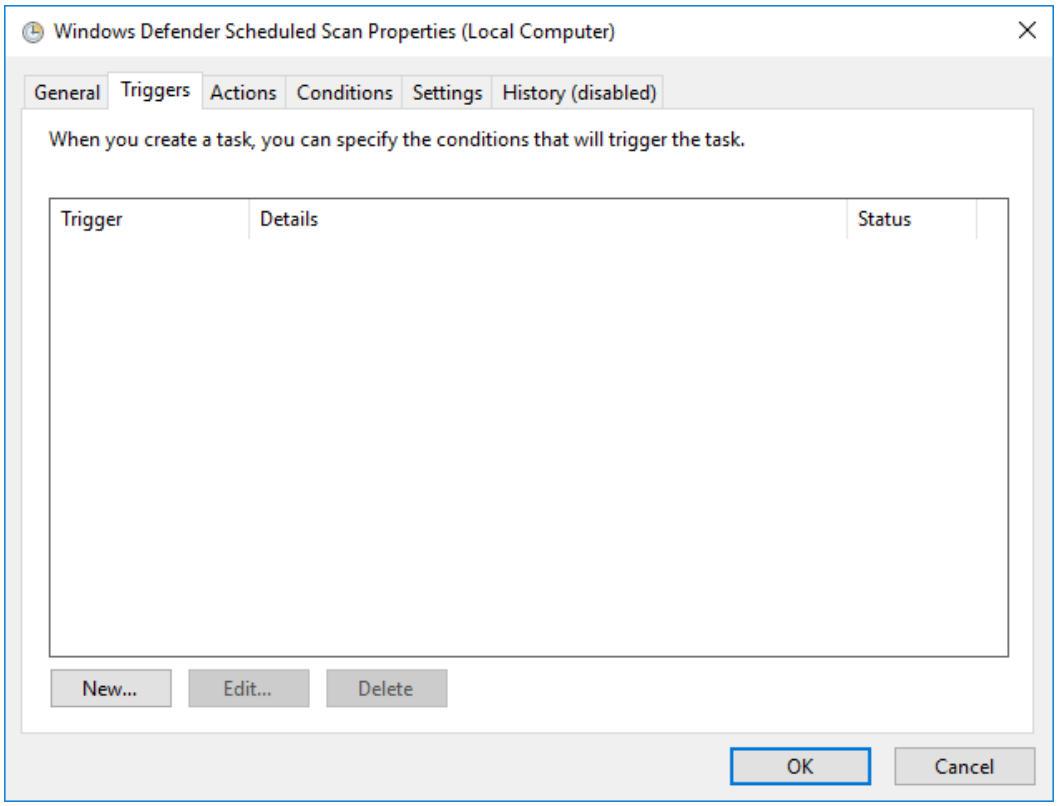
na požadovaný objekt pravým tlačidlom myšky a z ponuky si vyberieme možnosť "Skontrolovať aplikáciou Windows Defender".

Aby sme sa nemuseli starať o pravidelnú kontrolu súborov, môžeme si nastaviť ich kontrolu do tzv. plánovača. Program Windows Defender nemá vlastný plánovač, ale využíva integrovaný plánovač operačného systému (Task Scheduler). V tomto nástroji si v ľavom menu kliknutím otvoríme položku "Task Scheduler Library" a v stromovej štruktúre nájdeme položku "Microsoft/Windows/Windows Defender". Hore v strede máme zoznam úloh - vyberieme Windows Defender Scheduled Scan" (Obrázok 1) a v pravom menu v časti "Selected item" klikneme na tlačidlo "Properties".



Obrázok 1: Nastavenie pravidelnej kontroly súborov pomocou integrovaného plánovača operačného systému (Task Scheduler)

V otvorenom dialógovom okne vyberieme záložku "Triggers" (Obrázok 2). Po kliknutí na tlačidlo "New" je možné pridať rôzne typy "spúšťačov" naplánovaného skenovania. Takýchto spúšťačov môže byť nastavených viacero.



Obrázok 2: Okno pridania spúšťačov naplánovaného skenovania

2.2.5 Riziko pri využívaní zastaraného a nepodporovaného softvéru (zvýšené ohrozenie škodlivým softvérom, nekompatibilita)

Každý softvér má nejakého autora - človeka (alebo tím ľudí, spoločnosť), ktorý daný program naprogramoval, vyvinul. Pri vyvíjaní softvéru vždy dochádza k chybám. Aj keď je dobrým zvykom pri programovaní softvér dôsledne testovať, nie všetky chyby sa vychytajú hneď a k používateľom sa vždy dostane softvér s chybami. Časom sa tieto chyby odhaľujú (nielen autormi softvéru) a v prípade, že sa jedná o bezpečnostnú chybu, skôr či neskôr sa začne táto chyba zneužívať k útokom na daný počítačový systém. Preto je dôležité čo najskôr obdŕžať bezpečnostné záplaty novo objavených chýb.

Aby bol vývoj a používanie softvéru prehľadné, postupne takto vznikajú stále nové a nové verzie konkrétnych programov. Vývoj softvéru je však veľmi komplikovaná vec. V praxi často totiž nastáva situácia, kedy sa nová verzia programu natoľko zmení od predchádzajúcej, že v prípade objavenia chyby, ktorá sa vyskytuje v oboch verziách je natoľko nákladné ju včleniť do staršej verzie programu, že sa autor rozhodne aktualizovať iba novšiu verziu programu - a staršiu takto prestať podporovať. Znamená to, že používatelia sú nútení používať novšiu verziu programu, čo však nemusí byť vždy žiaduce (nová verzia sa napríklad funkčne líši od staršej a je tak pre dotyčného používateľa nepoužiteľná). Preto sa autori snažia podporovať aj staršie verzie softvéru (napríklad operačných systémov) aj nejakú dobu po vydaní novších verzií - prakticky a finančne to však po istom čase prestane byť rentabilné a preto každá verzia softvéru má iba obmedzenú dĺžku podpory. Používanie takej verzie softvéru po uplynutí tejto

doby sa potom stane bezpečnostným rizikom, pretože softvér obsahuje známe bezpečnostné chyby, ktoré sa neopravujú.

Doteraz sme sa na aktualizáciu softvéru pozerali z pohľadu bezpečnosti. Používanie neaktualizovaného a nepodporovaného softvéru má však aj ďalšie negatívum - a tým je kompatibilita. Problém napríklad nepodporovaných verzií operačných systémov je aj to, že ich nie je možné používať na novšom hardvéri, nakoľko aj tento podlieha vývoju a operačný systém sa priebežne musí tomuto vývoju tiež prispôsobovať, meniť (čo sa zo starším systémom už nedeje). Z pohľadu používateľských aplikácií zase staršie verzie programov nemusia korektne bežať na novších verziách operačných systémov alebo kooperovať s novšími verziami a podobne.

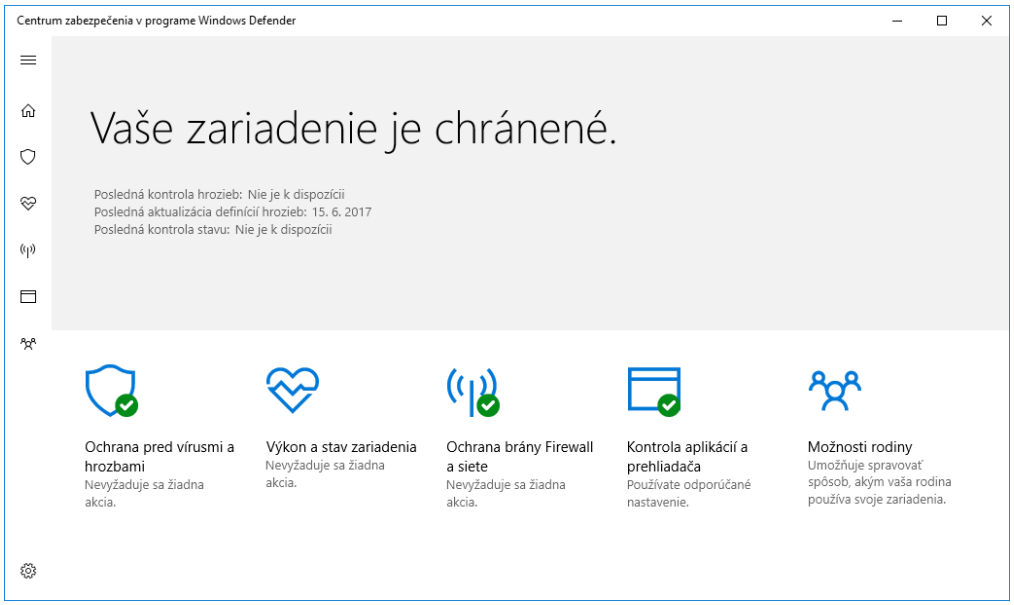
2.3 Vyriešenie a odstránenie

2.3.1 Karanténa a účinok umiestnenia infikovaných alebo podozrivých súborov do karantény

Karanténa je miesto (špeciálny priečinok), kam antivírusový softvér presúva súbory, ktoré detegoval ako nežiaduce. Používateľ má možnosť sa definitívne rozhodnúť či súbory z karantény vymaže alebo obnoví, pričom obnoviť má len súbory, pri ktorých si je istý, že ide o falošný poplach. Ďalšou možnosťou je ponechať si v karanténe súbory, ktoré boli označené len za podozrivé, a po nejakom čase ich skontrolovať znovu. Zaktualizovaný antivírusový softvér a vírusová databáza môžu potvrdiť alebo vyvrátiť podozrenie na infekciu a tým ovplyvniť rozhodovanie o obnove súboru.

2.3.2 Umiestnenie do karantény, vymazanie infikovaných/podozrivých súborov

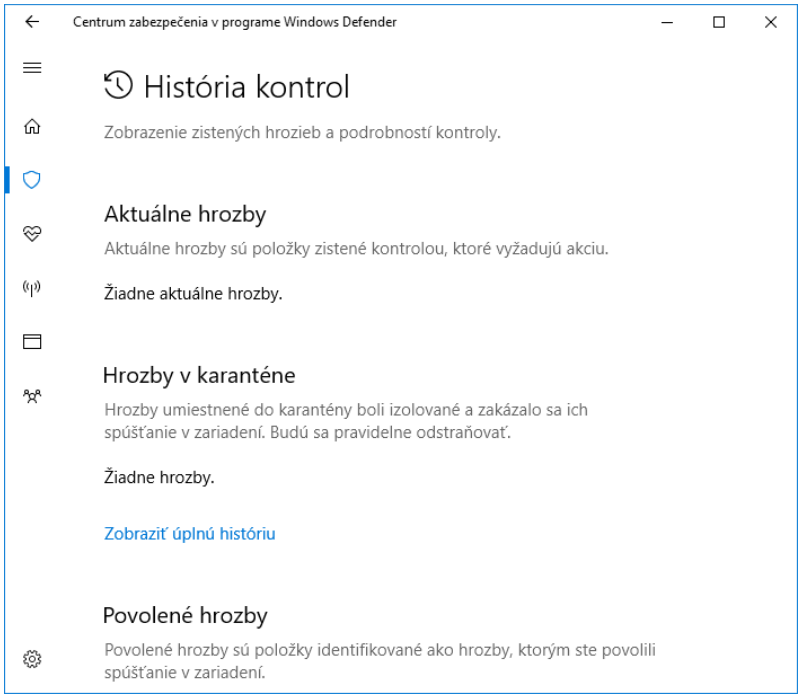
Ak antivírusový systém pri kontrole deteguje nejaký súbor ako podozrivý, presunie ho do tzv. karantény, kde je daný súbor svojim spôsobom izolovaný od zvyšku systému. Ak sa niečo podobné stane, je možné tento z karantény úplne vymazať alebo ho obnoviť (ak sme si istý, že daný súbor určite neobsahuje škodlivý software).



Obrázok 3: Centrum zabezpečenia v programe Windows Defender

Spustíme rozhranie antivírusového softvéru ("Centrum zabezpečenia v programe Windows Defender" (Obrázok 3).

V ľavom menu klikneme na tlačidlo "Ochrana pred vírusmi a hrozbami" a potom na "História kontrol". V časti "Hrozby v karanténe" je možné manažovať jednotlivé hrozby uložené v karanténe (Obrázok 4).



Obrázok 4: História kontrol programu Windows Defender

2.3.3 Diagnostika útokov škodlivým softvérom a ich riešenie pomocou využitia informácií z online zdrojov (webové stránky operačného systému, antivírusového programu, webového prehliadača a webové sídla zodpovedajúcich autorít)

Na webových sídlach použitého operačného systému, antivírusového programu a webového prehliadača je možné dohľadať informácie o možných útokoch a zraniteľnostiach a riešeniach týchto zraniteľností (resp. následkov útokov). V prípade útoku (prevencie) je možné tieto informácie sledovať a robiť individuálne opatrenia pre zvýšenie bezpečnosti.

Informácie o škodlivom softvéri sa nachádzajú aj na webových stránkach tvorcov antivírusových programov. Na špecifických miestach tvorcov webových prehliadačov môžeme nájsť aj informácie o počítačovej bezpečnosti či kriminalite (https://www.google.com/intl/sk_sk/safetycenter/resources/).

Zdrojmi informácií môžu byť aj stránky jednotlivcov (https://www.viry.cz/), pri ktorých si je potrebné uvedomiť, že nemusí ísť vždy o relevantné údaje.