STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Antivírus**

Spôsob fungovania a hrozby

**LUKÁŠ ELIAŠ**

2023/24

Obsah

Obsah 2

Anotácia 3

1 Antivírus 4

1.1 Úloha antivírusu 4

2 Technológie na detekciu vírusu 5

2.1 Detekčné metódy založené na podpise 5

2.2 Heuristická detekcia 5

3 Aktívne zapájanie umelej inteligencie 6

3.1 Antivírusový systém novej generácie 6

3.2 Umelá inteligencia ako ochranca 6

4 Porovnanie programov 7

4.1 Norton 7

4.2 Avast 7

5 Antivírus vo firemnom prostredí 8

5.1 Centralizovaná správa 8

5.2 Automatické aktualizácie a skenovanie 8

5.3 Segmentácia siete a prístupové politiky 8

5.4 Vzdelávanie zamestnancov 8

5.5 Záloha a obnova údajov 8

6 Kaapitola6 9

7 Kapitola 7 10

8 Kapitola8 11

9 Kapitola9 12

10 Kapitola10 13

11 Ilustrácie, tabuľky, rovnice 14

11.1 Ilustrácie 14

11.2 Tabuľky 14

11.3 Zdrojový kód programu 15

11.4 Rovnice, vzorce 15

12 Záver 16

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla) 17

Prílohy (štýl Nadpis Kapitoly, bez čísla) 18

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla) 18

Príloha B – <názov prílohy> 18

Príloha C – <názov prílohy> 18

Anotácia

**Annotation**

1. Antivírus

Antivírusový softvér, skrátene označovaný ako antivirus, je program navrhnutý na detekciu, prevenciu a odstránenie škodlivého softvéru z počítača, ako sú vírusy, červy, trojanské kone, špionážne programy a iné druhy malware. Jeho hlavným účelom je ochrana užívateľov počítačov pred stratou údajov, poškodením systému alebo zneužitím osobných informácií. Antivírus hrá kľúčovú úlohu v boji proti škodlivému softvéru a ochrane počítačových systémov. Jeho základnou funkcií je monitorovanie aktivít na počítači a detekcia prítomnosti potenciálne škodlivého kódu, ako sú vírusy, červy, trojanské kone a ďalšie formy malware. Keď antivírusový program identifikuje nebezpečný kód, okamžite reaguje a vykonáva kroky na jeho neutralizáciu.

* 1. Úloha antivírusu

Jednou z hlavných úloh antivírusového softvéru je prevencia infikácie systému. To znamená, že sa snaží zabrániť vstupu škodlivého kódu do počítača alebo jeho šíreniu v systéme. Tento cieľ sa dosahuje pomocou rôznych techník, ako sú skenovanie súborov a priečinkov, monitorovanie internetového prehliadania, kontrolovania príchodu a odchodu dát cez sieť, a iných bezpečnostných opatrení. Okrem prevencie sa antivírusový softvér tiež zaoberá liečbou infikovaných systémov. Ak sa počítač napriek opatreniam infikuje, antivírusový program sa snaží identifikovať, izolovať a odstrániť škodlivý kód a minimalizovať tak škody spôsobené infekciou. Tento proces zahŕňa čistenie infikovaných súborov, opravy poškodených systémových súborov a zabezpečenie, že sa infekcia nešíri ďalej. Celkovo možno povedať, že antivírusový softvér je nepostrádateľným nástrojom v ochrane počítačov a sietí pred škodlivým softvérom. Jeho schopnosť monitorovať, detegovať a neutralizovať hrozby je kľúčová pre udržanie bezpečnosti a integrity digitálnych prostredí. Bez neho by boli počítače a zariadenia vystavené vysokému riziku infikácie a možným závažným následkom.

1. Technológie na detekciu vírusu

Neustály vývoj malvéru viedol antivírusové programy k vývoju čoraz sofistikovanejších metód detekcie, ktoré sú nevyhnutné na efektívnu detekciu, analýzu a elimináciu akejkoľvek kybernetickej hrozby. V tomto článku podrobne analyzujeme rôzne metódy detekcie škodlivého softvéru používané v antivírusových programoch a poskytneme technický a neutrálny pohľad na tento kľúčový aspekt počítačovej bezpečnosti.

* 1. Detekčné metódy založené na podpise

Sú to techniky používané v kybernetickej bezpečnosti na identifikáciu známych počítačových hrozieb. Tieto metódy sú založené na porovnaní digitálnych podpisov škodlivých súborov s databázou známych podpisov. Digitálny podpis je jedinečný vzor, ​​ktorý identifikuje konkrétny malvér alebo vírus. Hlavným cieľom je identifikovať a blokovať hrozby, ktoré už boli predtým analyzované a kategorizované odborníkmi na počítačovú bezpečnosť. Na vykonanie tohto typu detekcie sa používajú algoritmy, ktoré skúmajú kód a vlastnosti daného súboru a porovnávajú ich s podpisy uložené v databáze.

* 1. Heuristická detekcia

Heuristická detekcia je preventívna metóda v technologickej oblasti, ktorá využíva algoritmy a heuristické pravidlá na včasnú identifikáciu a zastavenie potenciálnych hrozieb. Na rozdiel od tradičných metód detekcie, ktoré sa spoliehajú na známe podpisy, sa heuristická detekcia zameriava na detekciu nových variantov malvéru a podozrivého správania. To z neho robí kľúčový nástroj na ochranu pred čoraz sofistikovanejšími kybernetickými útokmi. Jednou z hlavných výhod heuristickej detekcie je jej schopnosť blokovať neznáme hrozby. Pomocou algoritmov strojového učenia, analýzy správania a sandboxingu dokáže identifikovať bežné vzory a charakteristiky škodlivého softvéru, a to dokonca ešte predtým, ako bol vyvinutý špecifický podpis. To chráni systémy pred novými hrozbami a útokmi zero-day a poskytuje ďalšiu vrstvu zabezpečenia.

1. Aktívne zapájanie umelej inteligencie

Príchod nových technológií zakaždým vyvolá nové kolo pretekov medzi kriminálnikmi pôsobiacimi v kybernetickom priestore a špecialistami v oblasti IT bezpečnosti. Aby sa firmy vyhli dôsledkom potenciálnych kybernetických útokov, už dávno nevystačia s klasickým antivírusovým softvérom. Musia budovať sofistikovanú obrannú líniu, ktorá zahŕňa komplexnú sieť moderných nástrojov, ktoré čoraz v širšej miere využívajú AI a strojové učenie. Obranná línia je tvorená vzájomne prepojenými obrannými systémami – od tradičných antimalvérových riešení až po najmodernejšie technológie, ako je antivírus novej generácie (NGAV), rozšírená detekcia a reakcia (XDR) a umelá inteligencia (AI).

* 1. Antivírusový systém novej generácie

Antivírusové systémy novej generácie (NGAV) vznikli ako reakcia na vyvíjajúce sa prostredie hrozieb s využitím kombinácie tradičných techník a pokročilých technológií, ako je strojové učenie a analýza správania. Riešenia NGAV presahujú rámec jednoduchého porovnávania signatúr a ponúkajú komplexnú ochranu pred širokou škálou kybernetických hrozieb vrátane útokov nultého dňa a sofistikovaných kampaní. Dobrý príklad je integrácia umelej inteligencie s riešeniami XDR (Extended Detection and Response). Riešenia XDR na rozšírenú detekciu a reakciu na hrozby a útoky sú ďalším vývojovým stupňom riešení na detekciu útokov na koncové zariadenia a následnú reakciu (EDR – Endpoint Detection and Response), aby firmy dokázali v reál­nom čase odhaliť sofistikované hrozby a adekvátne na ne reagovať. Riešenia XDR využívajú údaje z informačných kanálov mimo koncových zariadení.

* 1. Umelá inteligencia ako ochranca

Umelá inteligencia je veľmi účinný nástroj ochrany pred ransomvérom, ktorý zostáva jednou z najvýznamnejších hrozieb v oblasti kybernetickej bezpečnosti. Inovatívne nástroje na báze AI umožňujú predvídanie, odhaľovanie a reakciu na útoky ransomvéru skôr, ako stihnú napáchať škody. Tieto systémy analyzujú rozsiahle súbory údajov s cieľom identifikovať podprahové vzorce a anomálie, ktoré môžu uniknúť klasickému softvéru, čo umožňuje preventívne zasiahnuť proti potenciálnym ransomvérovým hrozbám. Strojové učenie umožňuje, aby sa tieto systémy postupne prispôsobili novým taktikám ransomvéru.

1. Porovnanie programov

Nezávislé testovanie [AV-Test](https://www.av-test.org/en/antivirus/home-windows/) pravidelne vyhodnocuje tie najlepšie antivírusové produkty na trhu a hodnotí ich podľa dôležitých kritérií, od ochrany zariadení cez výkon, až po použiteľnosť. V najnovšom októbrovom testovaní však opäť raz zvíťazil antivírus od Microsoftu, ktorý tak aj tento rok obhájil svoj titul a prekonal konkurenciu, informuje [MSPowerUser](https://mspoweruser.com/independent-test-finds-microsoft-defender-the-best-free-antivirus-in-october-2021/?utm_source=dlvr.it&utm_medium=facebook" \t "_blank). Microsoft vyrukoval s vlastným antivírusovým systémom pre svoj Windows ešte v roku 2007, no od tej doby sa zásadne zmenil. Ochranu systému Windows 10 a Windows 11 pritom odborníci znova vyhodnotili ako jednu z najlepších, ktorá v testoch miestami prekonala aj zvučné mená ako ESET, Avast, Kaspersky či Malwarebytes. Podobne tak [Microsoft Defender zvíťazil v rovnakom testovaní aj pred rokom](https://fontech.startitup.sk/platene-antivirusy-nie-su-zarukou-microsoft-defender-je-jeden-z-najlepsich-pre-windows-10-prekonal-ich-v-testoch/). Najnovšie si znova dokázal získať poprednú pozíciu, na ktorú sa dostal vďaka najvyššiemu hodnoteniu vo všetkých testoch. Za ochranu, výkon a použiteľnosť dostal vo všetkých kategóriách maximálny počet 6 bodov a svojimi výsledkami prekonal aj celkový priemer ochrany antivírusov voči 0-day zraniteľnostiam, ktoré odhalil so 100 % úspešnosťou.

* 1. Norton

Norton AntiVirus je [antivírusový softvér](https://sk.wikipedia.org/wiki/Antiv%C3%ADrusov%C3%BD_softv%C3%A9r) od firmy [Symantec](https://sk.wikipedia.org/w/index.php?title=Symantec&action=edit&redlink=1). Zabezpečuje a kontroluje emailové správy, chatové správy a všetky súbory automatickým odstraňovaním vírusov, červov a trójskych koňov. Funkcie novej verzie detegujú aj niektoré nevírusové hrozby ako napríklad [spyware](https://sk.wikipedia.org/wiki/Spyware). Program obsahuje funkciu skenovanie komprimovaných súborov, pred otvorením. Norton AntiVirus umožňuje automatické sťahovanie aktualizácií vírusovej databázy pomocou vlastnej služby LiveUpdate. Blokovanie červov a skriptov dokáže zabrániť infekcii systému aj takým vírusom, na ktoré ešte neboli vytvorené detekčné údaje.

* 1. Avast

Avast je [antivírusový program](https://sk.wikipedia.org/wiki/Antiv%C3%ADrusov%C3%BD_softv%C3%A9r) k dispozícii zadarmo od spoločnosti [AVAST Software](https://sk.wikipedia.org/w/index.php?title=AVAST_Software&action=edit&redlink=1), spoločnosti so sídlom v [Česku](https://sk.wikipedia.org/wiki/%C4%8Cesko), ktorý bol prvý raz uvedený na trh v roku [1988](https://sk.wikipedia.org/wiki/1988). Program je k dispozícii vo viac ako 20 jazykoch a je jedným z najpopulárnejších „[freeware](https://sk.wikipedia.org/wiki/Freeware)“ antivírusových aplikácií. Program pred rokmi vyvolal rozruch, keď hneď pri vstupe do porovnávacieho testu Virus Bulletin dokázal poraziť mnoho antivírov zvučných mien a onedlho potom ako prvý v histórii detegoval 100% vírusov vo všetkých kategóriách. Verzia avast! Free Edition je poskytovaná zadarmo. Avast! antivírus má na svete viac ako 400 miliónov používateľov.

1. Antivírus vo firemnom prostredí

Využívanie antivírusového softvéru vo firemnom prostredí si vyžaduje komplexný prístup a implementáciu najlepších postupov a stratégií. Tu je niekoľko kľúčových aspektov, na ktoré by mali firmy pri zavádzaní antivírusovej ochrany brať ohľad

* 1. Centralizovaná správa

Pre väčšie firmy je dôležité mať systém na centralizovanú správu antivírusového softvéru. Tento systém umožňuje administrátorom jednoducho spravovať a monitorovať ochranu všetkých zariadení v sieti a zabezpečiť, že sú všetky aktualizované a chránené.

* 1. Automatické aktualizácie a skenovanie

Je kľúčové mať nastavené automatické aktualizácie pre antivírusový softvér, aby sa zabezpečilo, že sú vždy na poslednej úrovni s najnovšími definíciami vírusov a ochrannými mechanizmami. Rovnako dôležité je pravidelné automatické skenovanie.

* 1. Segmentácia siete a prístupové politiky

Segmentácia siete a prísne prístupové politiky môžu pomôcť minimalizovať riziko šírenia malware v prípade infekcie jedného zariadenia. To znamená, že firmy by mali mať nastavené správne firewally a prístupové kontroly na zabránenie šírenia hrozieb naprieč svojimi sieťami.

* 1. Vzdelávanie zamestnancov

Informovaní zamestnanci sú kľúčom k úspechu antivírusovej stratégie vo firemnom prostredí. Firmy by mali zabezpečiť, aby ich zamestnanci boli oboznámení s najbežnejšími hrozbami z internetu a vedeli, ako sa im vyhnúť, ako aj kedy a ako nahlásiť podozrivé aktivity.

* 1. Záloha a obnova údajov

Napriek všetkým preventívnym opatreniam môže dôjsť k infekcii malware a strate údajov. Preto je dôležité mať zavedené pravidelné zálohy údajov a plán obnovy, aby sa minimalizovali škody v prípade úspešnej infekcie.

1. Kaapitola6
2. Kapitola 7

Využívanie antivírusového softvéru vo firemnom prostredí si vyžaduje komplexný prístup a implementáciu najlepších postupov a stratégií. Tu je niekoľko kľúčových aspektov, na ktoré by mali firmy pri zavádzaní antivírusovej ochrany brať ohľad

1. Kapitola8
2. Kapitola9
3. Kapitola10
4. Ilustrácie, tabuľky, rovnice

V práci sa môžu vyskytovať okrem slovného textu aj informácie vyjadrené v obrazovej forme a symbolmi.

* 1. Ilustrácie

**Ilustrácie** sú obrázky obsahujúce **grafy**, **diagramy**, **mapy**, **schémy** a pod. Nie je potrebné rozlišovať rozličné typy ilustrácií, stačí, ak sa všetky označia ako „Obrázok”. Všetky ilustrácie musia byť očíslované súvislým radom číslic v celej práci a musia mať titulky (názov obrázku) pri každom obrázku. Text titulku musí byť pochopiteľný aj bez kontextu. Majú sa zaradiť bezprostredne za textom, kde sa spomínajú po prvýkrát (najlepšie na tej istej strane). Obrázok by mal byť podľa možnosti centrovaný. Pri odkazovaní na daný obrázok v texte použijeme odkaz uvedený v zátvorke (napr. Obr. 1).



Obr. 1 Názov obrázka (štýl Popis, Popiska-Caption)

* 1. Tabuľky

Tabuľky prezentujú myšlienky a tvrdenia popisované v práci. Akýkoľvek tabuľkový materiál, ktorý sa skladá z viac než štyroch alebo piatich riadkov, by mal byť spracovaný do formy tabuľky. Popis a záhlavie tabuľky má byť zrozumiteľné samostatne bez odkazu na text. Záhlavia majú vyjadrovať druh veličiny a typy jednotiek vo forme „veličina/jednotka”, je potrebné používať rovnaké symboly a skratky ako v texte. Každá tabuľka musí mať poradové číslo a titulok, umiestnený zvyčajne nad tabuľkou. Tabuľka by mala mať rovnakú orientáciu, ako text práce.

Tab. 1 Názov tabuľky (štýl Popis, Popiska-Caption)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1.A | 1.B | 1.C | 1.D |
| prezentácie | 10 | 12 | 13 | 11 |
| videá | 7 | 4 | 6 | 3 |
| počítačové hry | 5 | 6 | 3 | 4 |
| blogy | 6 | 8 | 7 | 8 |
| postery | 4 | 3 | 5 | 6 |

* 1. Zdrojový kód programu

Na zápis zdrojového kódu programu použijeme štýl kód (písmo Courier New 11, zarovnanie vľavo, orámovanie s tieňom).

viem hľadajCestu

  kým [farbabodu <> "čierna] [vz 1]

  do 1 vp 90

  kým [farbabodu <> "červená] [

   vp 90 do 1

   ak farbabodu = "čierna [

    vz 1 vl 90 do 1

    ak farbabodu = "čierna [vz 1 vl 90]

   ]

   čakaj 1

  ]

koniec

* 1. Rovnice, vzorce

Rovnice sa uvádzajú v strede riadka, vysvetlivky symbolov na začiatku riadku. Vysvetlivky symbolov sa uvádzajú od začiatku riadka. Ak je v práci viac vzorcov, uvádzame číslo vzorca do okrúhlych zátvoriek bez medzier umiestnených na pravom konci riadka. Pre písanie fyzikálnych veličín a matematických premenných sa používa kurzíva. Používame sústavu jednotiek SI (ISO 31 a ISO 1001). Pri písaní rovníc používame **editor rovníc (musíme ho mať nainštalovaný)**.

1. Záver

Záver obsahuje vecné závery, sumarizáciu, vlastný prínos alebo pohľad autora, odporúčania pre prax (výučbu). Záver je uvedený na maximálne 1 stranu.

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla)

Všetky dokumenty, ktoré v práci použijete, je potrebné zoradiť do zoznamu pozostávajúceho z  bibliografických odkazov, ktorý označujeme **Zoznam použitej literatúry**. Pre tvorbu zoznamov použitej literatúry platia štandardy. Cieľom je, aby zo zoznamu použitej literatúry bolo možné jasne identifikovať použitý zdroj a aby ho bolo možné bez ťažkostí opäť vyhľadať.

Hlavným zdrojom údajov pre tvorbu bibl. odkazov je **titulný list** (tzn. prvý list v knihe, kde sú uvedené údaje o názve autorovi atď.), príp. jeho rub. Odkazy sa môžu týkať knižných, časopiseckých a iných zdrojov informácií (zborníky z konferencií, patentové dokumenty, normy, odporúčania, kvalifikačné práce, osobná korešpondencia a rukopisy, odkazy cez sprostredkujúci zdroj, elektronické publikácie), ktoré boli v práci použité.

**Technika citovania** určuje spôsob, akým označujeme citácie v dokumente, pričom podľa normy (pozri STN ISO 690) existuje viacero spôsobov citovania. Pri metóde **číselných citácií** sa v zozname bibliografických odkazov každé citované dielo uvádza v tom poradí, v akom bolo uvedené a číslované v texte. Číslované odkazy v texte sú uvedené v zátvorkách [3] a odkazujú na dokumenty v takom poradí, v akom sa citujú po prvýkrát. Nasledujúce citácie dostávajú také isté číslo, ako má prvá citácia. Ak sa citujú osobitné časti dokumentu, môžu sa za číslom citácie uviesť čísla strán.

**Príklad zoznamu použitej literatúry:**

1. KALAŠ, Ivan – BLAHO, Andrej: *Tvorivá informatika. 1. zošit z programovania.* Bratislava: SPN - Mladé letá, 2007. 48. s. ISBN 80-10-01723-2
2. CIMBALA, Roman – BALOGH, Jozef – DŽMURA, Jaroslav: Diagnostika výkonových transformátorov s využitím prvkov umelej inteligencie 1. In: *Elektrotechnický magazín ETM*. roč. 14, č. 1 (2004), s. 8-9.
3. Kolektív autorov: *Štátny vzdelávací program*. [online] Bratislava: ŠPU v Bratislave, 2008. Aktualizované 14.2.2010 [cit. 2010-02-17]. Dostupné na internete: <http://new.statpedu.sk/sk/filemanager/download/987>
4. Elektronické diplomové a dizertačné práce SR: ETD SK. [online]. Košice : ETD SK, 2004. Aktualizované 14-2-2005 [cit 2005-03-10]. Dostupné na internete: <http://www.etd.sk/>.
5. KATUŠČÁK, Dušan: *Ako písať záverečné a kvalifikačné práce*. Nitra: Enigma, 2004. 162 s. il. ISBN 80-89132-10-3

Prílohy (štýl Nadpis Kapitoly, bez čísla)

Zoznam príloh záverečnej práce:

* Príloha A – CD médium
* Príloha B – <názov prílohy>
* Príloha C – <názov prílohy>

Táto časť záverečnej práce obsahuje zoznam všetkých príloh. Číslovanie strán príloh nadväzuje na číslovanie strán v hlavnom texte.

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla)

Priložené CD médium **povinne** obsahuje text záverečnej práce vo formáte PDF. CD môže obsahovať edukačný hypertext, metodické listy, dotazníky a ukážky projektov atď. CD médium zabalené do papierového obalu sa vlepí na vnútornú stranu zadnej obálky záverečnej práce.

Príloha B – <názov prílohy>

<popis prílohy>

Príloha C – <názov prílohy>

<popis prílohy>