STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Zabezpečenie údajov**

ročníkový projekt

**Alexandra Bartolenová**

2024

Obsah

Obsah 2

Anotácia 3

1 Zabezpečenie údajov 4

1.1 Typy zabezpečenia údajov 4

1.1.1 Antivírus 5

1.1.2 Firewall 5

2 Riziká 7

3 Tvorba plagátu 8

3.1 Cieľová skupina 8

3.2 Návrhový nástroj 8

3.3 Rozlíšenie plagátu 9

3.4 Výber pozadia 9

3.5 Výber fontu 10

3.6 Výber farieb 10

3.7 Rozloženie informácií 10

3.8 Výber informácií 11

3.8.1 Hákovanie 11

3.8.2 Malvér 12

3.8.3 Únik údajov 12

3.8.4 Krádež 12

3.8.5 Podvod 12

3.8.6 Ransomware 12

4 Záver 14

Zoznam použitej literatúry 15

Anotácia

Zabezpečenie údajov je prax ochrany digitálnych informácií pred neoprávneným prístupom, poškodením alebo krádežou počas ich celého životného cyklu.

Tento koncept zahŕňa celé spektrum informačnej bezpečnosti. Zahrňuje fyzickú bezpečnosť hardvéru a úložných zariadení, spolu s administratívnymi a prístupovými kontrolami. Pokrýva aj logickú bezpečnosť softvérových aplikácií a organizačné politiky a postupy.

Rozprávanie o téme “zabezpečenie údajov” môže viesť k väčšej informovanosti a povedomiu o dôležitosti ochrany osobných údajov. Ak ľudia budú viac informovaní o tejto téme, môžeme predísť podvodom a krádežiam identity.

**Annotation**

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

This concept encompasses the entire spectrum of information security. It includes the physical security of hardware and storage devices, along with administrative and access controls. It also covers the logical security of software applications and organizational policies and procedures.

Talking about the topic of "data security" can lead to greater awareness and understanding of the importance of protecting personal data. If people are more informed about this topic, we can prevent fraud and identity theft.

1. Zabezpečenie údajov

Zabezpečenie údajov nám pomáha chrániť citlivé údaje počas ich životného cyklu, a zabrániť neoprávnenému použitiu alebo strate údajov.

* 1. Typy zabezpečenia údajov

Existuje niekoľko typov zabezpečenia údajov, ktoré organizácie a jednotlivci môžu implementovať na ochranu svojich informácií. Niektoré z najbežnejších typov zabezpečenia údajov zahŕňajú:

* Šifrovanie údajov: Proces konverzie dát do nečitateľnej podoby, aby sa predišlo neoprávnenému prístupu. Šifrovanie sa používa na ochranu dát v pohybe aj v úložiskách.
* Antivírus: pomáha chrániť vaše zariadenie pred rôznymi druhmi malware, ako sú vírusy, červy, trójske kone, ransomware a ďalšie škodlivé programy.
* Firewall: Zabezpečuje sieťovú bezpečnosť tým, že monitoruje a kontroluje prúdenie údajov medzi sieťami a zariadeniami. Blokuje nebezpečné alebo neautorizované prístupy.
* Zálohovanie údajov: Vytvorenie a uchovávanie kópií dôležitých údajov na bezpečných miestach, aby sa predišlo ich strate v prípade havárie alebo útoku.
* Ochrana prístupu: Tento typ zabezpečenia obmedzuje prístup k údajom iba na oprávnené osoby alebo systémy. Zahŕňa používanie silných hesiel, dvojfaktorovú autentifikáciu a riadenie prístupových práv.
* Aktualizácie: Pravidelné aktualizácie softvéru a systémov na odstránenie zraniteľností a ochranu pred hrozbami.
* Monitorovanie: Pravidelné monitorovanie a revízia bezpečnostných opatrení na identifikáciu potenciálnych hrozieb a nedostatkov v zabezpečení údajov.

Tieto typy zabezpečenia údajov môžu byť implementované samostatne alebo v kombinácii, aby sa zabezpečilo celkové bezpečnostné prostredie.

* + 1. Antivírus

Antivírusový softvér funguje ako ochranný štít pre vaše zariadenie a údaje, pričom využíva niekoľko spôsobov na ochranu pred škodlivým softvérom a zabezpečuje vaše údaje.

Antivírusový softvér pravidelne skenuje súbory a aplikácie na vašom zariadení, aby odhalil prítomnosť škodlivých súborov. Tento skenovací proces zahrňuje porovnávanie súborov s databázou známych škodlivých kódov a identifikáciu nezvyčajného správania, ktoré by mohlo naznačovať prítomnosť vírusu.

Keď antivírus identifikuje škodlivý súbor, buď ho karanténuje, aby zabránil jeho šíreniu, alebo ho odstráni z vášho zariadenia.

Mnoho moderných antivírusových programov používa heuristické analýzy a umelú inteligenciu na identifikáciu nových a neznámych hrozieb. Tieto nástroje sú schopné odhaliť potenciálne škodlivý kód na základe jeho charakteristík a správania, aj keď ešte táto hrozba nie je moc známa.

Niekedy antivírusový softvér ponúka funkcie na ochranu online aktivity, ako je kontrola webstránok, ochrana proti phishingu a firewall, ktorý monitoruje sieťovú komunikáciu a chráni pred neoprávneným prístupom.

* + 1. Firewall

Firewall je základným prvkom zabezpečenia počítačových sietí a slúži na ochranu pred neoprávneným prístupom a útokmi z internetu. Jeho úlohou je monitorovať a kontrolovať komunikáciu medzi rôznymi sieťami, ako napríklad lokálnou sieťou a internetom, a zabezpečiť, aby sa neželané alebo škodlivé dáta nedostali do chránenej siete.

Pri vstupe alebo výstupe dát z vášho zariadenia firewall kontroluje obsah dát, ktoré cestujú cez sieť. Používa rôzne pravidlá a filtre na rozhodovanie o tom, čo je povolené a čo je blokované.

V prípade, že firewall zistí, že dáta spĺňajú kritériá, umožní ich prechod cez sieť. Naopak, ak dáta nespĺňajú tieto kritériá alebo sú identifikované ako nebezpečné, firewall ich zablokuje a zabráni im vstúpiť do vašej siete.

Okrem blokovania nežiaducich dát môže firewall tiež upozorniť na možné hrozby alebo nezvyčajné aktivity v sieti. Tieto upozornenia umožňujú administrátorom siete identifikovať potenciálne bezpečnostné problémy.

Firewall môže byť implementovaný ako hardvérové zariadenie alebo softvérová aplikácia na vašom počítači alebo sieti.

Výhody použitia firewallu:

* Bezpečnosť siete – Firewall pomáha chrániť sieť pred neoprávneným prístupom a útokmi, čím znižuje riziko úniku citlivých dát alebo poškodenia systémov.
* Kontrola a filtrovanie prevádzky – Firewall umožňuje sledovať a riadiť sieťovú prevádzku, čím sa dá efektívne blokovať škodlivý obsah, spam a nežiaduce komunikácie.
* Ochrana pred malvérom – Firewall dokáže identifikovať a zablokovať pokusy o infikovanie malvérom, ako sú vírusy, červy, trójske kone a ďalšie škodlivé programy.
* Zvýšenie dôvernosti – Firewall umožňuje prístup k citlivým informáciám len autorizovaným používateľom a obmedzuje ich prístup pre ostatných.
* Monitorovanie a audit – Firewall poskytuje funkciu monitorovania a auditu siete, čo umožňuje sledovať sieťovú prevádzku, identifikovať hrozby a vyhodnocovať bezpečnostné udalosti.

|  |  |
| --- | --- |
| **Typ aplikácie** | **Percentá** |
| Office | 55,81% |
| Webový prehliadač | 29,13% |
| Android | 6,15% |
| Adobe Flash | 4,03% |
| Java | 3,34% |
| PDF | 1,53% |

Tabuľka č. 1, Rozdelenie exploitov používaných počítačovými zločincami podľa typu napadnutej aplikácie.

1. Riziká

Zlé zabezpečenie údajov prináša viacero rizík, ktoré môžu mať vážne následky pre jednotlivcov aj organizácie. Niektoré z nich sú:

* Strata súkromia: Únik citlivých a osobných údajov. Môže prísť k ich zneužitiu na rôzne spôsoby, ako je identity theft alebo spam.
* Finančné straty: Strata finančných údajov, ako sú bankové údaje alebo kreditné karty, môže viesť k finančným stratám prostredníctvom neoprávnených transakcií alebo podvodu.
* Strata dôveryhodnosti: Únik citlivých obchodných údajov môže poškodiť dôveru zákazníkov a obchodných partnerov.
* Zneužitie údajov: Neoprávnení jednotlivci alebo organizácie môžu zneužiť ukradnuté údaje na šírenie spamu, vydieranie alebo iné škodlivé aktivity.
* Kybernetické útoky: Zle zabezpečené údaje môžu byť cieľom kybernetických útokov, ako sú ransomware, malware alebo phishing, čo môže viesť k poškodeniu systémov a stratám dát.
* Strata konkurenčnej výhody: Únik obchodných tajomstiev alebo strategických informácií môže poškodiť konkurenčnú výhodu organizácie a umožniť konkurentom získať neoprávnený prístup k dôležitým informáciám.

Obrázok, na ktorom je text, snímka obrazovky, číslo, písmo

Automaticky generovaný popis

Graf č. 1, Distribúcia Malvérových Infekcií na Desktopových Počítačoch. []

1. Tvorba plagátu

Pri tvorbe plagátu na tému "Zabezpečenie údajov" som sa pustila do procesu s nadšením a odhodlaním. Každý detail, od výberu farieb po rozmiestnenie textu, bol dôkladne premyslený s cieľom vytvoriť vizuálne atraktívny a informatívny plagát. Dizajnovanie tohto plagátu ma obohatilo novými skúsenosťami a považovala som to za príležitosť prezentovať dôležité informácie v jednoduchom a zreteľnom formáte. S pomocou návrhového nástroja som mohla pretvoriť svoje myšlienky do života a vytvoriť plagát, ktorý zaujme a osvetlí túto dôležitú tému.

* 1. Cieľová skupina

Chcela som aby cieľová skupina zahŕňala široké spektrum vekových skupín, pričom by sa zameriavala predovšetkým na ľudí, ktorí možno nie sú dostatočne informovaní o hrozbách na internete a v oblasti bezpečnosti údajov. Cieľová skupina zahŕňa mladých ľudí, ktorí sú aktívni na internete, ale nemajú dostatočné znalosti o tom, ako sa chrániť pred rôznymi formami kybernetických hrozieb. Okrem toho sú tu aj starší ľudia, ktorí možno majú obmedzené technologické znalosti a môžu byť zraniteľní voči online podvodom a útokom. Pre tieto skupiny je dôležité ponúknuť základné informácie o zabezpečení údajov a o tom, ako fungujú rôzne ochranné mechanizmy. Plagát je navrhnutý tak, aby bol jednoduchý na pochopenie a prístupný pre každého, kto sa chce dozvedieť viac o tom, ako chrániť svoje osobné údaje a bezpečne surfovať na internete. Je to nástroj na osvetu a informovanie, ktorý sa snaží zvýšiť povedomie o zabezpečení svojich údajov a pomôcť ľuďom pochopiť hrozbám s ktorými sa môžu stretnúť, keď nebudú ich údaje dostatočne zabezpečené.

* 1. Návrhový nástroj

Pri tvorbe tohto plagátu som sa rozhodla využiť návrhový nástroj Figma. Tento nástroj mi poskytol flexibilitu a efektívne prostredie na vytvorenie dizajnu plagátu. S jeho pomocou som mohla jednoducho manipulovať s farbami, textom a obrázkami, čo mi umožnilo presne vyjadriť moje myšlienky a nápady. Celkovo mi použitie Figma ako nástroja na dizajn umožnilo efektívne a profesionálne vytvoriť plagát na tému zabezpečenia údajov.



Obr. č. 1, Figma. [4]

* 1. Rozlíšenie plagátu

Pri vyberaní rozlíšenia plagátu som sa zamerala na viaceré faktory. Začala som zvážením dostupných možností a potrieb cieľovej skupiny. Rozhodla som sa pre rozlíšenie 792x1224, pretože som chcela dosiahnuť dostatočne vysoké rozlíšenie, ktoré by umožnilo zobraziť detailné informácie a obrázky na plagáte. Zároveň som chcela zachovať pomer strán 2:3, aby plagát mal vyvážený a estetický vzhľad. Toto rozlíšenie mi tiež umožnilo vytvoriť plagát vhodný pre digitálny aj tlačený formát, čo zvýšilo jeho univerzálnosť a použiteľnosť. Celkovo som sa rozhodla pre toto rozlíšenie pre jeho schopnosť efektívne prezentovať obsah plagátu s detailmi a esteticky príjemným vzhľadom.

* 1. Výber pozadia

Vybrala si pozadie pre plagát v modrých farbách, čo je skvelá voľba, kvôli tomu, že tieto farby vytvárajú minimalistický a profesionálny vzhľad, ktorý je zároveň príjemný pre oko. Modrá farba sa často spája s technológiou a informačnými technológiami, takže toto pozadie okamžite evokuje spojenie s IT a zabezpečením údajov. Táto farba môže pôsobiť upokojujúco a dôveryhodne, čo je dôležité, keď prezentujeme informácie o zabezpečení údajov. Zároveň však neodvádza pozornosť od textu a iných prvkov na plagáte, čo umožňuje čitateľovi sústrediť sa na hlavné informácie. Toto minimalistické pozadie v modrých tónoch teda úspešne podporuje tému zabezpečenia údajov a prispieva k celkovému profesionálnemu a atraktívnemu vzhľadu plagátu.

* 1. Výber fontu

Pri výbere správneho fontu a jeho veľkosti som sa riadila niekoľkými kľúčovými faktormi. Začala som preskúmaním dostupných možností a zvážila som ich vhodnosť vzhľadom na tému a cieľovú skupinu plagátu. Zistila som, že font Jost je ideálnou voľbou pre svoju čitateľnosť a moderný vzhľad, ktorý je zároveň dostatočne univerzálny a profesionálny. Po vybraní tohto fontu som sa venovala určeniu správnej veľkosti. Zvolila som takú veľkosť, ktorá umožní, aby text bol ľahko čitateľný a zreteľný z diaľky, ale zároveň nezaberal príliš veľa miesta na plagáte a nevyzeral preplnený. Celkovým cieľom bolo zvoliť font a veľkosť, ktoré by podporili jasné a atraktívne prezentovanie informácií na plagáte a prispeli k celkovému estetickému dojmu.

* 1. Výber farieb

Pri výbere farieb pre môj plagát som zohľadnila niekoľko dôležitých faktorov. Pozadie som zvolila v odtieňoch modrej farby, ako som uvádzala vyššie. Text som zvolila vo farbe čiernej, pretože poskytuje dobrý kontrast s modrým pozadím a je ľahko čitateľný. Avšak pod textom sú geometrické útvary vo farbe sivej, ktoré zvýraznia napísané informácie na plagáte a dopomôžu, že text na týchto prvkoch bude ľahko čitateľný.

Okrem toho som zahrnula farby ako biela, ružová, žltá a ďalšie odtiene modrej, ktoré dopĺňajú celkový dizajn a prispievajú k estetike plagátu. Text v týchto farbách som opäť zvolila čierny, aby bol čo najviac kontrastný a zreteľný. Tieto farby som vybrala aj s ohľadom na ikonku na plagáte, aby sa celkový vizuálny dojem zhodoval s témou a cieľmi projektu.

* 1. Rozloženie informácií

Rozmýšľala som nad rozložením môjho plagátu a rozhodla som sa ho rozdeliť na hornú a dolnú časť, aby som lepšie zorganizovala informácie a aby bol plagát viacej priehľadný a ľahký na pochopenie.

V hornej časti som sa rozhodla umiestniť základné informácie o zabezpečení údajov. Cítila som, že je dôležité vysvetliť dôvody pre zabezpečenie údajov a poukázať na riziká, ktoré by mohli vzniknúť v prípade ich nedostatočného zabezpečenia. Preto som sa rozhodla zahrnúť aj informácie o opatreniach, ktoré môžu pomôcť zabrániť krádeži údajov. Verím, že táto časť poskytne jasné a zrozumiteľné informácie o zabezpečení údajov.

V dolnej časti som sa rozhodla popísať konkrétne riziká, ktoré môžu vzniknúť v súvislosti s nedostatočným zabezpečením údajov. Myslím si, že je dôležité poskytnúť čitateľom podrobnejší pohľad na tieto hrozby. Každé riziko som chcela podrobne vysvetliť a prípadne poskytnúť príklady alebo dôsledky, ktoré by mohli nastať pre jednotlivcov alebo organizácie. Týmto spôsobom som chcela poskytnúť čitateľom komplexný, ale za to jednoduchý pohľad na tému zabezpečenie údajov a pomôcť im lepšie porozumieť rizikám, ktorým môžu čeliť.

Informácie na plagáte som sa snažila napísať takým spôsobom, aby ich mohol pochopiť každý, kto si ich prečíta, bez ohľadu na ich vek alebo úroveň znalostí. Cítila som, že je dôležité, aby moje posolstvo bolo prístupné a zrozumiteľné pre širokú škálu ľudí - od dospelých po starších ľudí a dokonca aj deti. Chcela som, aby boli informácie jasné, priamočiare a ľahko interpretovateľné, aby sa každý mohol dozvedieť niečo nové o zabezpečení údajov, bez ohľadu na ich predchádzajúce skúsenosti alebo znalosti v tejto oblasti.

* 1. Výber informácií

V dolnej časti plagátu som sa rozhodla popísať konkrétne riziká ako hakovanie, malver, únik údajov, krádež, podvod a ransomware z niekoľkých dôvodov. Tieto riziká som považovala za veľmi dôležité, pretože v digitálnej ére sa čoraz častejšie s nimi stretávame.

Hakovanie a malvéry predstavujú hrozby, ktoré sa môžu zdať abstraktné, ale ich dôsledky môžu byť závažné. Únik údajov je tiež veľmi aktuálnou a alarmujúcou hrozbou, keďže sa stále viac dát ukladá online a ich bezpečnosť môže byť narušená rôznymi spôsobmi. Krádeže, podvody a ransomware sú taktiež závažné hrozby, ktoré môžu spôsobiť vážne finančné a emocionálne škody.

Cítila som, že je dôležité zvýšiť povedomie o týchto hrozbách a informovať ľudí o tom, ako fungujú. Týmto spôsobom som chcela divákom poskytnúť užitočné a praktické informácie, ktoré im pomôžu lepšie pochopiť digitálnu bezpečnosť.

* + 1. Hákovanie

Pri písaní o hákovaní vo svojom ročníkovom projekte som sa rozhodla podať jeho definíciu stručne a jasne. Identifikovala som ho ako pokus o krádež údajov, poškodenie sietí alebo súborov, ovládnutie digitálneho prostredia organizácie alebo poškodenie údajov. V mojom postupe som sa zamerala na zrozumiteľnosť a jednoduchosť vyjadrenia, aby som divákom umožnila ľahšie pochopiť podstatu tohto konceptu.

* + 1. Malvér

Pri písaní o malvéroch vo svojom ročníkovom projekte som sa sústredila na jeho stručnú a zrozumiteľnú charakteristiku. Definovala som ho ako kategóriu zahŕňajúcu červy, vírusy a spyware, ktoré umožňujú neoprávneným používateľom prístup do vašich zariadení. Vysvetlila som, že to môže viesť k poškodeniu siete a k ukradnutiu citlivých údajov. Mojím cieľom bolo poskytnúť čitateľom stručný a jasný prehľad o tejto problematike, aby mohli lepšie porozumieť hrozbám spojeným s malvérom.

* + 1. Únik údajov

Pri písaní o úniku údajov vo svojom ročníkovom projekte som sa sústredila na jeho stručnú a jasnú definíciu. Definovala som ho ako zámerný alebo náhodný prenos informácií zvnútra organizácie k externému príjemcovi. Cieľom bolo poskytnúť čitateľom jednoduchý a zrozumiteľný prehľad o tomto koncepte a jeho dôležitosti v oblasti kybernetickej bezpečnosti.

* + 1. Krádež

Pri písaní o krádeži vo svojom ročníkovom projekte som sa zamerala na stručný a jasný opis tohto fenoménu. Definovala som krádež zvnútra ako spôsobujúcu škodu prostredníctvom kradnutia údajov, peňazí alebo duševného vlastníctva. Cieľom bolo poskytnúť čitateľom jednoduché a zrozumiteľné vysvetlenie tohto pojmu a jeho významu v oblasti kybernetickej bezpečnosti.

* + 1. Podvod

Pri písaní o podvode vo svojom ročníkovom projekte som sa zameriavala na stručný a jasný opis tohto rizika. Definovala som podvod ako využívanie anonymitu online sveta na páchanie podvodov v reálnom čase, napríklad podvod s vrátením peňazí. Mojím cieľom bolo poskytnúť čitateľom jednoduché a zrozumiteľné vysvetlenie tohto pojmu a jeho významu v oblasti kybernetickej bezpečnosti.

* + 1. Ransomware

Pri písaní o ransomware vo svojom ročníkovom projekte som sa snažila poskytnúť stručný a zrozumiteľný opis tohto javu. Definovala som ransomware ako formu škodlivého softvéru, ktorý obmedzuje prístup k sieti a súborom, kým nie je zaplatené požadované výkupné. Mojím cieľom bolo jednoducho vysvetliť tento pojem a jeho význam v rámci problematiky kybernetickej bezpečnosti.

Obrázok, na ktorom je text, snímka obrazovky, plagát, tlač

Automaticky generovaný popis

Obr. č. 2, Plagát Zdroj: Autor práce

1. Záver

V rámci tohto projektu som podrobne preskúmala tému zabezpečenia údajov a navrhla plagát, ktorý slúži ako nástroj na osvetu a informovanie o tejto dôležitej problematike. Pri vytváraní plagátu som sa zameriavala na jeho estetiku, zrozumiteľnosť a relevantnosť pre cieľovú skupinu.

V prvých častiach projektu som vysvetlila dôvody pre zabezpečenie údajov, rôzne formy kybernetických hrozieb a opatrenia na ochranu osobných údajov. Následne som sa venovala detailnému popisu konkrétnych hrozieb ako hackovanie, malvér, únik údajov, krádež, podvod a ransomware, pričom som zdôraznila ich dôležitosť a riziká.

Pri tvorbe plagátu som sa snažila o optimalizáciu farieb, rozloženia a typografie, aby bol čo najúčinnejší vo vizuálnom komunikovaní. Modré pozadie vytvára atmosféru dôvery a spoľahlivosti, zatiaľ čo čierna farba textu zabezpečuje jeho čitateľnosť. Na tvary pod textom som použila svetlý odtieň šedej, aby bol text jasne viditeľný.

V závere odporúčam, aby bola problematika kybernetickej bezpečnosti integrovaná do vzdelávacieho systému, najmä na úrovni stredných a vysokých škôl. Je dôležité, aby sa mladí ľudia učili o rizikách a opatreniach týkajúcich sa zabezpečenia údajov už od mladého veku. Verím, že môj plagát, na ktorom sú vysvetlené najznámejšie a ľahko pochopiteľné informácie o tejto téme, môže v tomto úsilí významne pomôcť.

Zoznam použitej literatúry

1. Coderama. Firewall. [online]. [cit. 2024-04-21]. Dostupné na internete: <https://coderama.com/slovnik/firewall/>.
2. Diseven. 10 najčastejších bezpečnostných rizík, ktoré môže odhaliť bezpečnostný audit. [online]. [cit. 2024-04-21]. Dostupné na internete: <https://www.diseven.sk/bezpecnostna-sluzba/clanky/10-najcastejsich-bezpecnostnych-rizik-ktore-moze-odhalit-bezpecnostny-audit.html/>.
3. Esenc. Ako funguje antivírus? [online]. [cit. 2024-04-21]. Dostupné na internete: <https://esencsk.wordpress.com/2019/01/28/ako-funguje-antivirus/>.
4. Figma. Figma and Collaboration - Smart Animate Presentation. [online]. [cit.2024-04-21]. Dostupné na internete: <https://www.figma.com/community/file/950702083518868636/figma-and-collaboration-smart-animate-presentation />.
5. McAfee. Čo je to brána firewall? [online]. [cit. 2024-04-21]. Dostupné na internete: <https://www.mcafee.com/sk-sk/antivirus/firewall.html>.
6. Microsoft. Čo je zabezpečenie údajov? [online]. [cit. 2024-04-21]. Dostupné na internete: <https://www.microsoft.com/sk-sk/security/business/security-101/what-is-data-security>.
7. Safetydetectives. Antivirus and Cybersecurity Statistics, Trends & Facts 2024. [online]. [cit.2024-04-21]. Dostupné na internete: <https://www.safetydetectives.com/blog/antivirus-statistics/>.
8. Securelist. IT threat evolution in Q2 2021. PC statistics. [online]. [cit.2024-04-21]. Dostupné na internete: <https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/>.
9. Verizon. Antivirus. [online]. [cit.2024-04-21]. Dostupné na internete: <https://www.verizon.com/articles/internet-essentials/antivirus-definition/>.