STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Bezpečnosť na internete**

Vonkajšia aj vnútorná

**Michal Halagačka**

2024

Obsah

1 Internetová bezpečnosť 4

1.1 Prečo je Internetová bezpečnosť dôležitá 4

1.1.1 Krádež identity 4

1.1.2 Krádež údajov 4

2 VPN siete 5

2.1 Čo je to VPN a prečo ich používať 5

2.2 Čo robia VPN a prečo ich používať 5

2.2.1 Čo, to ale pre nás znamená? 5

2.3 Ich využitia 5

2.4 Šifrovanie a autentifikácia v VPN 6

2.5 Zraniteľnosti a riziká spojené s používaním VPN 6

3 Ochrana Firewallom 7

3.1 Čo to je a limitácie 7

3.2 Trocha histórie 7

3.3 Typy Firewallov 7

3.3.1 Ako ochraňuje hosťovský Firewall 8

3.3.2 Ako ochraňuje sieťový Firewall 8

3.4 Pokročilé techniky ochrany s pomocou Firewallu 8

3.4.1 Využitie ‚Intrusion Detection‘ a ‚Prevention System‘ s Firewallom 8

3.4.2 Využitie VPN cez Firewall pre zabezpečené prepojenie 8

4 Porovnanie 9

5 Produkt 10

5.1 Myšlienka 10

5.2 Prezentácia 10

5.2.1 Obsah prezentácie časť 1 10

5.2.2 Obsah prezentácie časť 2 11

5.2.3 Obsah prezentácie časť 3 11

5.3 Dizajn 12

5.3.1 Postup pri dizajne 13

5.3.2 Detaily 13

6 Záver 14

Zoznam použitej literatúry 15

Anotácia

Úloha bola spraviť produkt a k nemu dokumentáciu. Prvé čo ma napadlo bola téma, o ktorej som sa chcel viac naučiť a to bola bezpečnosť na internete. To ma prinieslo k hlavným spôsobom ochrany dôležitých údajov a zariadení, Firewall a VPN. Zároveň som chcel niečo o čom by som neskôr mohol naučiť ostatných. Toto je taktiež dôvod, prečo som sa rozhodol spraviť učebný materiál ako môj produkt. Predsa z internetových fórov a diskusií viem, že málo ľudí vie, prečo je dôležité mať Firewall zapnutý, či riziká ktoré VPN prináša.

**Annotation**

The task was to make a product and its documentation. The first thing that came to mind was the topic I wanted to learn more about and that was internet security. This brought me to the main ways to protect important data and devices, Firewall and VPN. At the same time, I wanted something that I could later teach others about. This is also the reason why I decided to make learning material as my product. After all, I know from Internet forums and discussions that few people know why it is important to have the Firewall on, or the risks that VPN brings.

1. Internetová bezpečnosť

Internet je plný nebezpečenstiev. Pomaly každý má osobné údaje niekde uložené na internete, či ich tam mať chceme a či nie, ale málo z nás si uvedomuje spôsoby, ktorými sú chránené pred hackermi a ďalšími nežiadanými osobami. Spôsoby ochrany dokážeme kategorizovať na vonkajšie (VPN) a vnútorné (Firewall).

* 1. Prečo je Internetová bezpečnosť dôležitá

Bez zavedených bezpečnostných opatrení je možné prezerať, zachytávať a dokonca ukradnúť súkromné ​​alebo dôverné informácie alebo správy. V závislosti od zámeru vniknutia sa môže čin hackera pohybovať od neškodných, ako je prieskum trhu, až po zničujúce, ako je krádež identity alebo iný podvod. Vlády a spoločnosti s citlivými informáciami sú tiež ohrozené, pretože ich vlastné informácie sú často cenné a tiež uchovávajú súkromné ​​informácie o jednotlivcoch, ako sú zákazníci alebo zamestnanci.

* + 1. Krádež identity

Krádež identity je prevládajúcim problémom v informačnom veku, pretože ľudia nakupujú, predávajú a vymieňajú si informácie online. Bez dostatočného zabezpečenia môžu online transakcie viesť k tomu, že podvodníci získajú informácie o vašej kreditnej karte, osobné údaje a dokonca aj číslo sociálneho poistenia. S týmito informáciami môžu vykonávať podvodné poplatky a nákupy, brať si pôžičky, žiadať o štátne dávky a spôsobiť zmätok vo vašom súkromnom živote. Aj keď vo všeobecnosti môžete všetko vyriešiť, odstránenie škody spôsobenej zlodejom identity si vyžaduje čas, úsilie a v niektorých prípadoch aj náklady.

* + 1. Krádež údajov

Ďalším problémom je krádež údajov, pri ktorej sa digitálne kradnú citlivé alebo osobné údaje, ako sú videá, dokumenty a fotografie. Tieto informácie sa potom môžu ďalej predávať alebo distribuovať na nezákonné účely. Spoločnosti riskujú stratu dôležitých testovacích údajov, dôverných finančných súborov, obchodných tajomstiev, návrhov produktov a ďalších údajov od zlodejov údajov. Vládam hrozí odcudzenie citlivých materiálov vrátane údajov o prebiehajúcich výskumných projektoch, osobnej korešpondencie medzi jednotlivcami a zoznamov s podrobnosťami o vojenských rozmiestneniach, stratégiách a menách agentov v zahraničí.

1. VPN siete
   1. Čo je to VPN a prečo ich používať

VPN (po anglicky Virtual Private Network‘) vytvára digitálne spojenie medzi osobným zariadením, ako je počítač či mobil, a vzdialeným serverom vo vlastníctve poskytovateľa VPN. Týmto spôsobom vytvára point-to-point tunel, ktorý šifruje vaše osobné údaje, maskuje vašu IP adresu a umožňuje vám obísť bloky webových stránok a brány firewall na internete. To zaisťuje, že vaše online skúsenosti sú súkromné, chránené a bezpečnejšie.

* 1. Čo robia VPN a prečo ich používať

Keď sa pripájate na VPN, vaše osobné zariadenie sa ako prvé pokúsi pripojiť na VPN server pomocou asymetricky a symetricky šifrovanej komunikácie. Je ťažké, aby ste boli v tomto kroku úplne zabezpečený, keďže práve počas pripájania sa na VPN sa vaše zariadenie snaží dohodnúť so serverom, akú šifru použiť a určiť pre ňu kľúč. Ten bude fungovať ako vstup do matematickej funkcie, ktorá tvorí túto šifru. Podľa typu šifry, je možné ho použiť na tvorbu druhého kľúča, ktorý je potom použitý na tvorbu danej šifry. Po tom, ako je celý tento proces dokončený, ste oficiálne pripojený na sieť VPN.

* + 1. Čo, to ale pre nás znamená?

Po pripojení na VPN, posiela naše zariadenie údaje na server VPN poskytovateľa v šifre, ktorá bola určená počas prepájacieho procesu. Táto šifra je potom dekódovaná serverom a neskôr je dešifrovaný paket poslaný na internet s IP adresou a celkovo informáciami VPN servera namiesto vašimi.

* 1. Ich využitia

Sieť VPN možno použiť na skrytie histórie prehliadača používateľa, IP adresy a geografickej polohy, webovej aktivity alebo používaných zariadení. Nikto v rovnakej sieti nebude môcť vidieť, čo robí používateľ VPN. Vďaka tomu sú siete VPN ideálnym nástrojom na ochranu súkromia online. Je ale pravda, že záleží na tom ako veríte svojmu VPN poskytovateľovi, keďže má schopnosť si o vás ukladať údaje a neskôr ich predávať, alebo môže mať zlú šifru.

* 1. Šifrovanie a autentifikácia v VPN

Pri používaní VPN sieťových spojení je kľúčová úroveň šifrovania a autentifikácie. Šifrovanie zabezpečuje, že všetky prenášané údaje sú chránené pred odpočúvaním a manipuláciou tretími stranami. Autentifikácia zaisťuje, že iba oprávnení používatelia majú prístup k VPN sieti. Rôzne protokoly a metódy autentifikácie môžu mať rôzne úrovne bezpečnosti a vhodnosti pre konkrétne použitie. Je dôležité, aby používatelia vybrali správny protokol a konfiguráciu autentifikácie podľa ich individuálnych potrieb a bezpečnostných požiadaviek. Je potrebné povedať, že dosť ľudí si nechá spôsob šifry nastaviť automaticky.

* 1. Zraniteľnosti a riziká spojené s používaním VPN

Hoci VPN siete môžu poskytovať významnú úroveň súkromia a bezpečnosti, nie sú imúnne voči rôznym zraniteľnostiam a rizikám. Napríklad niektoré protokoly VPN môžu byť náchylné na útoky, ako napríklad útoky hrubou silou alebo ‚man-in-the-middle‘ útoky. Okrem toho môžu byť niektoré VPN klienty alebo aplikácie zraniteľné voči rôznym softvérovým chybám a útokom na zariadenie. Používatelia by mali byť informovaní o týchto rizikách a prijímať opatrenia na ich minimalizáciu, ako napríklad aktualizáciu softvéru a zabezpečenie silného hesla pre svoje účty.

Graf 1. Percentá používateľov VPN podľa zariadení

1. Ochrana Firewallom
   1. Čo to je a limitácie

Firewall je zariadenie, alebo software, ktorý sleduje prichádzajúce a odchádzajúce údaje zo siete. Aj keď sú viac menej nevyhnutné a veľmi užitočné, nie sú perfektné. Na internete som zistil o týchto limitáciách:

1. Nezastaví používateľov od získavania údajov či súborov na zlomyseľných stránkach. Jednoduchšie povedané, niekto si stále môže stiahnuť vírus do počítača aj keď má na zariadení Firewall.
2. Nevedia ochrániť organizácie od sociálneho inžinierstva. Firewall nedokáže zabrániť niekomu aby použil ľudí na získanie prístupu ku sieti.
3. Nevie zabrániť vírusu, ktorý už je na počítači, keďže sa nenachádza na sieti.
4. Firewall nevie zabrániť hackerom používať už ukradnuté heslá, aby sa dostali k citlivým informáciám.
   1. Trocha histórie

Firewall bol prvou ochranou pre sieťové komunikácie. Existovali asi tak dlho ako routere, od približne 1985, avšak prvý papier rozoberajúci filtrovací proces používaný, v tej dobe ešte novým, ochranným spôsobom sa nevyšiel až do 1988. Napísal ho Jeff Mogul z Digital Equipment Corporation. V rokoch 1989-1990, Dave Presotto a Howard Trickey z AT&T Bell Laboratories vynašli druhú generáciu firewall štruktúry, taktiež nazývané ‚Firewally na úrovni okruhu‘ (circuit level firewalls) a taktiež implementovali prvý fungujúci model tretej generácie firewallov.

* 1. Typy Firewallov

Firewally môžeme rozlišovať na dva druhy, a to sú Hardware Firewall a Software Firewall. Fungujú dosť rozlične od seba ale spĺňajú ten istý ciel a to je bezpečnosť na internete. Software Firewally ochraňujú hosťa, teda zariadenie na ktorom bežia ako napríklad stolný počítač, či mobilný telefón. Hardware Firewall naopak ochraňuje sieť, ku ktorej je pripojená. Vďaka týmto rozdielom ich občas voláme hosťovská Firewall a sieťová Firewall. Ďalší rozdiel by bol v tom, že software Firewall je program, ktorý beží na osobnom zariadení a hardware býva samostatné zariadenie

* + 1. Ako ochraňuje hosťovský Firewall

Ochraňuje len jedno zariadenie, ale príde pribalená s operačným systémom. Softwarové Firewally ochraňujú. Najbežnejší druh Firewallu, ktorý je možné nájsť na väčšine osobných funguje tým, že prehľadáva si prichádzajúce či odchádzajúce údaje a porovnáva ich s listom nebezpečenstiev. Ak sa ‚data packet‘ rovná profilu známeho nebezpečenstva, zahodí ho.

* + 1. Ako ochraňuje sieťový Firewall

Hardware Firewall funguje ako samostatný spotrebič, ktorý sleduje 3. a 4. OSI vrstvy a skenuje prevádzku medzi vonkajšími zdrojmi a lokálnou sieťou alebo medzi segmentami v sieti. Pakety monitorujú hlbokou inšpekciou. Ak paket nespĺňa predtým vybraté kritéria, podľa pravidiel vybraných správcom siete, komunikácia bude odmietnutá a zablokovaná.

* 1. Pokročilé techniky ochrany s pomocou Firewallu

Tu sú trocha pokročilejšie témy ohľadom Firewall systémov a ich využitiami. Je to skôr ako doplnok pre tých, ktorí sú zaujatý. Aj tak doporučujem si to aspoň na rýchlo prečítať.

* + 1. Využitie ‚Intrusion Detection‘ a ‚Prevention System‘ s Firewallom

Integrácia ‚Intrusion Detection System‘ (IDS) a ‚Intrusion Prevention System‘ (IPS) s Firewallom má za cieľ detegovať a blokovať škodlivú aktivitu v sieti. IDS sleduje sieťovú prevádzku a identifikuje potenciálne hrozby, zatiaľ čo IPS aktívne zasahuje a blokuje nebezpečné spojenia alebo útoky.

* + 1. Využitie VPN cez Firewall pre zabezpečené prepojenie

Použitie VPN cez Firewall umožňuje zabezpečenú a šifrovanú komunikáciu medzi vzdialenými zariadeniami a sieťou. Táto technika poskytuje ochranu pred odpočúvaním a manipuláciou s dátami počas prenosu cez verejné siete, ako je internet. Podľa mňa je toto dosť ideálne riešenie, keďže sa ochranné spôsoby dobre dopĺňajú.

1. Porovnanie

Firewall a VPN fungujú prekvapivo odlišne od seba. Najskôr poviem niečo o Firewall, keďže o ňom zhrnúť moje predošlé body rýchlejšie. Firewall funguje ako strážca, ktorý nenechá nič nepovolené prejsť. Keďže filtruje čo ide von a aj dnu z počítača, zabraňuje cudzím ľudom, aby infikovali zariadenie používateľa. Na druhej strane máme VPN, ktorá funguje úplne odlišne. Podľa mňa práve tu nastáva problém s ľuďmi, ktorí hovoria o neschopnosti VPN. Firewall, ako sme už povedali, filtruje údaje na sieti a tým ochraňuje nie len počítač, ale aj celú sieť. Ak paket neprejde cez jeden počítač, nedostane sa k druhému. VPN chce tento krok urobiť irelevantným. VPN zašifruje všetky údaje medzi počítačom a serverom. V tomto prípade, aj keby sa niekto nabúral do tejto siete, bez kľúča by z toho nič nemal. Nie len, že by nedokázal niečo poslať do počítača, pretože by to dešifrovací algoritmus pravdepodobne zničil, ale nevedel by ani žiadne údaje prečítať.

|  |  |  |  |
| --- | --- | --- | --- |
| X | Hlavné výhody | Hlavné nevýhody | Osobný názor |
| Firewall | - Je predinštalovaný na väčšine osobných zariadení.  - Môže byť neustále zapnutý.  - Filtruje údaje prechádzajúce cez sieť .  - Ochraňuje od toho, aby počítač posielal pakety kam nemá, a aby neprijímal pakety odkiaľ nemá | - Ak nie je používaný na veľkej firemnej sieti, bude používaný len na špecifických zariadeniach.  - Nezašifruje žiadne pakety, ktoré počítač posiela. | - Firewall je spoľahlivý spôsob ako ochrániť osobné zariadenie na internete, avšak má limitácie, ktoré pomáha vyplniť VPN sieť. |
| VPN | - Je ľahko expandovateľná.  - Môže byť neustále zapnutá.  - Šifruje údaje medzi zariadeniami.  - Ochraňuje lokáciu, IP adresu, históriu užívateľa a používané zariadenie. | - Oslabená šifra pri pripájaní sa na server.  - Je možné, že si poskytovateľ uchováva informácie o používateľoch, ktoré môže potom predať ďalej.  - Nezabráni niekomu od poslúchať pakety, ak vie dešifrovať šifru. | - VPN sieť je skvelý nápad, ktorý je používaný na profit bez žiadneho spôsobu, ako overiť jeho spoľahlivosť. Jeho efektivita záleží podľa poskytovateľa a podľa toho, ako moc mu veríte. |

1. Produkt

Podarilo sa mi spraviť prezentáciu pripravenú ako edukačný materiál. Cieľom bolo dať ľudom možnosť sa naučiť niečo nové a užitočné. Z dokumentačných dôvodov by som chcel rozobrať môj proces pri tvorbe tohto projektu.

* 1. Myšlienka

Celý projekt začal myšlienkou ochrany a bezpečnosti na internete. Bol som dosť inšpirovaný hodinami počítačovej vedy, kde sme preberali, aj keď len zľahka oproti nejakému sieťarskému odboru, sieťové technológie a veľkým počtom reklám, ktoré bolo nemožné si nevšimnúť, všetky rozprávajúce o VPN-kách a Firewalloch. Chcel som nielen aby to bolo niečo z témou internetovej bezpečnosti, ale aby to bolo aj niečo dostatočne komplexné, nech sa mi oplatí naučiť sa o danej téme vo voľnom čase. Popravde mi to prišlo ako zaujímavá látka, ktorú som nikdy neskúsil študovať aj keď som celkom dosť chcel.

* 1. Prezentácia

Na môj produkt som si vybral učebný materiál, práve pretože som sa cítil sebavedomo o tvorení niečoho, z čoho by sa mohli iný ľudia niečo naučiť. Rozhodoval som sa medzi tvorením semi-dokumentácie na celú túto látku a dizajnovaním prezentácie, ako nám tvoria, alebo nájdu, naši učitelia. Nakoniec som sa rozhodol, že učebný materiál bude prezentácia, ktorá preberie hlavné myšlienky tejto témy tak, aby sa z nej mohol naučiť aj niekto mimo školy. To znamenalo, že text by nemal byť moc komplexný a nemalo by ho tam byť až moc veľa, ak by zas text bol moc krátky alebo moc zjednodušený na to, aby sa z neho dalo niečo užitočné naučiť, musel by som celý produkt prerábať. V poslednej dobe som taktiež viacej experimentoval z prezentáciami, čo som chcel už dlhšiu dobu a tento učebný materiál bol hlavný motivátor, prečo som sa v PowerPointe začal viacej realizovať.

* + 1. Obsah prezentácie časť 1

Obsah prezentácie je nakoniec tvorený desiatimi stranami náučného textu. Rozdelil som ho na dve hlavné časti, generálne a viacej upresnené informácie. Prvý slide uvádza názov učebného materiálu “Bezpečnosť na internete”, rovnako ako aj meno autora, mňa. Aby čitateľ mohol aspoň približne zistiť čo sa môže potenciálne naučiť, na druhom slide nasleduje obsah prezentácie.

* + 1. Obsah prezentácie časť 2

Prvá strana s edukačným textom otvára z privítaním čitateľa, teda úvodom do prezentácie. Spomínam tam, ako používatelia internetu môžu byť v nebezpečenstve bez ich vedomosti. Snažil som sa tak nalákať čitateľov k tomu, aby pokračovali čítať ďalej. Nepovedal som tam žiadne klamstvo a dúfal som, že ak bol niekto zaujatý prvou stranou s informáciami o učebnej látke, že bude čítať ďalej. Tam už môžem začať rozprávať dôležitejšie informácie. Dal som si do hlavy metódu písania informácií, ktorú som v písaní produktu nakoniec aj využil. Išlo mi o to informácie stupňovať podľa dôležitosti a podľa toho aké boli komplikované. Učebná látka by mala byť, v ideálnom svete, zaujímavá a komplexná akurát tak, aby sa čitateľ nad ňou zamyslel bez toho, aby ho to preťažilo alebo aby stratil záujem. Z mojich skúseností viem, že ľudia sú prirodzene zvedaví a chcú sa učiť nové veci. Mohol som dať všetky informácie zo strán 3-5 do jednej strany a  ušetriť tak asi ich počet, alebo som mohol rozobrať tie informácie omnoho viac dopodrobna. Problém s týmito prístupmi je ten, že podľa mňa to preťaží čitateľov. Predstavte si ako sa vám niekto pokúsi vysvetliť vysoký stupeň z odborného učiva ako je napríklad matematika. Priemerná osoba bude potrebovať viac len ako rýchle vysvetlenie aby sa to nielen naučila, ale aby tomu aj pochopila. S Učebným textom to je podobné. Ak preťažím čitateľa s ťažkým textom, nielen že stratí záujem, ale nepochopí pointe textu aj keď sa ho naučí naspamäť.

* + 1. Obsah prezentácie časť 3

Po tom ako som napísal o dôvodoch na čítanie mojej prezentácie v úvode, mal som na výber pokračovať o Firewall, alebo VPN. Moje rozhodnutie pokračovalo s textom o Firewalloch, pretože aj keď som o tom napísal viacej strán v produkte, pointa bola podľa mňa lepšie vysvetlená. S Firewallmi som chcel vysvetliť, že filtrujú čo počítač môže poslať a čo prijať. Prípadne takto môžu fungovať aj na sieti. S VPN to bolo zložitejšie, keďže si sám nie som istý koľko všetci tí ľudia, ktorí o tom toľko v online fórach a YouTube reklamách vedia o tom čo tam povedia. Strašne veľa sa o tom diskutuje ale nevedel som moc nájsť viac ako len veci o tom ako to je tunel medzi vami a dákym zahraničným serverom, alebo ako je všetko magicky zašifrované. Aj keď ma to dosť hnevá, nič moc som o tom nespomenul, keďže väčšinu ľudí veci ako spôsob, ktorým tá šifra funguje či ktoré vecí si môže server potenciálne zapisovať nezaujíma. Áno opakujem sa, ale je podľa mňa dosť ľahké stratiť čitateľov kôli textu, ktorý je moc zložitý alebo dlhý. Tá časť textu by skončila zbytočne dlhá, pretože viem že by som neprestal písať.

* 1. Dizajn

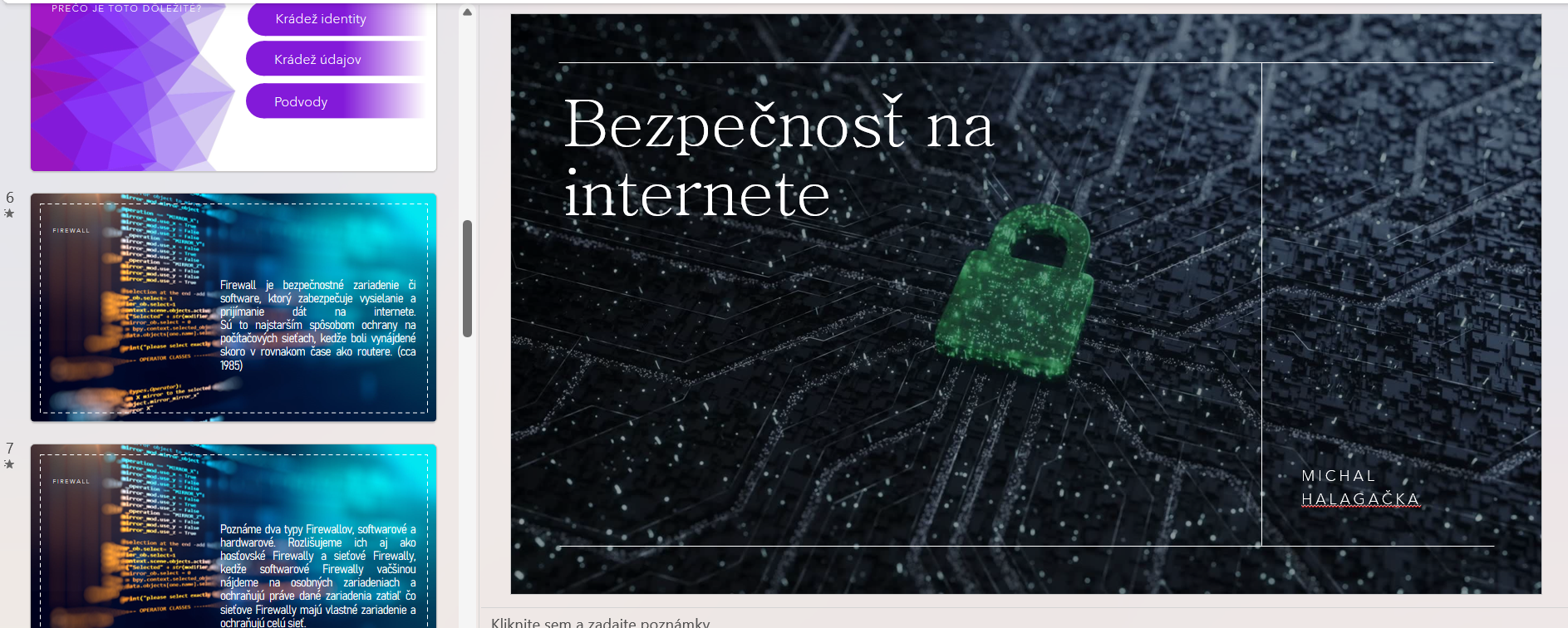
Dizajn prezentácie som robil dva razy. Pôvodne môj produkt vyzeral futuristicky a narozdiel od dnešného dizajnu, všetky strany mali ten istý motív a pozadie. Mal som tam spravené komplexné animácie, ale boli zle implementované. Príkladom bolo občasne myklo textom, alebo nesprávne pohnutie objektom. Avšak najväčší problém bol, v zlých objektoch. Nedalo sa mi s nimi efektívne pracovať ďalej a preto som sa rozhodol to celé prerobiť. Bola bolesť celý produkt prerábať, ale bolo to niečo, čo som musel spraviť. Stará prezentácia bez animácií vyzerala ako niečo, čo niekto hodil do kopy za 10 minút a za to by som sa hanbil.

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

Automaticky generovaný popis

Obr. 1 Stará prezentácia

Nakoniec som rád, že som sa rozhodol ju prerobiť. Momentálny produkt je výzorom o dosť zaujímavejší a ide z neho viacej energia náučného materiálu.



Obr. 2 Nová prezentácia

* + 1. Postup pri dizajne

Pôvodne som nevedel, ako by som chcel, aby môj druhý produkt vyzeral. Ako pri skoro každej prezentácií som napísal text, ktorý chcem na snímke použiť, bez žiadneho dizajnu. Potom som použil PowerPointovú funkciu ‚Návrhár‘ aby som dostal základný nápad na dizajn snímky, ktorý potom upravím aby bol použiteľný s už napísaným textom. Rozhodol som sa tematicky rozdeliť prezentáciu na tri časti podľa obsahu textu. Toto rozhodnutie som spravil, aby bola každá časť z prezentácie ľahšia na zapamätanie. Je ľahšie si spomenúť na niečo, keď si to dokážete vizuálne vybaviť.

* + 1. Detaily

Je tam veľa detailov, ako v práci každého zaujatého tvorcu, takže spomeniem len niektoré veci, ktoré sa mi fakt páčia. Chcel som sa vyhrať s animáciami a prechodmi, aj keď nie až tak ako v prvej prezentácií. Zároveň som chcel aby boli viacej oddelené všetky 3 tematické časti prezentácie, preto každá prvá strana tematickej časti má prechod, kde odsúva predošlú stranu. Aby si toto čitateľ všimol, všetky strany s textom používajú ako prechod ‚morfovanie‘. Ďalej chcem spomenúť malý detail pri Firewall časti prezentácie, kde kôli malému nadpisu kapitoly a podkapitoly som použil podčiarknutie hneď ako prejdeme z celkových informácií do podrobnejších. Taktiež som chcel aby sa prezentácia držala tematicky pokope aj napriek rozličným štýlom všetkých kapitol. Celkom som spokojný s tým ako sa mi to podarilo. Vo Firewall časti to najviac upadá, ale je to taktiež aj najviac zapamätateľná časť prezentácie, takže som s tým v poriadku.

1. Záver

Pri bezpečnosti na internete sú z môjho názoru dôležité mať aj Firewall a aj VPN. Aj keď Firewall dokáže filtrovať čo je poslané z vášho zariadenia na internet a naopak, nezabráni cudzím ľudom, aby sledovali čo na internete robíte. S Firewallom mám kľudnejšiu myseľ ako pri VPN, keďže filtrujú údaje a nikam ich neposielajú. Hlavný ciel je vyhodiť veci, ktoré by mohli poškodiť zariadenie, alebo ukradnúť údaje. Zasa pri VPN je názor ľudí rozdelený na dve strany. Na jednej vravia, že by malo byť povinné používať ich a na druhej vravia, že tvoria ďalšiu slabinu pri komunikácií medzi dvoma zariadeniami. Z toho čo viem, cieľom VPN je hlavne zašifrovať údaje, ktoré niekto posiela na internet tak, aby ich tretia strana nedokázala odpočúvať. Problém nastáva, keď by niekto chcel posielať šifru na server stránky, pretože by to nemalo ako fungovať bez medzikroku, ktorý rozšifruje správu. Ako som vravel, podľa mňa záleží na dôvere voči dodávateľovi prístupu na VPN. Ohľadom tohto projektu, aj keď som bol najskôr dosť nespokojný so svojou prácou a témou, zapáčila sa mi. Dosť sa mi páči fakt, že som vytvoril niečo prínosné a niečo sa naučil. Aj keď na začiatku vyzeral produkt dosť zle a bola bolesť ho prerábať, páči sa mi ako dopadol. Nemám moc čo viac povedať.

Zoznam použitej literatúry

1. What is a Firewall 🡪 CISCO, Použité na komplexnejšie témy a na typy Firewallov, dostupné dňa [30.4.2024] na stránke: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
2. What is a Firewall 🡪 Fortinet, Použité všeobecne, dostupné dňa [30.4.2024] na stránke: <https://www.fortinet.com/resources/cyberglossary/firewall>
3. What is a Firewall 🡪 CheckPoint, Použité na históriu Firewallov, dostupné dňa [30.4.2024] na stránke: <https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/>
4. Understanding Firewalls for home and small office use 🡪 CISA, Použité na rozdelenie Firewallov na hardware a software, dostupné dňa [30.4.2024] na stránke: <https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use>
5. What is a Firewall? - Definition & Explanation 🡪 Kaspersky, Použité všeobecne, dostupné dňa [30.4.2024] na stránke: <https://usa.kaspersky.com/resource-center/definitions/firewall>
6. VPN (Virtual Private Network) 🡪 TechTarget, Všeobecné informácie a typy VPN, dostupné dňa [30.4.2024] na stránke: <https://www.techtarget.com/searchnetworking/definition/virtual-private-network>
7. What is a VPN? Meaning, Benefits, and How to Get One – CGP Holdings, Informácie o hackeroch a ako VPN chráni údaje, dostupné dňa [30.4.2024] na stránke: <https://whatismyipaddress.com/vpn-explanation>
8. Virtual Private Network 🡪 TechoPedia – Margaret Rouse, Výhody a nevýhody VPN, dostupné dňa [30.4.2024] na stránke: <https://www.techopedia.com/definition/4806/virtual-private-network-vpn>
9. What is a VPN 🡪 Microsoft, Komplexné informácie o VPN, dostupné dňa [30.4.2024] na stránke: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn>
10. VPN Statistics And Trends In 2024 🡪 Forbes – Lauren Holznienkemper, Chauncey Crail, Použité na štatistiky v grafe, dostupné dňa [30.4.2024] na stránke: <https://www.forbes.com/advisor/business/vpn-statistics/>
11. Why is Internet security important? 🡪 Techwalla – Shea Laverty, Dôvody prečo na bezpečnosti na internete záleží, dostupné dňa [30.4.2024] na stránke: <https://www.techwalla.com/articles/why-is-internet-security-important>