STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Antivírus**

ročníkový projekt

**LUKÁŠ ELIAŠ**

**2.D**

2024

Obsah

Obsah 2

Anotácia 3

1 Antivírus 4

1.1 Dôvod nutnosti antivírusu 4

1.2 Úloha antivírusu 5

1.3 Vhodný antivírus 6

2 Vírus 7

2.1 Malware 7

2.2 Spyware 9

2.3 Phishing 9

3 Tvorba učebného materiálu 10

3.1 Začiatok 10

3.2 Hľadanie potrebných materiálov 10

4 Špecifikácia produktu 11

4.1 Dizajn a rozloženie 11

4.2 Fonty 11

4.3 Obrázky 12

4.3.1 Prvky prezentácie 12

5 Vnútorné spracovanie 13

5.1 Jednoduchosť 13

6 Záver 14

Zoznam použitej literatúry 15

Anotácia

Táto práca sa zameriava na význam antivírusového softvéru v kontexte kybernetickej bezpečnosti. Analyzujem úlohu antivírusového softvéru pri ochrane počítačových systémov pred rôznymi typmi malvéru, vrátane vírusov, spyware a phishingu. Práca obsahuje rozdelenie malvéru do kategórií a diskutuje o ich charakteristikách a metódach infekcie. Okrem toho sa zaoberá aj vývojom antivírusového softvéru a jeho schopnosťou prispôsobiť sa neustále sa meniacim kybernetickým hrozbám. Cieľom práce je poskytnúť ucelený prehľad o význame antivírusového sofvéru v ochrane pred kybernetickými hrozbami a jeho úlohe pri zabezpečovaní bezpečnosti používateľských systémov.

**Annotation**

This work focuses on the importance of antivirus software in the context of cyber security. I analyze the role of antivirus software in protecting computer systems from various types of malware, including viruses, spyware, and phishing. It contains the division of malware into colors and products by their characteristics and methods of infection. In addition, it is also reflected in the development of antivirus software and its ability to adapt to constantly changing cyber threats. The aim of the thesis is to provide a comprehensive overview of the importance of antivirus software in protection against cyber threats and its role in ensuring the security of user systems.

1. Antivírus

Antivírusový softvér (antivírusový program) je bezpečnostný program určený na prevenciu, detekciu, vyhľadávanie a odstraňovanie vírusov a iných typov škodlivého softvéru z počítačov, sietí a iných zariadení. Antivírusový softvér, ktorý je často súčasťou bezpečnostného balíka, je možné zakúpiť aj ako samostatnú možnosť. Antivírusový program, ktorý sa zvyčajne inštaluje do počítača ako proaktívny prístup ku kybernetickej bezpečnosti, môže pomôcť zmierniť rôzne kybernetické hrozby vrátane keyloggerov, únoscov prehliadača, trójskych koní, červov, spywaru, pokusov o phishing a útokov ransomware. Kvôli neustále sa vyvíjajúcom prostredí pre počítačovú kriminalitu a denne vydávaným novým verziám malvéru vrátane zero-day útokov nemôže žiadny antivírusový program ponúknuť detekciu a ochranu pred všetkými druhmi hrozieb. [1] 

Obr. 1 Antivírus[]

* 1. Dôvod nutnosti antivírusu

Informácie majú v dnešnom svete obrovskú hodnotu. To si uvedomujú aj útočníci a zneužívajú preto mnohé technické aj psychologické nástroje, aby sa k nim dostali a mohli ich výhodne predať, prípadne využiť na vlastné obohatenie. Mnohí používatelia si myslia, že nemajú žiadne cenné informácie, no opak je často pravdou. Infikované zariadenie používateľa navyše môže byť cenným zdrojom alebo prostredníkom na ďalšie šírenie škodlivého kódu. Technickejšie zdatnejší útočníci, ktorých cieľom je zarobiť na obeti alebo jej dátach, píšu vlastný škodlivý kód a neustále sa ho snažia vylepšovať.[2]

* 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. Antivírusový softvér zvyčajne beží ako proces na pozadí, skenuje počítače, servery alebo mobilné zariadenia, aby zistil a obmedzil šírenie malvéru. Mnohé antivírusové softvérové ​​programy zahŕňajú detekciu a ochranu hrozieb v reálnom čase na ochranu pred potenciálnymi zraniteľnosťami a vykonávajú kontroly systému, ktoré monitorujú zariadenia a systémové súbory a hľadajú možné riziká. Stará sa o skenovanie adresárov alebo konkrétnych súborov proti knižnici známych zlomyseľných podpisov na detekciu neobvyklých vzorov, ktoré naznačujú prítomnosť nebezbečného softvéru. Povoľuje používateľom plánovať skenovania malvéru tak, aby sa spúšťali automaticky a umožňuje používateľom spustiť nové skenovania kedykoľvek. Odstráni akýkoľvek nebezpečný softvér pre počítač, ktorý odhalí, buď automaticky na pozadí, alebo upozorní používateľov na infekcie a vyzve ich, aby súbory vyčistili. Na komplexné skenovanie systémov musí mať antivírusový softvér vo všeobecnosti privilegovaný prístup k celému systému. To robí samotný antivírusový softvér bežným cieľom útočníkov a výskumníci v posledných rokoch objavili vzdialené spustenie kódu a ďalšie vážne zraniteľnosti v antivírusových softvérových produktoch. [1]

Graf 1 Graf závislosti od roku a percentuálnych útokov na organizácie a firmy []

* 1. Vhodný antivírus

Dobrou praxou pri výbere antivírusu je sledovanie jeho výsledkov v nezávislých testoch. Príkladom organizácií, ktoré robia podobné testy, AV Comparatives alebo AV-Test. V ich testoch si používateľ môže pozrieť rôzne vlastnosti bezpečnostného softvéru – napríklad akú záťaž pre zariadenie daný antivírus predstavuje, aké percento škodlivých kódov dokáže zachytiť a zablokovať či koľko falošných poplachov pri svojej činnosti vyvolá. Kľúčovým pri výbere by mal byť aj fakt, že daný bezpečnostný softvér používa mix viacerých technológií, ktoré dokážu používateľa chrániť na viacerých úrovniach. Antivírusy, ktoré majú jednu dominantnú technológiu alebo sa zameriavajú len na jeden typ detekcie, môžu útočníci ľahšie obísť. Môžeme to prirovnať k bezpečnostným prvkom auta. Vozidlo, ktoré má asistenčné systémy, dokáže vyrovnať šmyk, má bezpečnostné pásy a množstvo airbagov, je určite bezpečnejšie ako starší model, ktorý chráni posádku len jedným z týchto prvkov. Dôležité je tiež sledovať, či bezpečnostný softvér, ktorý si používateľ vybral, požiada o súhlas so spracovaním dát. [2]

* 1. Nieco este

1. Vírus

Počítačový vírus je škodlivý softvérový program, ktorý sa navrhol s cieľom infikovať počítače a šíriť sa bez vedomia a súhlasu používateľa. Podobne ako biologický vírus, počítačový vírus sa môže replikovať a šíriť z jedného systému na ďalší. Jeho účelom môže byť spôsobiť škodu, zhromažďovať citlivé informácie alebo narúšať normálne fungovanie počítača.[3]

|  |  |
| --- | --- |
|  | Percentuálne napadnuté firmy a organizácie |
| 2018 | 55.10 |
| 2019 | 56.10 |
| 2020 | 62.40 |
| 2021 | 68.50 |
| 2022 | 71 |
| 2023 | 72.70 |

Tab. 1 Tabuľka zobrazujúca percentuálne napadnuté firmy ransomwarom[]

* 1. Malware

Malware je zlomyseľný kód či softvér, ktorý obyčajne poškodí alebo zablokuje, zmocní sa alebo odcudzí informácie z počítačového systému. Malvér zahŕňa všetky druhy škodlivého softvéru vrátane najznámejších foriem, ako sú trójske kone, ransomware, vírusy, červy a bankový malvér. Spoločným menovateľom všetkého, čo spadá pod termín malvér, je nekalý úmysel jeho autorov alebo prevádzkovateľov. [4]



Obr. 2 Malware, Phishing a nástrahy na internete[]

* 1. Spyware

Spyware je počítačový program, ktorý sa bez vedomia používateľa pokúša „vyšpehovať“ citlivé dáta z počítača (napr. heslá). Tieto dáta sa potom pokúša poslať tretej strane. Spyware je ťažko odhaliteľný. Inštaluje sa na pozadí a v systéme sa chová veľmi nenápadne. Skrýva svoju činnosť za dôveryhodne vyzerajúce procesy. Užívateľ ho môže odhaliť, až keď sa spyware aktivuje a začne vykonávať podozrivú činnosť. Užívateľ zaznamená spomalenie internetu, všimne si podozrivú prevádzku v sieti alebo odhalí podozrivý softvér v zozname bežiacich procesov. [5]

* 1. Phishing

Phishing je pokus o podvodné získanie citlivých informácií, ako sú heslá a podrobnosti o kreditných kartách, maskovaním sa za dôveryhodnú osobu alebo dôveryhodný obchod (alebo banku)[6] pri elektronickej komunikácii. Existuje viacero spôsobov „lovenia hesiel“. Najčastejšie phishing prebieha tak, že podvodník (útočník) sa pomocou podvodného ([klamlivého](https://sk.wikipedia.org/wiki/Klam)) [e-mailu](https://sk.wikipedia.org/wiki/E-mail) snaží nasmerovať používateľa na [webstránku](https://sk.wikipedia.org/wiki/Webstr%C3%A1nka) alebo všeobecnejšie [URL adresu](https://sk.wikipedia.org/wiki/Jednotn%C3%BD_vyh%C4%BEad%C3%A1va%C4%8D_prostriedku), ktorú pripravil práve na tento podvodný účel.[7] 

Obr. 3 Spyware []

1. Tvorba učebného materiálu

Úvod do mojej prezentácie o antivírusovom softvéri je vchodová brána do sveta kybernetickej bezpečnosti. Snažil som sa vytvoriť atmosféru zvýrazňujúcu dôležitosť ochrany našich digitálnych prostriedkov, ktorá sa stáva nevyhnutnosťou v dnešnej digitálnej ére. Antivírusový softvér, ktorý budem predstavovať, je viac než len obyčajný program - je to štít, ktorý bráni naše dáta, súkromie a identitu pred rôznymi kybernetickými hrozbami. Cieľom mojej prezentácie je priblížiť divákom základné pojmy a princípy, ktoré sú spojené s antivírusovým softvérom, a ukázať, ako môže táto technológia pomôcť chrániť nás a naše digitálne zariadenia. Chcem, aby diváci odchádzali s jasným pochopením toho, ako môžu chrániť seba a svoje digitálne životy pred kybernetickými hrozbami, a aby sa cítili povzbudení k aktívnej ochrane svojich dát a zariadení.

* 1. Začiatok

Začiatky tvorby prezentácie sú ako prvý krok na dlhej ceste od myšlienky k hotovému výsledku. Vymyslenie vhodnej témy je rozhodujúcim momentom, ktorý určuje smer a zameranie celej prezentácie. Téma je veľmi zaujímavá, produkt bol robený rovnako pútavo aby čitateľa nielen zaujal ale dokonca aj presvedčil a vstúpil do jeho mysle, aby sa nad danou problematikou zamyslel. Týmto chcem dosiahnuť aj to aby si čo najviac ako sa dá zabezpečil svoju elektroniku, či je to počítač, notebook alebo mobilný telefón a neveril všetkému na internete, takisto sa nedal nachytať osobám páchajúcim zločiny cez internet.

* 1. Hľadanie potrebných materiálov

Moja príprava na prezentáciu o antivírusovom softvéri bola veľmi dôkladná. Začal som s literatúrou a online zdrojmi, kde som sa hlbšie ponoril do tém ako kybernetické bezpečnostné hrozby, fungovanie antivírusového softvéru a trendy v oblasti ochrany pred malwarom a phishingom. Skúmal som rôzne zdroje, aby som získal široký pohľad na tému, a snažil som sa overiť autenticitu informácií. Bolo to veľmi náročné pretože som sa stretol s duplikátmi ktoré každý uvádzali inú skutočnosť. Analyzoval som prípadové štúdie a reálne príklady, čo mi pomohlo lepšie pochopiť úlohu antivírusového softvéru. Príprava mi dáva dobrý základ pre úspešnú prezentáciu, ktorá bude dúfam zaujímavá pre čitateľov.

1. Špecifikácia produktu

Táto kapitola je zameraná na dizajn a rozloženie prezentácie o antivírusovom softvéri a kybernetickej bezpečnosti. Dizajn a rozloženie sú kľúčovými prvky, ktoré ovplyvňujú úspech prezentácie a schopnosť publiku efektívne absorbovať informácie. Budeme skúmať spôsoby, ako správne využiť obrázky, grafiku, text a ďalšie prvky, aby sme vytvorili prezentáciu, ktorá bude nielen atraktívna vizuálne, ale aj informatívna a ľahko pochopiteľná pre naše publikum. Pri navrhovaní dizajnu a rozloženia sme sa snažili dosiahnuť rovnováhu medzi estetikou a funkcionalitou, aby sme maximalizovali efektivitu komunikácie a zanechali trvalý dojem na našich poslucháčov. Poďme teraz spoločne preskúmať, aké konkrétne kroky sme podnikli pri tvorbe dizajnu a rozloženia tejto prezentácie.

* 1. Dizajn a rozloženie

Pri tvorbe dizajnu a rozloženia prezentácie som sa zameriaval na jednoduchosť a estetiku, aby som zabezpečil, že moje posolstvo bude jasne a účinne komunikované. Prezentácia má moderný a futuristický vzhľad, s obrazmi a grafikou, ktoré okamžite pritiahnu pozornosť čitateľa a udržia ju. Využil som obrázky s hravými a inovatívnymi formami, ktoré majú za cieľ zapôsobiť na čitateľa a zanechať si v jeho mysli trvalý dojem. Rozloženie textu som zvolil tak, aby bolo prehľadné a organizované. Text bol umiestnený po stranách prezentácie, čím som dosiahol rovnováhu medzi obsahom a vizuálnym prvkom. Tento prístup mi umožnil vytvoriť prezentáciu, ktorá pôsobí dobre premyslene a usporiadané, čo pomáha udržať pozornosť diváka a zabezpečiť, že informácie sú ľahko dostupné a zrozumiteľné. Týmto spôsobom som sa snažil minimalizovať chaotický dojem a zabezpečiť, že prezentácia bude pôsobiť profesionálne a presvedčivo.

* 1. Fonty

Fonty, ktoré som použil vo svojej prezentácii, boli starostlivo vybrané s ohľadom na ich vhodnosť pre tému a rozloženie textu. Pre telo textu som zvolil font Tw Cen MT, ktorý je moderný a plynulý, čo zabezpečuje ľahkú čitateľnosť. Tento font sa hodí k téme antivírusového softvéru a kybernetickej bezpečnosti svojím profesionálnym vzhľadom a moderným štýlom. Na nadpisy som použil font Tw Cen MT Condensed, ktorý pridáva určitý nádych štýlu a zároveň pomáha zvýrazniť dôležité body a hlavné témy prezentácie.

* 1. Obrázky

Obrázky v mojej prezentácii sú podobné kruhom v digitálnom vesmíre, ktoré pripomínajú moderné portály do sveta IT bezpečnosti. Ich futuristický dizajn a formy do kruhov dodávajú vizuálnu atraktivitu a zároveň evokujú pocit inovácie a technologického pokroku. Tento estetický prístup bol zvolený s cieľom zaujať a udržať pozornosť divákov. Každý slide obsahuje iba jeden obrazok, ktorý sa nachádza vo vyváženom stredovom bode, čo umožňuje divákom ľahko sa sústrediť na jeho obsah. Okrem toho boli do obrazov pridané malé detaily a prvky, ktoré pomáhajú vytvoriť atmosféru a zvýrazňujú ich význam v kontexte prezentácie o kybernetickej bezpečnosti. Tieto prvky dopĺňajú hlavný obsah a podčiarkujú hlavné myšlienky, čo prispieva k celkovému dojmu profesionality a vizuálnej príťažlivosti prezentácie.

* + 1. Prvky prezentácie

V mojej prezentácii som zahrnul niekoľko dizajnových prvkov, ktoré pomáhajú vizualizovať koncepty a hrozby v oblasti kybernetickej bezpečnosti. Do produktu boli implementované, pretože si čitateľ bude môcť lepšie zapamätať danú tému aj pri pohlade na objekty. Uľahčuje mu to potom učenie. Prvým dizajnovým prvkom je oranžová ryba, ktorá symbolizuje phishing. Tento 3D objekt predstavuje, ako rýchlo sa človek môže stať obeťou útoku phishingu a ako ľahko môže byť zvedený na klamné správy a podvodné požiadavky. Ryba je výrazná a zaujímavá, čo pomáha upútať pozornosť divákov a zdôrazniť vážnosť tohto typu kybernetického útoku. Ďalším dizajnovým prvkom je modré oko, ktoré reprezentuje spyware. Tento symbol zdôrazňuje, že používateľ je pod dohľadom pri útoku spywareu. Oko evokuje pocit sledovania a invázie do súkromia, čím vizuálne demonštruje nebezpečenstvo, ktoré predstavuje tento typ malvéru. Nakoniec, na slide o malvéroch, som zahrnul obraz vírusu v ktorý bežne napáda ľudské telo. Tento obraz ponúka ďalší spôsob, ako vizualizovať škodlivé účinky malvéru na počítačové systémy. Podobnosť s ľudským telom môže zdôrazniť invazívnu a deštruktívnu povahu malvéru a jeho schopnosť poškodiť a infikovať cieľový systém. Tieto dizajnové prvky nielenže pomáhajú vizualizovať rôzne hrozby v kybernetickej bezpečnosti, ale aj pridávajú estetickú hodnotu prezentácii a pomáhajú udržať pozornosť divákov.

1. Vnútorné spracovanie

V rámci vnútorného spracovania produktu som sa zameral na štruktúrovanie textu a obsahu tak, aby boli pre čitateľa jasné a prístupné. Rozhodol som sa umiestniť text do malých odsekov na pravú alebo ľavú stranu snímky, čo umožňuje plynulé čítanie a zabraňuje divákovi v záplave informácií. Tieto odseky dodávajú estetickú hodnotu prezentácii a zabezpečujú, že čitatelia sa v texte nestratia. Umiestnenie textu na pravú alebo ľavú stranu snímky zlepšuje celkovú rovnováhu dizajnu a umožňuje efektívnejšie využitie priestoru na prezentácii. Tento prístup tiež pomáha divákom sústrediť sa na obsah, keďže text je jasne oddelený od ostatných vizuálnych prvkov. Spoločne s kvalitným obsahom textu tieto estetické prvky pridávajú hodnotu prezentácii a zabezpečujú, že jej vizuálny dojem bude príťažlivý a profesionálny.

* 1. Jednoduchosť

V tejto podkapitole sa zameriavam na jednoduchosť textu a predstavujem veľmi jednoducho spracovaný obsah, ktorý je priateľský k čitateľovi nielen vo svojom dizajne, ale aj vo svojom obsahu. Cieľom je poskytnúť čitateľovi rýchlo pochopiteľné a zrozumiteľné informácie, ktoré sú vystihnuté jasne a stručne.

Pri tvorbe tejto časti som sa snažil o minimalizáciu odborných termínov a zložitých konceptov, aby bol obsah prístupný širokej škále divákov, dokonca aj študentom. Text bol navrhnutý tak, aby bol priateľský a prístupný, pričom sa zároveň zachováva jeho informačná hodnota. Tieto jednoducho spracované informácie budú rýchlo pochopiteľné pri pohľade na slide, čo umožní čitateľovi rýchlo sa oboznámiť s obsahom a porozumieť mu bez zbytočného zaváhania. Výsledkom je prezentácia, ktorá je jednoduchá, zrozumiteľná a prívetivá pre svoje publikum.

1. Záver

V závere mojej práce o antivírusovom softvéri a kybernetickej bezpečnosti by som rád zdôraznil niekoľko kľúčových myšlienok. Táto práca mi poskytla možnosť hlbšie sa ponoriť do problematiky kybernetickej bezpečnosti a porozumieť dôležitosti antivírusového softvéru v ochrane našich digitálnych systémov. Jedným z hlavných zistení tejto práce je, že dôkladná príprava a použitie spoľahlivých zdrojov sú nevyhnutné pre úspech v akejkoľvek prezentácii alebo projekte.

Hľadanie kvalitných informácií a ich overovanie je kľúčové pre vytvorenie dôveryhodného a informatívneho obsahu. Okrem toho som sa naučil, že estetický a priateľský dizajn môže zlepšiť celkový dojem prezentácie a pomôcť divákom lepšie pochopiť a zapamätať si prezentované informácie. Použitie vizuálnych prvkov, ako sú obrázky a grafika, môže výrazne obohatiť prezentáciu a prispieť k efektívnej komunikácii obsahu. Nakoniec, táto práca ma motivovala k ďalšiemu preskúmaniu problematiky kybernetickej bezpečnosti a k neustálemu vzdelávaniu sa v tejto oblasti. Súčasný digitálny svet prináša stále nové výzvy a hrozby, a je nevyhnutné byť neustále informovaný a pripravený na ochranu našich systémov a údajov. Celkovo som presvedčený, že pochopenie a osvojenie si princípov kybernetickej bezpečnosti a dôkladná príprava sú kľúčovými krokmi k zlepšeniu bezpečnosti a ochrany našich digitálnych prostredí. Som vďačný za túto príležitosť sa venovať tejto problematike a verím, že moja práca môže prispieť k šíreniu informácií a zvýšeniu povedomia o dôležitosti kybernetickej bezpečnosti v dnešnom digitálnom veku.

Zoznam použitej literatúry

**Príklad zoznamu použitej literatúry:**

1. YASAR, Kinza. Antivirus Software. [online]. [cit 2024-4-24]. Dostupné na:

<https://www.techtarget.com/searchsecurity/definition/antivirus-software >

1. ESET. Čo robí antivírus a prečo ho potrebujem ?. [online]. [cit. 2024-4-20]. Dostupné na : <https://bezpecnenanete.eset.com/sk/pre-ucitelov/co-robi-antivirus-a-preco-ho-potrebujem>
2. SLOVÁKOVÁ, Ai. Čo je to počítačový vírus a prečo je pre ľudí nebezbečný?. [online]. [citované 2024-4-20]. Dostupné na:

<https://www.techbox.sk/co-je-to-pocitacovy-virus-a-preco-je-pre-ludi-nebezpecny>

1. ESET. Malvér. [online]. [citované 2024-4-25]. Dostupné na:

<https://www.eset.com/cz/spyware>

1. ESET. Spyware. [online]. [citované 2024-4-25]. Dostupné na:

<https://www.eset.com/cz/spyware>

1. KOSNO, Lukáš. *Tatra banka eviduje nárast podvodných e-mailov, vystríha klientov* [online]. Živé.sk, [cit. 2019-01-18]. Dostupné na:

< https://zive.aktuality.sk>

1. Ako rozpoznať phishing? [online]. eset.com, [cit. 2024-04-25]. Dostupné na:

<https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-rozpoznat-phishing/>

1. Obrazok1
2. Obrazok 2
3. Obrazok 3