VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

VIRTUÁLNÍ PRIVÁTNÍ SÍTĚ Z POHLEDU KYBERNETICKÉ BEZPEČNOSTI

Autor práce: Lukáš Mixa

Studijní program: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Prezenční

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Lukáš Mixa

Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Prezenční
Místo studia: České Budějovice

Název bakalářské práce: Virtuální privátní sítě z pohledu kybernetické bezpečnosti

Název bakalářské práce v anglickém jazyce: Virtual Private Networks from the Perspective of Cyber Security

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): Červen 2021

Cíl bakalářské práce:
Hlavním cílem bakalářské práce bude charakteristika virtuálních privátních sítí a jejich užití pro kybernetickou bezpečnost.
Vedlejším cílem bude zjistit, jakou znalost mají o virtuálních privátních sítích žáci středních a vysokých škol v Jihočeském kraji.

Vedoucí práce: RNDr. Růžena Ferebauerová	28.6.2021 *datum*	*podpis*
Student: Lukáš Mixa	28.6.2021 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	30.6.2021 *datum*	*podpis*
Prorektorka pro studium a vnitřní záležitosti: Ing. Štěpánka Petroušová	12.7.2021 *datum*	*podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	19.7.2021 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

Mixa, L. *Virtuální privátní sítě z pohledu kybernetické bezpečnosti: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 61s .Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: Kybernetická bezpečnost, Internet, Kyberprostor, Virtuální privátní sítě, Ochrana dat

Hlavním cílem bakalářské práce bude charakteristika virtuálních privátních sítí a jejich užití pro kybernetickou bezpečnost. Vedlejším cílem bude zjistit, jakou znalost mají o virtuálních privátních sítích žáci středních a vysokých škol v Jihočeském kraji

ABSTRACT

Mixa, L. Virtual Private Networks from the Perspective of Cyber Security*: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2022. 61s. Supervisor: RNDr. Růžena Ferebauerová

Key words: Cyber security, Internet, Cyberspace, Virtual private networks, Data protection

The main goal of the bachelor thesis will be the characteristics of virtual private networks and their use for cyber security. The secondary goal will be to find out what knowledge of high school and university students in the South Bohemian Region have about virtual private networks.

Obsah

Úvod

Bakalářská práce je zaměřena na téma virtuální privátní sítě z pohledu kybernetické bezpečnosti. Ty se ve světě stávají čím dál více diskutovanějším tématem, obzvláště v dnešní době moderní techniky, kdy způsoby bezpečného a soukromého používání internetu stále více upadají. Vzhledem k tomu, že se stálé jedná o poměrně mladou problematiku, která dosud nebyla více komplexně zpracována, je cílem této bakalářské práce zabývat se daným tématem nejen z pohledu kybernetické bezpečnosti, ale i celkového zasazení do kyberprostoru. Za tímto účelem je proto nutné seznámit se s nejpotřebnější odbornou literaturou v oblasti kybernetického prostoru a kybernetické bezpečnosti. Dalším důvodem je, že výpočetní zařízení a moderní komunikační prostředky jsou součástí našeho života na každém kroku a jejich absenci si již nedokážeme představit.

Tato problematika je fenoménem dnešní doby. Poskytovatel internetových služeb se sice může zdát důvěryhodný, ale přesto je zde možnost, že předá historii prohlížení inzerentům. Mnoho uživatelů internetu používá veřejné připojení wi-fi, kde může snadno dojít k napadení uživatele hackery a mohou být ohrožena právě jejich osobní a soukromá data. Tyto problémy týkající se narušení soukromí nedokážeme zcela odstranit, nicméně se můžeme pokusit vyhnout případným nežádoucím vstupům do soukromí uživatelů.

Internet je v dnešní době místo, které je bezesporu nedílnou součastí snad každého z nás. Myslet si a spoléhat na to, že naše digitální stopa nikoho vlastně nezajímá a ani nám nemůže nikterak uškodit, by bylo pošetilé.

Vzhledem k tomu, že jsem studoval střední školu v oboru informační technologie, tak s touto problematikou mám již zkušenosti. Chtěl bych se proto tomuto tématu věnovat z osobního zájmu. Jsem přesvědčen, že mi toto téma poskytne mnoho nových informací a to nejenom z tohoto tématu, ale především získám větší povědomí o této problematice, což bych mohl využít ve svém životě.

1 Cíl a metodika bakalářské práce

Bakalářská práce se zaměřuje na virtuální privátní sítě. Toto téma je v dnešní době velmi aktuální, jelikož způsoby bezpečného a soukromého používání internetu stále více upadají, což se stává závažným problémem. V dnešním světě je ztráta, nebo odcizení citlivých osobních dat na internetu běžnou věcí. V rámci dané problematiky bude důležité poukázat na to, co virtuální privátní sítě představují, tedy stručně technické fungování, historie, kdo a jak jej používá a k čemu slouží.

Pro teoretickou část byla použita metoda rešerše literatury. Zde bude toto téma specifikováno obecně a budou popsány jednotlivé základní pojmy, které budou v bakalářské práci používány. Budou nezbytné pro pochopení virtuálních privátních sítí a jejich přínos pro kybernetickou bezpečnost, jako je představení VPN a její hardwarové a softwarové rozlišení. Dále je zcela nezbytné, aby čtenář znal pojmy jako je internet, kyberprostor, internetové protokoly, IP adresa, tunelování, Mac adresa a v neposlední řadě rizika v podobě hackingu. Jako další bude kapitola věnována právním aspektům, tedy zaměřena na legislativu kybernetické bezpečnosti České republiky, dále zpracovávání osobních údajů, Národní úřad pro kybernetickou a informační bezpečnost a legalita VPN jak v ČR, tak i v jiných zemích. V další části je zde historický vývoj virtuálních privátních sítí, následují uživatelé virtuálních privátních sítí a data ze světových statistik pro rok 2022. Na závěr zde budou komplexně popsány formy připojení virtuálních privátních sítí. Posledním tématem bude rozbor jejich kladů a záporů.

V praktické části bylo pro statistiky využita metoda dotazníkového šetření, při které byli žáci středních a vysokých škol v Jihočeském kraji dotazováni, zda podobné formy kybernetické ochrany užívají, popřípadě na kolik jsou s nimi obeznámeni. Na základě statistik bylo zjištěno, jaké zkušenosti mají žáci o virtualních privátních sítích. Čtenáře zde bude čekat stručné představení praktické části s formulací výzkumného problému bakalářské práce na téma “Virtuální privátní sítě z pohledu kybernetické bezpečnosti“ a jeho hlavní a dílčí výzkumné cíle. Dále budou k dispozici výzkumné otázky a hypotézy. Následovat budou metody výzkumu a sběru dat. V této kapitole budou s největší pravděpodobností k dispozici informace, jako zajišťování respondentů

a tvorba dotazníku. Další podrobné informace budou uvedeny i ve výzkumném souboru. Důležitou částí bude realizace výzkumu, jenž obsahuje důležité informace ohledně postupu získávání dat. Jako další by měl přijít způsob zpracování dat, kde bude potřeba seznámit čtenáře s užívaným softwarem k budoucí analýze dat, ve které bude jak graficky znázorněno, tak také písemně odpovězeno na každou z následně položených otázek. V závěru praktické části bude čtenáři k dizpozici interpretace dat, ve které díky odpovědím od respondentů bylo odpovězeno na předem stanovené hypotézy H1:Virtuální privátní sítě užívají pro svou bezpečnost více muži než ženy. H2: Uživatelé nevyužívají VPN ačkoli chtějí mít zabezpečená data H3: Žáci středních škol mají menší povědomí o problematice virtualních privatních sítí, než žáci vysokých škol

2 Základní pojmy

Tato kapitola obsahuje vysvětlení některých základních pojmů, které budou v bakalářské práci používány. Tyto jsou nezbytné pro pochopení virtuálních privátních sítí a jejich přínosu pro kybernetickou bezpečnost. Virtuální a privátní síť je z pohledu kybernetické bezpečnosti velmi diskutovaným tématem, protože soukromí na internetu je jeden z nejzávažnějších problémů současnosti. Použité pojmy proto vycházejí z technického prostředí a jsou nezbytné k plnému porozumění jak virtuálních privátních sítí a jejich možností, tak i lepší orientace v kybernetickém prostředí.

2.1 Představení virtuální privátní sítě

Virtuální privátní síť, nebo také jen VPN, je tedy rozšíření privátní sítě, která zahrnuje propojení napříč veřejnými, nebo sdílenými sítěmi, čímž je především internet. Díky virtuální privátní síti je možné posílat data mezi dvěma počítači přes veřejnou, nebo sdílenou síť a to způsobem, který napodobuje vlastnosti soukromého propojení typu point-to-point, což je jeden z hlavních síťových protokolů, které se používají pro tunelování PPTP k vytvoření virtuální privátní sítě a tunelů mezi nimi. Tímto způsobem je provoz mezi jednotlivými sítěmi chráněn. Průběh konfigurace a vytvoření VPN je známé jako virtuální privátní síť.[1]

2.1.1 Hardware

Dostál ve své knize tvrdí, že etymologický původ termínu hardware, který nyní najdeme jednoznačně v anglickém jazyce spočívá v tom, že se skládá ze spojení dvou slov anglického jazyka hard, které lze přeložit jako tvrdé a ware, které je synonymem pro věci. Definuje hardware jako soubor komponentů, které tvoří hmotnou část počítače. Na rozdíl od softwaru, který odkazuje na nehmotné komponenty. Některé příklady hardwaru zahrnují grafickou kartu, tiskárnu, monitor počítače a pevný disk. Pro hardware je důležité poskytnout softwaru platformu, na které může fungovat. Dokud není plně funkční hardware, nemůže fungovat ani software. Software a hardware vzájemně interagují při plnění úkolů. Bez těchto dvou komponentů nemůže počítačový systém efektivně fungo-

[1] Představení VPN. *Geeksforgeeks* [online]. [cit. 2021-12-10]. Dostupné z: https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/

vat. Hardware je tedy platforma potřebná ke spouštění a ukládání softwaru. Software na druhé straně shromažďuje pokyny od uživatele.

Software neprovádí obecné úkoly. Každý software provádí úkoly na základě připojeného hardwaru. Některé typy hardwaru zahrnují ovládání, zpracování, ukládání, výstup a vstup, zatímco software zahrnuje aplikační software, programovací software a systémový software.[2][3]

Hardwarová virtuální privátní síť je zařízení k tomu určené. Má tedy možnost poskytnout funkce virtuální privátní sítě zařízením, jako jsou mobilní telefon, tablet, nebo počítač. Mezi tato zařízení patří některé routery, které mají vestavěné funkce pro poskytování virtuální privátní sítě. Lze k nim tedy přistupovat jako k hardwarovému vybavení. Toto hardwarové vybavení je postaveno tak, aby dokázalo pracovat přesně k tomu, k čemu bylo určeno, což je šifrování a dešifrování dat, která jimi procházejí díky specifickému procesoru. Hardwarové virtuální privátní sítě mají tu výhodu, že uživateli ulehčí od používání softwarových virtuálních privátních sítí. Jeho další výhodou je dnes již kvalitní vybavení v hardwarových virtuálních privátních sítích, zpravidla jde o bezpečné připojení SSL a firewall.[4]

2.1.2 Software

Software je často označován, a tedy snadno zaměnován, za počítačový program. Kolouch to ve své knize však vyvrací a uvádí, že pojmy software, počítačový program a programové vybavení jsou různé a dále je charakterizuje.

Software je programové vybavení a to všeho druhu. Jde o programové vybavení, které je potřebné k fungování počítače, jako jsou základní programy operačního systémů až po běžné aplikace. Z jistého úhlu pohledu to jsou veškeré informace, které jsou v počítači určitým způsobem někde uloženy. Dále je možné je dělit do dvou základních

---

[2] DOSTÁL, J. *Hardware moderního počítače*. Olomouc: Univerzita Palackého v Olomouci, 2011. s 6 - 9

[3] Hardware VPN. *Macpaw* [online]. [cit. 2021-12-10]. Dostupné z:https://macpaw.com/how-to/hardware-vpn-vs-software-vpn

[4] Hardware. T*cholidays* [online]. [cit. 2021-12-10]. Dostupné z:https://www.tcholidays.com/hardware-and-software-a-professionally-written-essay-sample

skupin podle způsobu jejich využití na data a programy. Počítačový program je chráněn autorským zákonem a jde tedy o soupis algoritmů v takovém tvaru, který systém dokáže zpracovat. Je možné jej charakterizovat jako komplexní soubor instrukcí, které počítač používá k provádění činnosti. Programové vybavení představuje programy, o které je daný hardware doplněn, aby bylo pro uživatele možné počítač vůbec použít. Jsou tedy nezbytně nutné k jeho užívání. Zahrnuje počítačové programy včetně softwaru. Jde o programy, postupy, pravidla, procedury a danou dokumentaci systému zpracování informací, nebo jejích částí“[5]

Pakliže se jedná o softwarovou virtuální privátní síť, jde o program, jenž je k dizpozici pro ruzná zařízení od telefonu, až po počítač. Softwarová virtuální privátní síť má za úkol připojit dané zařízení k VPN serveru. Softvarová virtuální privátní síť' tak může v této podobě poskytnout vizuální rozhraní pro vytvoření bezpečeného, šifrovaného spojení mezi zařízením a serverem. Tím jsou zařízení zašifrována a zabezpečena protokolem virtuální privátní sítě.[6]

2.2 Internet

Historie internetu sahá do 60. let minulého století, kdy se Spojené státy rozhodly, že chtějí novou komunikační síť, která by zprostředkovávala rychlou výměnu dat v nejrůznějších podmínkách. Hrozící jaderná válka byla vnímána jako jeden z důvodů tvorby nové komunikace. Tato komunikační síť byla navržena tak, aby spojovala země, města, nebo velitelská stanoviště pro bezproblémovou výměnu taktických informací.[7] Dále je internet třeba brát, mimo jiné, jako publikačního zprostředkovatele, kde může uveřejňovat kdokoli cokoliv. Internet není odpovědný žádnému síťovému centru. Uživatelé si mohou vybírat z nastavení od poskytovatele až po celkový obsah na obrazovce. Může plnit jak komunikační, informační, tak i komerciální úlohu a to je pouze zlomek. Internet může být zdrojem informací pro výzkum i prostorem pro hry. Internet lze tedy vní-

[5]KOLOUCH, J. Cybercrime. Praha, 2016, s. 62 – 63

[6]Software VPN. *Macpaw* [online]. [cit. 2021-12-10]. Dostupné z:https://macpaw.com/how-to/hardware-vpn-vs-software-vpn

[7] KRČMÁŘ, P. Linux: postavte si počítačovou síť. Praha, 2008, s. 20.

mat jako zprostředkovatele publikací, kde může kdokoli publikovat cokoli [8] [9]

2.3 Kyberprostor

V informatice lze za kybernetický prostor považovat téměř každý systém s významnou uživatelskou základnou, nebo systém s dostatečně dobře navrženým rozhraním. Kyberprostor je možné vnímat a nahlížet na něho, jako na virtuální počítačový svět a to konkrétně jako na elektronické médium, používané k vybudování globální počítačové sítě pro usnadnění online komunikace. Jedná se o rozsáhlou počítačovou síť složenou z mnoha světových počítačových sítí, které pro podporu komunikace a výměny dat využívají protokol TCP/IP.[10]

2.4 IP adresa

IP adresa je jedinečná adresa, která identifikuje zařízení na internetu, nebo v místní síti. IP je zkratka pro „Internet Protocol“, což je soubor pravidel upravujících formát dat odesílaných přes internet, nebo místní síť. V současné době existují dvě verze internetového protokolu IPv4 a IPv6. IPv4 používá 32 bitové schéma adres, které umožňuje uložit 2^{32} adres 4,29 miliardy adres. IPv6 je 128bitová adresa IP, která podporuje celkem 2^{128} internetových adres. Použití IPv6 nejen řeší problém omezených zdrojů síťových adres, ale také řeší překážky pro připojení více přístupových zařízení k internetu.

IP adresy jsou v podstatě identifikátorem, který umožňuje posílání informací mezi zařízeními v síti. Obsahují informace o poloze a zpřístupňují zařízení pro komunikaci. Internet potřebuje způsob, jak odlišit různé počítače, routery a webové stránky. IP adresy poskytují způsob, jak toho dosáhnout a tvoří nezbytnou součást fungování internetu. Všechny počítače světa v internetové síti spolu komunikují pomocí podzemních, podvodních kabelů, koaxiálních kabelů až po bezdrátové připojení. Pokud je potřeba

---

[8] SKLENÁK, V. Data, informace, znalosti a Internet. Praha, 2001, s. 10.

[9] KMOCH, P. *Informatika a výpočetní technika: pro základní školy*. Praha: Computer Press, 1997. s. 128

[10] Kyberprostor. *Technopedia* [online]. [cit. 2022-1-20]. Dostupné z:https://www.techopedia.-com/definition/2493/cyberspace

stáhnout soubor z internetu, nebo načíst webovou stránku, či doslova dělat cokoli souvisejícího s internetem, počítač musí mít adresu, aby ostatní počítače mohly najít a lokalizovat dané zařízení a tím tak doručit konkrétní soubor, nebo webovou stránku, kterou žádá.[11] [12]

2.5 MAC adresa

MAC adresa je fyzická adresa, která jednoznačně identifikuje každé zařízení v dané síti. Mac adresu je možné rozdělit na dvě poloviny. První polovinu musí výrobce získat od centrálního správce adresního prostoru. Tato část je u všech karet daného výrobce totožná, nebo alespoň u velké skupiny karet, větší výrobci mají k dispozici několik hodnot pro první polovinu. Následně pak výrobce každé vyrobené kartě či zařízení přiřazuje jedinečnou hodnotu druhé poloviny adresy. Tato přímočarost velmi usnadňuje kooperaci lokálních sítí a novou kartu lze tak zapojit a spolehnout se na to, že bude snadno identifikována. MAC adresa je tedy přidělena výrobcem vašeho zařízení a jde tedy o identifikátor zařízení, který virtuální privátní sítě nemění. Virtuální privátní síť skryje podrobnosti o poloze, nicméně aby bylo možné připojení k internetu, musí být MAC adresa zařízení viditelná. Pokud je však potřeba před připojením skrýt, nebo změnit MAC adresu, jsou k dispozici nástroje pro změnu MAC adresy.[13]

2.6 Tunelování

Tunelování je proces, kterým pakety virtuálních privátních sítí dosáhnou zamýšleného cíle. Jde o procesy zapouzdření, směrování a konečné odpouzdření. Tunel je tedy brán jako logická trasa, která emuluje připojení Point-to-Point síťového spojení. Veškeré informace o zařízení jsou uvnitř tohoto tunelu skryty a to jak před zdrojem, tak před cílem. Tunelování může být zajištěno různými transportními protokoly. Některé sady protokolů mají za úkol zapouzdřovat šifrované pakety, zatímco jiné mají za úkol přenášet data v tunelované síti. Třetí protokol lze použít v záhlaví šifrovacího protokolu a ob-

---

[11] JIRÁSEK, P., NOVÁK, L., POŽÁR, J., Cyber security glossary, Praha, 2015, s.104

[12] IP adresa. *Geeksforgeeks* [online]. [cit. 2022-1-20]. Dostupné z: https://www.geeksforgeeks.org/what-is-an-ip-address/

[13] MAC adresa. *Alphr* [online]. [cit. 2022-2-9]. Dostupné z:https://www.alphr.com/does-using-a-vpn-change-your-mac-address/

sahuje informace o adrese paketu. Satrapa uvádí, že se uživatelé s tunelováním v počítačových sítích setkávají celkem běžně a to ve stádiích, kdy je pořeba tunelovat IPv6 datagramy pro průchod IPv4 sítí. Stejně tak je myslitelný i obrácený postup.

Některé virtuální privátní sítě umožnují rozdělené tunelování, nebo-li split tunneling. To uživatelům umožnuje zároveň komunikovat jak přes virtuální privátní sítě, tak i přes internet. Pakliže možnost rozděleného tunelování není k dispozici, je veškerý uživatelký provoz směrován přes klasické tunely. Hlavním rozdílem mezi plným tunelem a rozděleným tunelování je ten, že plný tunel používá virtuální privátní sítě uživatelů pro veškerý provoz, zatímco rozdělené tunelování znamená odesílání části provozu přes virtuální privátní sít' a část přes otevřenou síť. To znamená, že úplné tunelování je bezpečnější, než rozdělené tunelování, protože šifruje veškerý uživatelský provoz, nikoli jen jeho část.[14] [15]

2.7 Síťové protokoly

Síťové protokoly jsou souborem pokynů upravujících výměnu informací jednoduchým, spolehlivým a bezpečným způsobem. Jsou to formální standardy a zásady složené z pravidel, metodologie a konfigurací, které definují komunikaci mezi dvěma, nebo více zařízeními v síti. Aby bylo možné efektivně odesílat a přijímat informace, musí zařízení na obou stranách komunikační výměny dodržovat protokoly. Každá velká data odeslaná mezi dvěma síťovými zařízeními jsou rozdělena na menší pakety základním hardwarem a softwarem. Každý síťový protokol definuje pravidla pro to, jak musí být jeho datové pakety organizovány specifickými způsoby podle protokolů, které síť podporuje. Existuje spousta protokolů pro virtuální privátní sítě, ale nejběžnější jsou, Transport Layer Security TLS, Internet Key Exchange IKEv1 nebo IKEv2. Point-to-Point Tunneling Protocol PPTP, IP Security IPSec, Layer 2 Tunneling Protocol L2TP, WireGuard a OpenVPN. S neustále se vyvíjejícími službami VPN protokoly rychle za-

[14]SATRAPA,P. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: 2011. s 252

[15]Tunelování(2). *Cybernews* [online]. [cit. 2022-1-20]. Dostupné z::https://cybernews.com/what-is-vpn/split-tunneling/

starávají a do odvětví vstupují nové.[16] [17]

2.7.1 Protokol TCP/IP

TCP/IP transmission control protocol a Internet Protocol je seskupení protokolů datové komunikace. Pojmenován je podle dvou protokolů, které jej tvoří, TCP neboli Transmission Control Protocol a IP, nebo-li Internet Protocol. Model TCP/IP je výchozím způsobem datové komunikace na internetu. Rozděluje zprávy na pakety, aby se nemusely znovu odesílat celé zprávy v případě, že během přenosu narazí na problém. Pakety jsou automaticky znovu sestaveny, jakmile dosáhnou svého cíle. Každý paket se může ubírat jinou cestou mezi zdrojovým a cílovým počítačem v závislosti na tom, zda se původní použitá trasa stane přetíženou, nebo nedostupnou.[18]

2.7.2 Protokol IPsec

IPsec zkratka pro Internet Protocol security je sada internetových bezpečnostních protokolů určených k ochraně datových paketů odeslaných přes IP. IPsec používá šifrování k zaručení soukromí odesílaných dat a k ověření, že je čtou pouze jejich legitimní příjemci, což brání třetím stranám v přístupu k nim. IPsec je jedním z preferovaných protokolů pro ochranu dat odeslaných přes internet. IPsec obsahuje sadu kryptografických protokolů pro zabezpečení toku paketů, zajištění vzájemné autentizace a nastavení kryptografických parametrů.[19]

2.7.3 Protokol PPTP

PPTP nebo Point-to-Point tunneling Protocol je protokol používaný k vytváření virtuálních privátních sítí přes Internet. PPTP nemá za funkci šifrování, nebo ověřování a spoléhá na protokol Point-to-Point, jenž je následně tunelován. PPP protokol definuje, jak

---

[16]Protokoly(1). *Geeksforgeeks* [online]. [cit. 2022-1-20]. Dostupné z:https://www.geeksforgeeks.org/types-of-internet-protocols/

[17]Protokoly(2). *Tomsguide* [online]. [cit. 2022-1-20]. Dostupné z: https://www.tomsguide.com/features/how-does-a-vpn-work

[18]MCCARTHY, L a WELDON-SIVIY D, ed. Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online. Praha: 2013 s 239

[19] SATRAPA, P. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: 2011. s 199

jsou data a informace zapouzdřena v rámci datového spoje dále. Pro kontrolu využívá zpravidla 16 nebo 32 bitů z důvodu kontroly datového rámce, zda nebyl během přenosu poškozen. Učel protokolu PPP je zpřístupnít po jedné lince přenos více síťových protokolů najednou.[20]

2.7.3 Protokol TLS

Zkratka TLS tedy Transport Layer Security a SSL pro Secure Socket Layer je vlastně starší verze TLS. Oba jsou šifrovacími protokoly pro přenosovou vrstvu internetu. Jejich úkolem je šifrovat datové toky mezi klientem a serverem. Když je komunikace prováděna prostřednictvím této šifrované transportní vrstvy, je k názvu protokolu připojeno HTTP, jenž se změní na HTTPS.[21][22]

2.8 Hacking

V současném smyslu bychom mohli hacking definovat jednoduše, jako proniknutí do počítače, nebo řídicího systému jiným způsobem, než je standardní metoda. Hacker používá různé hardwarové, nebo softwarové nástroje k nabourání se do počítače, nebo řídicího systému. Hacking lze rozdělit na dva typy. Nelegální a etické hackování.

Při nelegálním hackování hacker pracuje na vybraných cílech s pomocí hardwarových a softwarových nástrojů. Obvykle se utěšuje pozitivním obcházením, prolomením bezpečnostních ochran počítače, nebo řídicího systému bez motivu finančního zisku. Tato činnost je prováděna pro jeho uspokojení. Hackeři v současné době preferují jiný nástroj v podobě toho, co je známé jako sociální inženýrství. V takovém případě se snaží oklamat svou předem vybranou oběť, aby zcela ochotně poskytla své přihlašovací údaje ke konkrétnímu účtu, díky čemuž tak hacker jednoduše získá heslo, které si následně uloží. Hacker se k sociálnímu inženýrství dostává především přes sociální sítě, kde se snaží pod smyšleným příběhem, či identitou buď odcizenou, nebo fiktivní, okla-

---

[20] KABELOVÁ, A a DOSTÁLEK L. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008.s 82

[21] KABELOVÁ, A a DOSTÁLEK L. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008 s 369

SSL-TLS. Master [online]. [cit. 2022-6-6]. https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod/

mat konkrétní vybranou oběť tak, aby jim uvěřila a jednoduše odhalila své přihlašovací údaje. V některých případech také využívá chyby obětí, které v dobré víře zveřejnily důležitá data, ale může se jednat o data, která by měla být před veřejností důvěrná, protože se může jednat o osobní, nebo obchodní tajemství.

Etický hacking spočívá v tom, že profesionální hacker za úplatu prostřednictvím například formou penetračních testů testuje komerční produkt s cílem vyhledat slabinu počítačového, nebo řídícího systému v podobě nedostatečně vytvořené bezpečnostní ochrany. Při jejím zjištění tento poznatek předává objednateli, případně vytvoří a naprogramuje konkrétní záplatu tak, aby byl komerční produkt dostatečně bezpečnostně ochráněn. Tyto zjištěné informace o bezpečnostní hrozbě však nezneužije a neposkytne třetí straně. V opačném případě by se již jednalo o hacking nelegální a trestně právně postižitelný.[23]

2.9 Kybernetická bezpečnost

Na pojem kybernetická bezpečnost lze nahlížet ruznými způsoby, nicméně podle webu Vlády České republiky, ji lze obecně pojmout, jako obecnou ochranu sítí před kybernetickými útoky, což představuje i ochranu před hrozbami pro zachování bezpečnosti informací. vzhledem k tomu, že je Kybernetická bezpečnost stále relativně novou oblastí, je tedy naprosto nezbytné, pokusit se reagovat na konkrétní výzvy a to co nejrychleji. To je důvodem, proč se Česká republika a Evropská unie snaží nacházet nejnovější a nejefektivnejší řešení na tyto situace. Díky dobré koordinaci a kvalitní spolupráci na mezinárodní úrovni se tak velmi daří. Jak již bylo zmíněno, stále se jedná o jeden ze silně rozvíjejících se oborů. S určitou pravděpodobností zde může dojít na nové převratné technologie, jako je například umělá inteligence a kvantové počítače. Ty nicméně extrémně změní používání kryptografie, tedy i fungování virtuálních privátních sítí a dalších odvětví.[24]

---

[23] JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. s. 102.

[24]Kybernetická bezpečnost. *VládaČR* [online]. [cit. 2022-2-9]. Dostupné z:https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

3 Hranice kyberprostoru

Od doby, kdy byly počítače připojeny k internetu, zažívá kybernetická kriminalita nebývalý rozmach. Zde se objevují nová fakta. Nové typy důkazů a řada nových právních problémů. Kyberkriminalita je odborníky vnímána jako nový druh kriminality, i když do kybernetického prostředí přenáší drtivou většinu v současnosti známých a dobře popsaných forem kriminality. Implementace v kybernetickém prostoru je pro pachatele mnohem jednodušší, rychlejší a efektivnější, než ve fyzickém prostředí. Patří mezi ně hackování, DoS a DDoS útoky, botnet a další. Prostředí internetu má svá pravidla a vzorce lidského chování oproti reálnému prostředí a lidé se nechovají jako ve skutečném světě. Pro představu osoba, která by v obchodě nikdy neukradla CD s filmem, nemá žádný problém si film, který je chráněn autorskými právy stáhnou bez zaplacení. Dalším protiprávní jednání, kterého se dopouští, je rozšiřování a to jak mezi přáteli, tak prodejem. Podobných nepochopitelných vzorců chování v kybernetické kriminalitě existuje celá řada. To je důvod, proč je kybernetická kriminalita celosvětový problém.[25]

Jedním z prvních trestných činů spáchaných v kyberprostoru byly sabotáže. Ty byly prováděny pracovníky s cílem poškodit zaměstnavatele, nebo různými aktivisty, aby vyjádřili svůj nesouhlas s politikou. Jedna z těchto sabotáží byla provedena na tkalcovském stroji a to již v 19. století jejich poškozováním a ničením děrných štítků.[26] Extrémní rozšíření informačních a komunikačních technologií přineslo společnosti silný smysl a dopad, který se snad projevil ve všech aspektech lidského života. Internet dříve býval spíše uzavřenou sítí akademiků a intelektuálů, ale tomu už tak není a stal se každodenním, široce užívaným nástrojem společnosti. Do takové míry je zcela přirozené, že neetické chování v kyberprostoru začalo mít skutečné a reálně hmatatelné důsledky v offline světě. Tyto důsledky přichází právě v traumatické události, způsobené možnou ztrátou velice citlivých dat a jejich zneužití proti uživateli. Každý člověk tuto událost prožívá jinak, a proto začala být potřeba celou tuto problematiku uchopit a právně ji re-

[25]KOLOUCH, J. Cybercrime. Praha, 2016, s.205.

[26]YONAZI, J. J., SEDOYEKA, E., ARIWA, E., EL-QAWASMEH, E. e-Technologies and Networks for Development. Heidelberg, 2011, s. 172.

gulovat.[27] [28]

Dle Šulce vzhledem ke zhoršujícímu se vývoji kyber-kriminality v ČR byli zákonodárci nuceni zavést náležitá opatření. Proto byl vydán zákon 181/2014 Sb., o kybernetické bezpečnosti. Rovněž byla vydána vyhláška s ním související č. 316/2014 Sb., o bezpečnostních opatřeních, reaktivních opatřeních, kybernetických bezpečnostních incidentech a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Tato vyhláška definuje hlavní povinnosti subjektů, které významný informační systém nebo kritickou informační infrastrukturu provozují. Dle vyhlášky č. 317/2014 Sb. lze za informační systém, považovat orgán veřejné moci, který je organizační složkou státu, krajem, nebo hlavním městem Praha, využívaný k zajištění např. elektronické pošty. Je-li určena k použití v rámci výkonu veřejné moci, nebo výkonu veřejné moci při přípravě na krizové situace a jejich řešení.[29]

Jak uvádí Glenny, je pro policii nejvetším problemém anonymita co se dodržování legislativy v online světe týče. Především pokud je člověk dostatečně schopný, používá internet opatrně a dokáže své zařízení maskovat fyzicky. Dále také autor v knize uvádí, že jsou využívány právě metody užití virtuální privátní sítě v kombinaci proxy serverů, jenž maskují IP adresu. Nicméně k tomuto nastavení je potřeba už větších schopnotí.[30]

3.1 Osobní údaje

Pod pojmem osobní údaje je možné zařadit zakladní informace, jako jsou jméno a příjmení, datum narození, rodné číslo, adresa bydlište, e-mailová adresa, telefoní číslo, ale také fotografie, pakliže lze vyfocenou osobu identifikovat a v neposlední řadě IP adresa. To vše jsou způsoby, jak je možné se dostat do soukromí osoby. Osobní údaje jsou

---

[27]ATKINSON, R. L. *Psychologie*. Vyd. 1. Praha: Portál, 2003. s 488-489.

[28]Právní aspekty. *Fakulta informatiky Masarykovy univerzity* [online]. [cit. 2022-2-9]. Dostupné z:https://is.muni.cz/do/ics/el/sitmu/law/html/pravni-aspekty.html

[29]ŠULC, V. Kybernetická Bezpečnost. Plzeň, 2018, s. 12

[30] GLENNY, M. *Temný trh: kyberzloději, kyberpolicisté a vy*. Praha: Argo, 2013. s. 13

pro uživatele internetu to nejcenější, a proto vešlo v platnost v květnu 2018 nařízení GDPR, tedy obecné nařízení o ochraně osobních údajů. V tomto nařízení bylo nutné jasně specifikovat všechny podstatné aspekty týkající se ochrany osobních údajů. Co se zpracování osobních údajů týče, jedná se o jakoukoli operaci zahrnující osobní údaje, od sběru, přes uložení, až po zničení. Cílem takto komplexních vymezení je co nejvíce chránit osobní údaje občanů Evropské unie. Přispívajícím faktorem je, že společnosti, které mají sídlo mimo EU, ale zpracovávají údaje na jejím území, se také musí přizpůsobit pravidlům EU. Za zpracováním údajů zpravidla stojí daný správce, nebo pracovník k tomu pověřený. V dnešním světe jsou osobní údaje vnímány jako měna, díky níž uživatelé mohou používat služby. Společnosti, jako jsou např. Facebook, nebo Google své příjmy musí někdě získávat. Společnosti díky potřebným údajům následně přesně ví, kdy využít osobní informace k poskytnutí vhodné reklamy.[31]

3.2 NÚKIB

Ústředním správním orgánem pro kybernetickou bezpečnost, včetně ochrany utajovaných informací v oblasti informační a komunikační technologie a kryptografické ochrany existuje Národní úřad pro kybernetickou a informační bezpečnost, nebo-li (NÚKIB). Sídlo Národního úřadu pro kybernetickou a informační bezpečnost je v Brně. Instituce byla zřízena 1. srpna 2017 novelou zákon č. 205/2017 Sb. zákona o kybernetické bezpečnosti, tj. zákonem č. 181/2014 Sb., ve znění pozdějších předpisů.[32] 20. března 2020 se stal ředitelem Národního úřadu pro kybernetickou a informační bezpečnost Karel Řehka.[33] Národní úřad pro kybernetickou a informační bezpečnost vykonává řadu činností v souladu se zákonem, což představuje například ukládání opatření, ukládání příslušných správních sankcí, dále ve stavu kybernetického nebezpečí působí jako koordinační orgán, zřizuje rekognoskaci, prevenci a metodickou podporu v kybernetické bezpečnosti a v daných částech ochrany utajovaných informací monitoruje a

---

[31] Osobní údaje. *Dtest* [online]. [cit. 2022-2-9]. Dostupné z:www.dtest.cz/clanek-8588/jak-je-to-s-osobnimi-udaji-na-internetu?subscribe=292

[32] č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění účinném k 1.9.2021 © AION CS 2010- 2019 [cit. 4. 5. 2022].Dostupné z: https://www.zakonyprolidi.cz.

[33] NÚKIB(1). *Centrumkyberbezpečnosti* [online]. [cit. 2022-2-9]. Dostupné z:https://centrum-kyberbezpecnosti.cz/novym-reditelem-nukib-se-stal-brig-general-karel-rehka/

analyzuje kybernetické rizika a hrozby.[34]

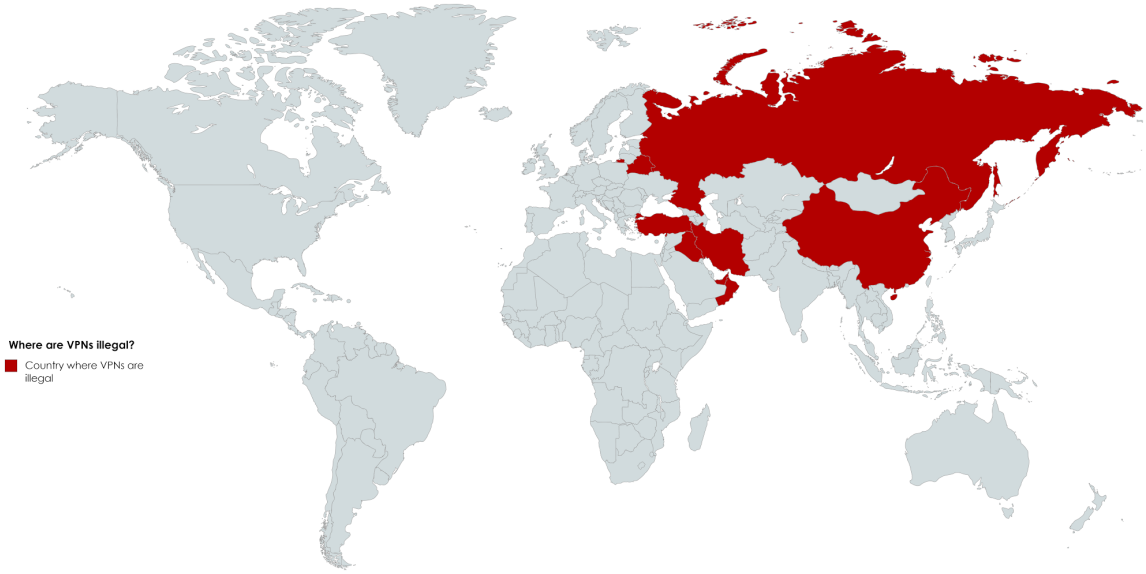
3.3 Užívání v České republice

Virtuální privátní sítě v České republice nelegální nejsou. Žádný zákon jejich používání nezakazuj. Uživatelé České republiky je tedy mouhou požívat ve svém zařízení. Pakliže nejsou používany například ke stahování obsahu chráněného autorskými právy, nebo k jiným ilegálním aktivitám, není důvod k obavám.[35]

3.4 Užívání ve světě

Přísné cenzurní zákony platí v zemích, jako je například Rusko, Čína nebo Írán, kde je použití jakýchkoliv virtuálních privátních sítí neschválených vládou nelegální. Nicméně ty, které jsou vládou schválené, bývají nedůvěryhodné a to z toho důvodu, že se řídí pravidly cenzury.[36]

Užívání ve státech OBR č.1[37]



[34]NÚKIB(2). *NÚKIB* [online]. [cit. 2022-2-9]. Dostupné z:https://www.nukib.cz/cs/o-nukib/

[35]Užívání VPN. *Vpnmentor* [online]. [cit. 2022-2-9]. Dostupné z:https://cs.vpnmentor.com/blog/vpn-101-vpn-prirucka-pro-novacky-od-vpnmentor/

[36]Užívání VPN. *Vpnmentor* [online]. [cit. 2022-2-9]. Dostupné z:https://cs.vpnmentor.com/blog/vpn-101-vpn-prirucka-pro-novacky-od-vpnmentor/

[37]Užívání ve státech OBRč1. *Vpnmentor* [online]. [cit. 2022-2-9]. Dostupné z:https://cs.vpnmentor.com/blog/jsou-vpn-legalni/

4 Historický vývoj virtuálních privátních sítí

Co se týče potřeby zabezpečit data uživatelů, ta tu byla již od vzniku internetu. Když Agentura pro obranné pokročilé výzkumné projekty vytvořila v 60. letech ARPANET, což byl předchůdce internetu, síť pro přepínání paketů, používali pro své sítě TCP/IP protokol, jenž počítače v tomto případě používaly ke komunikaci přes síť ARPANET. Ve své době zahrnoval hypertextové odkazy, HTML, FTP atd. a umožňoval tak přenos dat na velké vzdálenosti.

V roce 1983 se stal standardem pro americkou vojenskou komunikaci a v roce 1985 byl zaveden do komerčních počítačů, jako síť sítí, nebo-li internet. Snadná síťová konektivita poskytovaná protokolem TCP/IP byla rychle přijata velkými společnostmi, i když jejich stávající interní sítě byly značně odlišné. Zařízení připojená k internetu však nebyla zcela bezpečná, i když data mohla být snadno přenášena po síti, ten, kdo byl dostatečně zvědavý, mohl je zachytit, nebo dokonce vystopovat zpět ke zdroji. Při přenosu dat bylo málo soukromí, nebo bezpečnosti a brzy se ukázala potřeba bezpečného a soukromého internetu. V roce 1993 byl na základě výzkumu Johna Ioannidise představen softwarový IP šifrovací protokol SWIPE, nejstarší forma virtuální privátní sítě. To však bylo pouze experimentální a uživatelům sítě to jednoduše poskytlo autentizaci a důvěrnost. V roce 1994 byl vyvinut systém IPsec rozvoj IPsec a pokrok v rychlosti internetu je to, co vedlo k tomu, že se komerční virtuální privátní sítě staly realitou.

Poprvé bylo uskutečněno formou tunelovacího protokolu peer-to-peer, nebo-li PPTP v roce 1996, kdy zaměstnanec Microsoftu Gurdeep Singh Pall vyvinul první PPTP k vytvoření zabezpečeného spojení mezi internetem a počítačem. Dnes je viceprezidentem společnosti Microsoft. Jeho PPTP byl prvním krokem k moderním VPN a s nárůstem používání internetu v 90. letech 20. století byla mezi uživateli vysoká poptávka po zabezpečeném připojení. Byl přidán software, jako je antivirus, aby se zabránilo poškození uživatelských dat. Poptávka po internetové bezpečnosti však nadále rostla. PPTP od Gurdeep byla první virtuální privátní síť, která vytvořila bezpečnou síť mezi uživateli šifrováním dat a vytvořením tunelu přes LAN nebo WAN připojení. Díky tomu byl přenos dat přes soukromé i veřejné sítě bezpečný.

Uživatelé potřebovali k bezpečnému odesílání dat přes internet pouze přihlašo-

vací údaje a adresu serveru, a proto se dodnes používá jako známý a uživatelsky přívětivý systém virtuálních privátních sítí. Téměř na přelomu tisíciletí začaly korporace a podniky po celém světě používat PPTP a další formy virtuálních privátních sítí, aby zabránily úniku dat. Brzy se však veřejné používání internetu rozjelo. Nyní každý potřeboval virtuální privátní síť k zabezpečení internetového připojení. Když masy uživatelů začaly sdílet své osobní údaje přes internet, potřebovaly způsob, jak zabezpečit své soukromí a osobní údaje, a virtuální privátní sítě byly odpovědí. Tento nárůst poptávky vedl k dalším síťovým vylepšením a vývoji technologií virtuálních privátních sítí spolu s lepším a rychlejším připojením k internetu. To vše se spojilo a vytvořilo přizpůsobivější virtuální privátní sítě, které byly schopny pracovat rychleji a stát se řešením pro zabezpečení internetu v současnosti. Sloučení nových technologií s těmi stávajícími učinilo moderní virtuální privátní sítě všestrannější, flexibilnější a žádoucí pro všechny dnešní uživatele internetu. [38] [39] [40]

[38] Historie(1) VPN. *Csijax* [online]. [cit. 2022-2-9]. Dostupné z:https://csijax.com/a-brief-history-of-vpn/

[39] Historie(2) VPN. *Cactusvpn* [online]. [cit. 2022-2-9]. Dostupné z:https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/

[40] Historie(3) VPN. *Le-vpn* [online]. [cit. 2022-2-9]. Dostupné z:https://www.le-vpn.com/history-of-vpn/

5 Uživatelé virtuálních privátních sítí

Běžný uživatel Internetu se pohybuje pouze ve viditelné části. Uživatelé tedy nemají ve většině případů ani tušení, že se pohybují jen na špičce ledovce. Kyberprostor je pro běžného uživatele, tedy jen část internetu a tato část je nazývána Surface Web, nebo také viditelný web.[41] Virtuální privátní sít' umožňuje uživateli zašifrovat veškerý internetový provoz cestující do a z jeho zařízení a směrovat jej přes server v místě, které si uživatel zvolí. Virtuální privátní sít' v kombinaci se softwarem Tor dále zvyšuje bezpečnost a anonymitu uživatele, který se tak pokouší pracovat v neidexováném internetu.

Google indexuje pouze nepatrný zlomek internetu. Podle některých odhadů web obsahuje 500krát více obsahu, než kolik Google vrací ve výsledcích vyhledávání. Odkazy, které Google a další vyhledávače vrátí se nazývají jak již bylo zmíněno Surface Web, zatímco veškerý ostatní obsah, který nelze prohledávat bez příslušného softwaru, se označuje jako „hluboký web".

Dark web tvoří malý zlomek hlubokého webu. Dark web tvoří účelově skryté webové stránky a služby. Majitelé i uživatelé temného webu jsou anonymní. Lze zde nalézt mnoho internetových černých trhů, fór hackerů, prodejců malwaru a další nezákonné činnosti na druhou stranu je to místo, kde není nic cenzurováno a svoboda projevu je v nekterých zemích ohrožena, tak se uživatelé přesunou sem.[42]

Níže se podíváme na statistiky, které nám umožní nahlédnutí do toho, kolik uživatelů virtuální privátní sítě užívá, o jaké uživatele se zejména jedná a k čemu virtuální privátní sítě používají. Následující data vycházejí ze statistik z roku 2022. Informace, které z nich získáme jsou tedy aktuální. Počet uživatelů používající virtuální privátní sítě po celém světě, silně roste a pro rok 2022 nejsou ani žádné známky zpomalení. Díky její rostoucí popularitě však nyní existuje spousta různých poskytovatelů virtuálních privátních sítí, což je jeden z důvodů, proč je tak obtížné určit přesné číslo uživatelů virtuálních privátních sítí a jde tak o hrubý odhad. Uživatelů virtuálních privátních sítí je odhadem 1,2 miliardy a to z 5 miliard uživatelů internetu. Dále podle světových

---

[41] KOLOUCH, J. Cybercrime. Praha, 2016, s. 46-47.

[42] Deep web. *Comparitech* [online]. [cit. 2022-2-9]. Dostupné z:https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/

statistik k roku 2022 víme, že zhruba 62 % všech uživatelů virtuálních privátních sítí jsou muži. Starší generace k virtuálním privátním sítím nemá tak blízko, jako ta mladší. Přibližně tři čtvrtiny všech uživatelů, jsou mladší než 37 let. Nadpoloviční vetšina všech uživatelů virtuálních privátních sítí je používá k ochraně svého soukromí na veřejných Wi-Fi. Co se týče otázky na kterém zařízení jsou virtuálních privátní sítě využívány více, zda PC, nebo mobil, jde o teměř shodný výsledek. A jako poslední, více než 77 % uživatelů virtuálních privátních sítí, je využívá pro nákup digitálního obsahu, jelikož uživatelé díky změně geolokace ušetří.[43]

[43] Uživatelé VPN. *Dataprot* [online]. [cit. 2022-2-9]. Dostupné z:https://dataprot.net/statistics/vpn-statistics/

6 Formy virtuálních privátních sítí

Virtuální privátní sítě jsou nezbytným nástrojem jak pro mnoho podniků, tak i samotných uživatelů. Umožňují jim bezpečně rozšířit svou síť prostřednictvím veřejného připojení, jako je internet. Virtuální privátní sítě lze konfigurovat dvěma různými způsoby: Client-to-site a site-to-site. U obou těchto modelů existuje jasný rozdíl mezi koncovými body klientem a serverem.[44]

6.1 Client to Site

Virtuální privátní sítě typu Client-to-site se vytvářejí, když se zařízení, jako je iPhone, iPad, nebo notebook připojí zpět k podnikové síti prostřednictvím svého vlastního poskytovatele internetových služeb, nebo připojení jiného poskytovatele internetu na webu společnosti pro přístup k soukromým zdrojům. Klienti se obvykle připojují prostřednictvím protokolu RDP, zatímco pokročilejší konfigurace klientů mohou používat více protokolů, jako je PPTP a LNSAP. Tyto typy připojení jsou užitečné, když uživatelé potřebují vzdálený přístup k systémům v jejich soukromých sítích využívajících veřejné hotspoty Wi-Fi, mobilní datové sítě atd. bez připojení přes otevřené, nebo jinak nezabezpečené přenosové linky, jako jsou WAN připojení od externích poskytovatelů, zvláště pokud nejsou šifrována službami šifrování odkazů, jako je virtuální privátní síť'.[45]

6.2 Site-to-site

Model site-to-site poskytuje zabezpečené připojení mezi vzdálenými klienty a jejich privátními sítěmi pomocí nainstalovaného routeru, nebo jiného zařízení, které je nakonfigurováno, jako server virtuální privátní sítě na jedné straně WAN linky připojující se k perimetru podnikové sítě firewall. Klient se připojí zpět k tomuto zařízení s jiným nainstalovaným směrovačem, nebo jiným zařízením fungujícím jako jeho koncový bod. Ve virtuálních privátních sítích je veškerý provoz šifrován přes toto spojení proto-

---

[44] Formy VPN. *Paloaltoneworks* [online]. [cit. 2022-3-1]. Dostupné z:https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

[45] Formy VPN Client to site. *Rantdriven* [online]. [cit. 2022-3-1]. Dostupné z:https://rantdriven.com/the-difference-between-the-client-to-site-and-site-to-site-vpn-models/

kolem buď LNSAP/IP Sec nebo SSL přes TCP. Tento typ konfigurace uživatelům umožňuje plnou kontrolu nad jejich přístupovými body pro sofistikovanější bezpečnostní služby, jako je filtrování paketů, systémy detekce narušení atd., spolu s jakoukoli požadovanou úrovní sumarizace tras tam, kde to dává smysl ve větších podnicích [46]

[46] Formy VPN site to site. *Rantdriven* [online]. [cit. 2022-3-1]. Dostupné z:https://rantdriven.-com/the-difference-between-the-client-to-site-and-site-to-site-vpn-models

7 Možnosti ochrany

Hromadné využívání počítačů je možné díky technologickému pokroku a nástupu nových technologií, bohužel negativní stránka tohoto technologického pokroku je masivní nárůst počítačové kriminality. Smejkal v knize Kybernetická kriminalita datuje novou dobu kybernetické kriminality dvěma zásadními momenty, tím prvním momentem je nástup osobních počítačů, druhým pak vznik počítačových sítí a vzdáleného přístupu k počítačům. Ke zmíněným faktorům je zapotřebí přidat ještě poslední a to extrémně rychlý růst IT technologie a její vybavenosti mezi občany. Virtuální privátní sítě pomáhají uživatelům internetu chránit jejich soukromí, chránit jejich osobní údaje a získat anonymitu. Vytváří bezpečné soukromé síťové připojení k internetu směrováním internetového provozu uživatele přes servery virtuálních privátních sítí.[47]

7.1 Zabezpečení virtuálních privátních sítí

V životech uživatelů hrají čím dál tím větší roli sociální sítě, neustále se rozšiřuje sociální spektrum a uživatelé sociálních sítí začínají v digitálním světě žít další život. Na příklad neustálá potřeba být k dispozici na telefonu, patří mezi samozřejmosti. V opačném případě lidé trpí výčitkami svědomí, či se cítí nepatřičně. Jeden ze známých teoretiků Jan Jirák na jedné z jeho přednášek vyslovil myšlenku, že *"stálá dostupnost je vlastně vyžadována"*[48] a tato silná potřeba být k dispozici přináší mnoho rizik. Obvykle, když jsou uživatelé online, jejich poskytovatel internetových služeb je ten, kdo uživatelům poskytuje připojení, ale také je sleduje prostřednictvím IP adresy. Uživatelský webový provoz prochází skrz servery jejich poskytovatelů, tudíž se mohou přihlásit a vidět vše, co uživatelé dělají online. Na základě informací, které uživatelé generují se snaží firmy a společnosti využít velké množství lidí přítomných na sociálních sítí pro cílenou reklamu. Zajímavé informace, například co a kdy publikovat, lze totiž vyvodit z analýz dat. Virtuální privátní sítě se primárně používají, protože mohou chránit jakákoli data v jakémkoli komunikačním kanálu, který může online uživatel používat. Virtuální privátní sítě jsou také například účinné při skrytí IP adresy zařízení, když je zaří-

[47] SMEJKAL, V. Kybernetická kriminalita. Plzeň, 2018, s. 103.

[48]ECKERTOVÁ, L. a D. DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013. s 22

zení připojeno k internetu. Stále větší část uživatelů internetu používá virtuální privátní sítě k obcházení omezeného obsahu, blokovaných webových stránek a cenzurních programů.[49] [50]

7.1.1 Zabezpečení veřejné Wi-Fi

Veřejná Wi-Fi je pohodlná, ale jde na úkor bezpečnosti. Když uživatelé odpovídají na e-maily v místní kavárně, nebo bezmyšlenkovitě prochází sociální sítě na letišti, někdo může sledovat jejich online aktivitu. Použití virtuálních privátních sítí chrání uživatelská data, především v jiných sítích, skrývá historii procházení, bankovní informace, hesla k účtům a další před neúmyslnými cizinci na internetu.

7.1.2 Ochrana dat od poskytovatele internetových služeb

Ochranou dat je myšlen soubor bezpečnostních prostředků proti neoprávněnému užití, deformování, kopírování, poškozování, či likvidaci počítačových dat, nebo informací. Ochrana probíhá prostřednictvím programového a technického vybavení. Když jsou uživatelé připojeni k domácí síti Wi-Fi, je menší pravděpodobnost, že je napadnou cizí lidé, než na veřejném připojení. Uživatelská data jsou však stále zranitelná. Poskytovatel internetových služeb, nebo jiná společnosti, kterým uživatelé každý měsíc platí za internetové připojení, má přístup ke všem internetovým datům jejich uživatelů. Dalé poskytovatel internetových služeb vidí kdy, kde, jak a co uživatelé prohlížejí. Tato data mohou shromažďovat a prodávat inzerentům, i když je použita funkce soukromého prohlížení a v případě narušení dat mohou být ve špatných rukou nebezpečné. Virtuální privátní sítě tedy mohou pomoci skrýt IP adresu před vlastním poskytovatelem internetových služeb, nebo jinou společností, které je každý měsíc placeno za internetové připojení. U některých poskytovatelů internetových služeb, kteří ve svých zemích nemají zákony týkající se síťové neutrality, které musí dodržovat, bylo zjištěno, že záměrně snižují množství obsahu, ke kterému můžete přistupovat, nebo jej sledovat. Tento přístup jim umožňuje získat vyšší zisky, protože vytváří umělé omezení vašich interneto-

---

[49] VYHNÁNKOVÁ, E., LOSEKOOT, M., Jak na sítě (Ovládněte čtyři principy úspěchu na sociálních sítích), Brno, 2019, s. 278-290

[50] ŠEVČÍKOVÁ, A. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 2014. s 21

vých aktivit. Když se přihlásíte k odběru služeb virtuálních privátních sítí, můžete zabránit některým poskytovatelům internetových služeb, aby vás mohli identifikovat, nebo třeba, aby mohli zpomalit rychlost vašeho přístupu. Tento problém se týká datových limitů, které se někdy vztahují na zákazníky poskytovatele internetu, dokonce i ve Spojených státech. [51] [52]

7.1.3 Ochrana osobních údajů z aplikací a služeb

Bohužel mnoho oblíbených aplikací a internetových služeb může ohrozit data uživatelů . Zejména Facebook, kde se nový uživatelé začleňují do sítě přidáním profilového obrázku a ostatních osobních informací. Navíc je zde nutné, stejně jako u většiny aplikací, či služeb potvrzení registrace přes samotný email.[53] V minulosti byly některé aplikace a služby velmi kritizovány kvůli způsobu, jakým využívají data svých uživatelů. Virtuální privátní sítě zabraňují aplikacím a webům připisovat jejich chování IP adrese počítači uživatelům. Sociální sítě jsou pro uživatele internetu důležitější než kdykoliv před tím. S neustále narůstajícím počtem uživatelů se stává svět více digitálním, než kdy dříve byl. Obrovské množství uživatelů užívajích sociální sítě se snaží využít společnosti a firmy, které mohou mířit reklamu na základě informací, které získávají od uživatelů. Díky analýze dat daného uživatele lze snadno zjistit, co mu kdy doporučit.[54] Během surfování na internetu toho o sobě a svém počítači uživatelé prozrazují poměrně hodně. Například jaký používají operační systém a internetový prohlížeč, jakou mají IP adresu, pomocí které dokážou hackeři celkem přesně lokalizovat jejich polohu. Lokalizace uživatele podle IP adresy využívá třeba síť YouTube pro řízení přístupnosti obsahu uživatelům z různých zemí. Podobně fungují například servery amerických televizních stanic, na kterých si uživatelé s americkou IP adresou mohou zdarma přehrávat filmy a seriály. Omezení lze snadno obejít. Stačí k tomu mít virtuální pri-

---

[51] Ochrana dat od poskytovatele internetových služeb *Vittana* [online]. [cit. 2022-4-3]. Dostupné z:https://vittana.org/16-major-advantages-and-disadvantages-of-a-vpn

[52] BÍMOVÁ, A. Počítačová kriminalita a naše doba. Praha, 1990, s. 85.

[53] DĚDIČEK, D. *Facebook jednoduše*. Vyd. 1. Brno 2010: Computer Press, a. s. 4

[54]VYHNÁNKOVÁ, E., LOSEKOOT, M., Jak na sítě (Ovládněte čtyři principy úspěchu na sociálních sítích), Brno, 2019, s. 278-290

vátní síť na zvýšení zabezpečení počítače při pohybu po síti.[55]

7.1.4 Ochrana osobních údajů a dat

Nejdůležitejším, proč se útočníci snaží zjistit hesla a další informace, je získat osobní udaje či data, které jim mohou pomoci buď ukrást peníze z bankovních účtů, použít účty majitelú kreditní karty k zasílání položek, nebo ještě něco horšího. Když útočníci mají osobní údaje, mohou snadno zfalšovat dokumenty a v nekterých případech to může způsobit fatální následky. Jak již bylo řečeno i organizace nakládaly s osobními údaji a daty víceméně bez souhlasu. Od prosazení obecného nařízení o ochraně osobních údajů GDPR se mnoho organizací dostalo do problémů se zákonem. Faktory, které ignorovaly při nakládání s osobními údaji lidí, se vrátily, aby je překonaly. Na základě stížností lidí a sdružení několik úřadů na ochranu údajů odhalilo roky porušování, neúmyslného i úmyslného. Některé organizace vyvázly s mírnějšími pokutami a postihy GDPR, jiné takové štěstí neměly. Nedodržení zákona má za následek vysoké pokuty GDPR, nebo přísná opatření v závislosti na porušení. Závažné porušení bude podléhat 4 % ročního celosvětového obratu nebo 20 milionům EUR podle toho, která hodnota je vyšší. Méně závažné porušení bude podléhat 2 % ročního celosvětového obratu nebo 10 milionům EUR podle toho, která hodnota je vyšší. Mezi další akce patří písemné varování, dočasný nebo trvalý zákaz, smazání dat a omezení datových přenosů. V konečném důsledku to vede ke ztrátě důvěry a pověsti příslušných organizací. Toto všechno je dalším z důvodů, proč uživatelé virtuální privátní sítě používají.[56]

7.2 Limity virtuálních privátních sítí

I virtuální privátní síte mají limity, které nemohou vyřešit, a tak se anonymita uživatelů může vytratit špatným kliknutím v podobě například olajkováním fotky na Instagramu.

---

[55]Ochrana osobních údajů z aplikací a služeb VPN. *Forbes* [online]. [cit. 2022-4-2]. Dostupné z:https://www.forbes.com/advisor/business/software/why-use-a-vpn/

[56] Ochrana osobních údajů. *Cookielawinfo* [online]. [cit. 2022-4-2]. Dostupné z:https://www.-cookielawinfo.com/gdpr-fines-biggest-gdpr-violation-examples/

Virtuální privátní sítě se snaží co nejlépe chránit uživatelská data a online identitu, ale žádná služba na světě nemůže zaručit anonymitu pokaždé, když se uživatel připojí k serveru. Internet je nestabilní místo a tato nestabilita přináší stále nové problémy, které mohou ohrozit soukromí a bezpečnost dat. Kromě toho mají společnosti, webové služby, streamovací služby, webové stránky a aplikace další způsoby sledování uživatelů. Pokud znají chování uživatele při procházení, mohou použít techniky, jako je snímání otisků prstů a podívat se na aktivitu přátelského uživatele, aby se o uživateli dozvěděly více. To jsou problémy, které virtuální privátní sítě nemohou vyřešit.[57]

7.2.1 Limity podnikových virtuálních privátních sítí

Uživatelé by také měli pochopit, že podnikové virtuální privátní sítě se liší od virtuálních privátních sítí, které slouží individuálním spotřebitelům. Často jsou navrženy speciálně pro přístup k síti zaměstnavatele, nikoli pro zajištění bezpečnosti a anonymity na internetu pro osobní použití. S největší pravděpodobností dá správce sítě společnosti, pro kterou uživatel pracuje, uživateli pokyny, jak postupovat při nastavení VPN na zařízení uživatele. Pro podnikové uživatele může být obtížné nastavit virtuální privátní síť kvůli rozsahu operace. Osobní uživatelé potřebují pouze nainstalovat aplikaci virtuální privátní sítě a zakoupit balíček, aby získali soukromí a anonymitu, ale firemní uživatelé se musí ujistit, že je celá kancelářská síť zabezpečená. To je složitý úkol, který mnoho firem není připraveno vyřešit. Kancelářské sítě jsou vždy složité a přidání virtuální privátní sítě tuto složitost zvyšuje. Bez týmu síťových expertů nemohou podniky implementovat virtuální privátní síť způsobem, který ochrání jejich data a ochrání jejich síť. Rozsáhlost je dalším problémem, kterému musí obchodní uživatelé čelit. Jedna věc je poskytnout ochranu 10 uživatelům virtuálních privátních sítí, ale úplně jiná je nabídnout stejnou ochranu tisícům. Služby virtuální privátní sítě také nejsou dobré v poskytování granulární kontroly. Jakmile se uživatel připojí ke službě virtuální privátní sítě, obvykle získá přístup k celé síti. I ty oblasti, které nejsou určeny pro ne-

[57] Limity VPN. *Forbes* [online]. [cit. 2022-4-2]. Dostupné z:https://www.forbes.com/advisor/business/software/why-use-a-vpn/

administrátory. To může vystavit kritickou obchodní infrastrukturu zbytečnému riziku.[58]

7.2.2 Kvalitní virtuální privátní sítě stojí peníze

Kvalitní sítě virtuální privátní sítě chrání uživatelská data a poskytují soukromí online, ale nejsou zdarma. I když cena obvykle není extrémní, často se pohybuje kolem 10 $ měsíčně v ČR okolo 300 Kč na vyšší úrovni, nemusí být v rámci rozpočtu všech uživatelů. Virtuální privátní sítě poskytují obrovské slevy na své dvou a tříleté plány, ale ty vyžadují, aby uživatel zaplatil po celou dobu trvání předem s očekáváním, že virtuální privátní sít' bude na konci předplaceného období stále v provozu. Dalším problémem při zavazování se ke službě virtuální privátní sítě je, že neexistuje žádná záruka. Dotyčná služba virtuální privátní sít' bude i nadále dobře fungovat. Vysoce kvalitní služba dnes může časem snižovat kvalitu, což je třeba vzít v úvahu, než se uživatel dlouhodobě zaváže ke službě. VPN sice dokonale působí, ale nejsou to bezchybné nástroje. Jako každý počítačový program jsou zranitelné vůči malware a online útokům. V případě napadení jsou bezpečnostní výhody VPN anulovány. Používání bezplatné služby VPN zvyšuje pravděpodobnost útoků a narušení bezpečnosti. K pokrytí obchodních nákladů mohou „bezplatné“ služby VPN prodávat uživatelská data, nebo zobrazovat reklamy, které by mohly být infikovány malware. Pokud je cílem zvýšit soukromí dat, pak je nejlepší možností investovat do placené VPN.[59]

7.2.3 Přerušená připojení

Vzhledem k přirozené chaotické povaze internetu služby virtuálních privátních sítí čas od času přeruší zabezpečené připojení. Přerušená připojení mohou vést k únikům dat, které mohou ohrozit bezpečnost, soukromí a anonymitu uživatele. Většina elitních virtuálních privátních sítí má k řešení tohoto problému funkci kill switch, ale pokud tato funkce není přítomna, nebo nefunguje správně, může být odhalena skutečná IP adresa uživatele. Přerušená připojení jsou pro korporace ještě větším problémem, protože virtuální privátní sítě nejsou stavěny pro nepřetržité intenzivní používání. V

---

[58]Limity podnikové VPN. *SecurityGladiators* [online]. [cit. 2022-4-3]. Dostupné z:https://securitygladiators.com/vpn/advantages-disadvantages/

[59] Kvalitní VPN stojí peníze. *SecurityGladiators* [online]. [cit. 2022-4-3]. Dostupné z:https://securitygladiators.com/vpn/advantages-disadvantages/

prostředí, jako je kancelář, kde přes virtuální privátní síť neustále prochází velké množství provozu, může zvýšené zatížení ovlivnit výkon serveru virtuální privátní sítě a může vést k výpadkům připojení[60]

7.2.4 I virtuální privátní síť může sledovat

I přes to, že se virtuální privátní sítě zaměřují na to, aby byli uživatelé více v anonimitě, není tomu vždy tak. Některé z virtuálních privátních sítí jsou k dizpozici zdarma s tím, že jejich uživatelé platí výměnou za data, která odesílají a přijímají. Tyto virtuální privátní sítě stále pomáhají obejít určitá omezení. Nicméně, některé z těchto společností poskytující virtuální privátní sítě, mohou sledovat, co dělají jejich uživatelé. Pakliže tito poskytovatelé virtuálních privátních sítí data schromažďují, mohou být uživatelé v ohrožení. To je důvod, proč by bezplatná, nebo velmi nízká cena virtuální privátní sítě měla být něčím, k čemu by uživatelé měli přistupovat velmi opatrně.[61]

7.2.5 Limity anonymity

Virtuální privátní síť je sice skvělým nástrojem pro oddělení polohy zařízení od dat, ale nedokáže uživatele ochránit uplně před vším. Pakliže je vyplněn kvíz na Facebooku, nebo například interakce s příspěvkem na Instagramu, tak aplikace, kterou uživatelé používají, může stále sledovat jejich chování k přizpůsobení reklam a obsahu, i když jsou připojeni na virtuální privátní síť. Možná sociální sítě nevědí, co uživatelé jinak hledají, ale stále vědí, co dělají v jejich aplikacích. Podobně tomu je, pokud jsou na počítači povoleny soubory cookie. Společnosti mohou sledovat, když jsou uživatelé na jejich webových stránkách. Veškerá data uživatelů tedy nejsou samotnou virtuální privátní sítí zakryta. Pro lepší zabezpečení jsou k dizpozici nástroje jako je Tor, který umožní procházet web anonymně a dalšími bezpečnostními opatřeními, jako například přesměrovávání přes proxy servery. V dnešním světě není ochrana před cílenými útoky skupin, nebo jednotlivců na vybrané cíle nijak jednoduchá a může na některých obětech zanechat silné psychické následky. Tyto útoky mohou oběti dohnat dokonce až k sebe-

---

60 I VPN může sledovat. *SecurityGladiators* [online]. [cit. 2022-4-3]. Dostupné z:https://securitygladiators.com/vpn/advantages-disadvantages/

61 Výhody a nevýhody VPN . *Vittana* [online]. [cit. 2022-4-3]. Dostupné z:https://vittana.org/16-major-advantages-and-disadvantages-of-a-vpn

vraždě. Tento jistý druh anonymity na Internetu a možnost vydávání se za někoho úplně jiného je velmi silnou zbraní útočníků. Co se prevence kriminality týče patří ČR v rámci Evropy mezi špičky. Vznikla zde tedy celá řada projektů, které se zabývají vzděláváním všech skupin uživatelů od dětí, až po seniory. Jsou to například projekty Seznam se bezpečně, E-Bezpečí, Bezpečný internet, Linka bezpečí a různá krizová centra.[62] [63]

[62]KOŽÍŠEK, M., PÍSECKÝ V. Bezpečně na internetu. Průvodce chováním ve světě online. Praha, 2016, s. 144-152.

[63] Výhody a nevýhody VPN (3). *Forbes* [online]. [cit. 2022-4-2]. Dostupné z:https://www.forbes.com/advisor/business/software/why-use-a-vpn/

8 Praktická část

Praktická část bakalářské práce se zabývá žáky vybraných střeních a vysokých škol v jihočeském kraji a jejich znalostmi o virtuálních privátních sítích. Pro tento empirický výzkum bylo vybráno všech sedm okresů. Data se však podařilo nazbírat pouze z pěti okresů. Úkolem bylo zjistit, jaký mají dotázaní žáci přehled o virtuálních privátních sítích. K čemu a jak často jej užívají, zda si cení soukromí na internetu natolik, že jsou obeznámeni s touto technologií. Ostatně žáci středních škol, jsou stále ve věku, kdy si ještě neuvědomují jak moc by si měli své soukromí střežit. Oproti tomu, se od žáku vysokých škol očekává, že budou s touto problematikou dostatečně obeznámeni a to nejen vzhledem k jejich věku, ale i výši vzdělání.

8.1 Formulace výzkumného problému

Výzkumným problémem bakalářské práce je: „Virtuální privátní síť z pohledu kybernetické bezpečnosti.“

Hlavní výzkumný cíl

Zjistit znalosti a způsoby užívání virtuálních privátních sítí žáků vybraných střeních a vysokých škol v jihočeském kraji z pohledu kybernetické bezpečnosti.

8.2 Výzkumné otázky a hypotézy

Otázky dotazníku:

a) V jakém z uvedených okresů studujete?

b) Jste žák/žákyně střední nebo vysoké školy?

c) Jaké je vaše pohlaví?

1. Je pro vás soukromí na internetu důležité?

2. Jak by jste popsali Vaše znalosti ohledně bezpečného užívání internetu?

3. Víte co je Virtuální privátní sít (VPN)?

4. Věděli byste před čím vás VPN může chránit?

5. Dokázali byste vysvětlit princip fungování VPN?

6. Používáte VPN nebo jste ji někdy použili?

7. Jak často VPN používáte?

8. Na jakých zařízeních VPN používáte?

9. K čemu VPN používáte?

Stanovené výzkumné otázky a hypotézy jsou následující:

H1:Virtuální privátní sítě užívají pro svou bezpečnost více muži než ženy .

H2: Uživatelé nevyužívají VPN ačkoli chtějí mít zabezpečená data.

H3: Žáci středních škol mají menší povědomí o problematice virtualních privatních sítí, než žáci vysokých škol

8.3 Metody výzkumu a sběr dat

V rámci metodologického zpracování výzkumu, byl vybrán kvantitativní typ výzkumu. Pro sběr dat na tento kvantitativní výzkum byla zvolena metoda dotazníkového šetření. Silnou výhodou dotazníku je to, že poměrně rychle a ekonomicky shromažďuje data od většího počtu respondentů. Cílem tedy bylo získat větší počet informací, od dostatečného počtu respondentů. Vytvořený dotazník je tvořen elektronicky pomocí aplikace Google docs, proto bylo jednoduché rozčlenit některé otázky na sekce a v případě nevědomosti respondentů je automaticky přesunout na konec dotazníku. V dotazníku můžeme nalézt 12 otázek, které jsou uzavřené, respondenti proto mohli vybírat pouze z předem nastavených odpovědí a to až na poslední otázku, která byla polouzavřená, možností zde bylo více. Žáci byli vybráni z pěti ruzných okresů. Všichni respondenti byli osloveni prostřednictvím sociální sítě facebook nebo Instagram, kam jim byl odkaz zaslán.

8.4 Výzkumný soubor

Jak již bylo zde zmíněno, cílovou skupinou pro výzkum bakalářské práce byli žáci vybraných středních a vysokých škol v Jihočeském kraji. Výzkum je tedy zaměřen na mladistvé a dospělé, kde se počítá s věkovým rozmezím mezi 15-26 let věku. Šetření v podobě dotazníku se zůčastnilo celkem 101 respondentů.

8.5 Realizace výzkumu

Před rozesláním dotazníku středním a vysokým školám v Jihočeském kraji byl proveden test a to z důvodu ověření jasnosti uvedených otázek. Dotazníky byly proto dobrovolně vyplněny uživateli na sociálních sítích. Dotázaných 8 respondentů dotazníku jeho otázkám zcela porozumělo a nebyl zde důvod jej jakýmkoliv způsobem upravovat. Vyplněné testové dotazníky nebyly do výzkumného šetření zařazeny, a to vzhledem k tomu, že se nejednalo o respondenty splňující podmínky šetření. Na začátku realizace výzkumu byli osloveni žáci z pěti ruzných okresů, a to České Budějovice, Český Krumlov, Písek, Strakonice a Tábor. Následně byl odkaz na dotazník rozeslán žákům, jenž byl doplněn o zprávu "Ahoj prosím pošleš ten dotazník do vaší školní skupiny? Děkuji". Vzhledem k elektronické formě testu nebylo nutné před zahájením dotazníku složitých informací. Díky jeho jednoduchému postupu vše proběhlo bez jakýchkoliv potíží. Délka pro vyplnění testu se odhaduje mezi 1 - 3 minuty.

8.6 Způsob zpracování dat

Aplikace Google docs nejprve zaznamenávala četnost všech odpovědí na každou z položených otázek dotazníku. Následně byly tyto informace převedeny do grafů, jimiž Aplikace Google docs disponuje. Dále byla vygenerována tabulka v programu Excel, kde se všechna data porovnávala.

8.7 Analýza dat

Dotazníkového šetření se zúčastnilo, jak bylo již zmíněno výše, 101 respondentů.

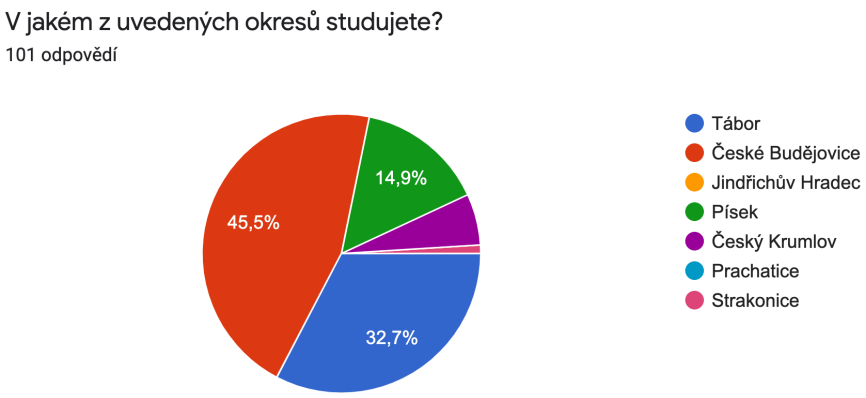
Z důvodu přehlednosti si respondenty rozdělíme podle škol na:

-žáci středních škol: 49 respondentů (z toho: 31 žen a 18 mužů)

-žáci vysokých škol: 52 respondentů (z toho: 25 žen a 27 mužů)

Analýza respektuje sled otázek v dotazníku. Jednotlivé analýzy jsou vyjádřeny graficky.

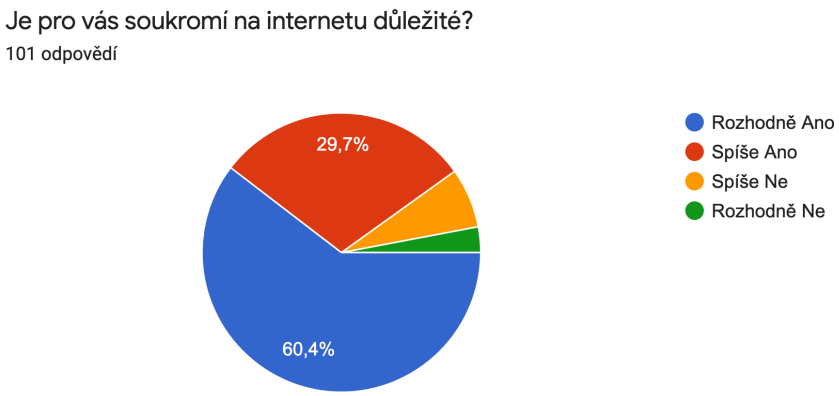
Graf a): V jakém z uvedených okresů studujete?[64]



Otázka a) „V jakém z uvedených okresů studujete?"

Na výše uvedeném grafu můžeme vidět procentuální zastoupení dotázaných žáků v jednotlivých okresech.

Graf č.1: Je pro vás soukromí na internetu důležité?[65]



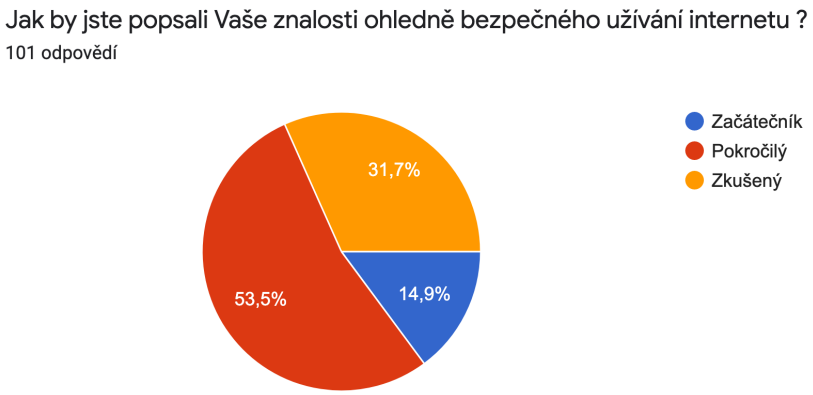
[64] Vlastní: Graf a): V jakém z uvedených okresů studujete?

[65] Vlastní: Graf č.1: Je pro vás soukromí na internetu důležité?

Otázka č.1 „Je pro vás soukromí na internetu důležité?”

Na tuto otázku odpovědělo celkem 101 respondentů. Respondenti měli na výběr ze čtyř možných odpovědí od „rozhodně ano” až po „rozhodně ne”. Nejčastější odpovědí byla odpověď „rozhodně ano”, kterou uvedlo 61 respondentů. Druhou nejčastější odpovědí pak byla odpověď „spíše ano”, která byla uvedena ve 30 případech. Na třetím místě se umístila odpověď' „spíše ne” a to se 7 počty. Jako poslední udávanou odpovedí byla možnost „rozhodně ne” s počtem 3 respondentů. Na výše uvedeném grafu můžeme vidět, že kladné odpovědi, tedy „rozhodně ano” a „spíše ano” mají dohromady 90,1%, opravdu drtivé většině respondentů tedy na svém soukromí na internetu záleží a je pro ně důležité. Problém ale nastává, jak uvidíme v následujících grafech, že pro ochranu svého soukromí ale většina respondentů při každém připojení k internetu VPN nevyužívá. Na ochraně jim sice záleží, ale jediné co pravděpodobně dělají, aby své soukromí na internetu ochránili je, že používají například anonymní okna v prohlížeči, která zdaleka neposkytují takovou ochranu jako VPN. V praxi tato anonymní okna pouze zamezují ukládání historie vyhledávání a ukládání souborů cookies, což se rozhodně nedá považovat za dostatečnou ochranu.

Graf č.2: Jak byste popsali vaše znalosti ohledně bezpečného užívání internetu?[66]



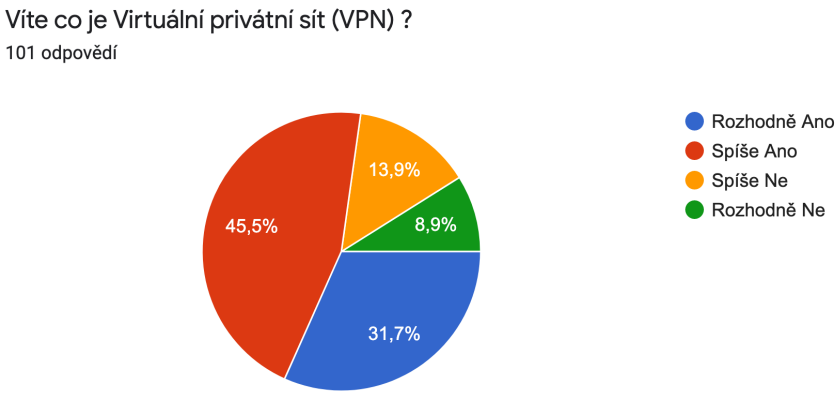
Otázka č.2 „Jak byste popsali vaše znalosti ohledně bezpečného užívání internetu?“

Na tuto otázku měli respondenti na výběr ze tří možných odpovědí, ze kterých si

[66] Vlastní: Graf č.2: Jak byste popsali vaše znalosti ohledně bezpečného užívání internetu?

mohli vybrat. Celkem na tuto otázku odpovědělo 101 respondentů. Nejčastější odpověď byla, že se respondent považuje za pokročilého ve znalostech ohledně bezpečného užívání internetu, tuto odpověď zvolilo 54 respondentů. Druhou nejčastější odpovědí bylo, že se respondent považuje za zkušeného, takto odpovědělo 32 respondentů. Nejméně častá odpověď pak byla, že se respondent považuje za začátečníka, takto odpovědělo pouze 15 respondentů. Zajímavé je, že z celkových 15 respondentů, kteří uvedli, že se považují za začátečníka, je 11 žen, což tvoří zhruba 75%.

Graf č.3 Víte co je VPN?[67]



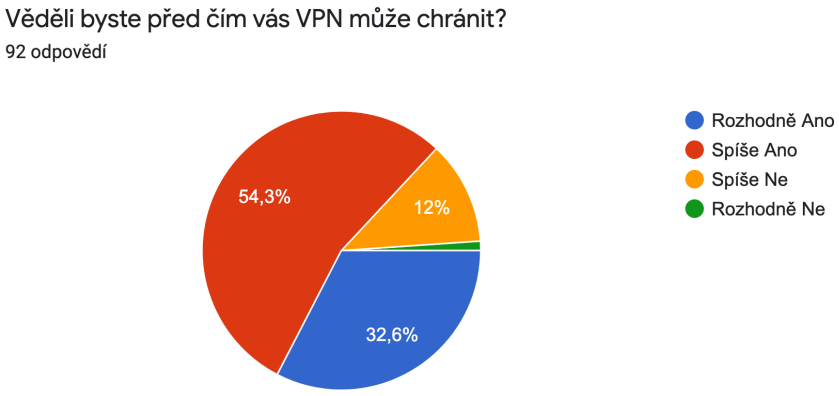
Otázka číslo 3 „Víte co je VPN?“

Z grafu který můžeme vidět výše vyplývá, že velká většina respondentů má alespoň nějakou představu o tom, co to VPN je. Odpověď „rozhodně ano” a „spíše ano“ uvedlo dohromady 77,2% respondentů. Nejčastější odpovědí bylo „spíše ano”, což uvedlo 46 respondentů. Druhou nejčastější odpovědí bylo „rozhodně ano”, což bylo uvedeno 32krát, dále 14krát odpověď „spíše ne“ a nejméně častou odpovědí bylo „rozhodně ne“, kterou uvedlo pouze 9 respondentů. Ti žáci, kteří uvedli tuto odpověď už nepokračovali dále v dotazníku a byli odkázáni na konec. Celkem na tuto otázku odpovědělo 101 respondentů.

Graf č.4 :Věděli byste, před čím vás může VPN chránit?[68]

[67]Vlastní:Graf č.3 Víte co je VPN?

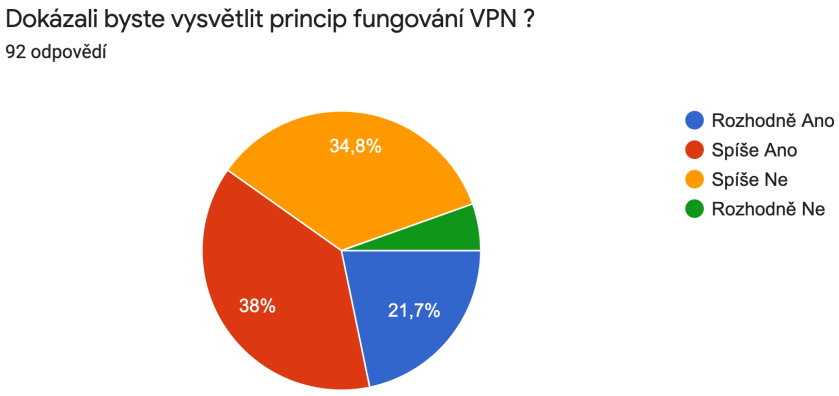
[68] Vlastní:Graf č.4 :Věděli byste, před čím vás může VPN chránit?



Otázka číslo 4 „Věděli byste, před čím vás může VPN chránit?“

Na tuto otázku odpovědělo celkem 92 respondentů. Žáci měli na výběr ze 4 možností. Nejčastější odpovědí bylo „spíše ano”, což uvedlo 50 respondentů. Druhou nejčastější odpovědí bylo „rozhodně ano“, což uvedlo 30 dotázaných respondentů, dále pak 11 respondentů uvedlo „spíše ne“, a pouze jeden respondent uvedl „rozhodně ne“. Zbylých 9 respondentů se k této otázce nepropracovalo, protože odpověděli „rozhodně ne“ na otázku, zda ví, co je VPN.

Graf č.5: Dokázali byste vysvětlit princip fungování VPN?[69]



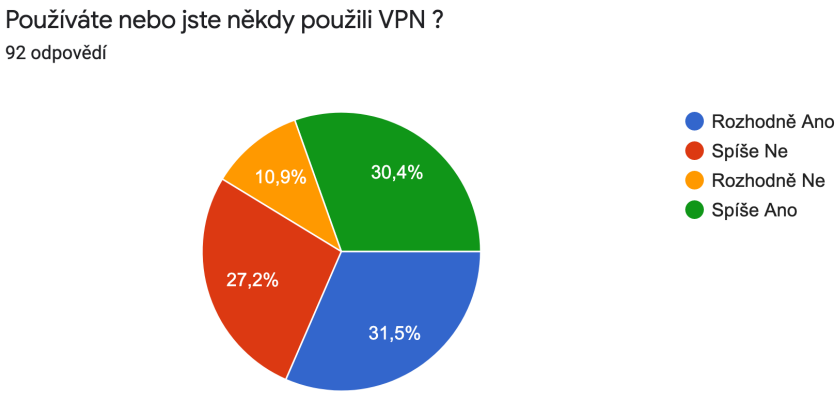
Otázka číslo 5 „Dokázali byste vysvětlit princip fungování VPN?“

Na tuto otázku odpovídalo celkem 92 respondentů. Respondenti měli opět možnost vybrat v této otázce více možností. Nejčastější odpovědí bylo „spíše ano“,

[69]Vlastní:Graf č.5: Dokázali byste vysvětlit princip fungování VPN?

tedy, že by s největší pravděpodobností dokázali princip fungování VPN vysvětlit. Tato odpověď se objevila 35krát. Druhou nejčastější odpovědí bylo„ spíše ne“, tedy že by princip fungování VPN spíše vysvětlit nedokázali, tato odpověď byla uvedena 32krát. Další nejčastější odpovědí bylo „rozhodně ano“, takto odpovědělo 20 respondentů. Nejméně častou odpovědí pak bylo „rozhodně ne“, tuto odpověď zvolilo pouze 5 respondentů. Podmínkou pro zobrazení této otázky bylo, že respondent musel v otázce „Víte co je VPN?“ odpovědět jinak než „rozhodně ne“, vidíme tedy, že i mezi lidmi se znalostmi o VPN je zhruba jen polovina, kteří by ale dokázali také vysvětlit princip jejího fungování.

Graf č.6: Používáte nebo jste někdy použili VPN?[70]

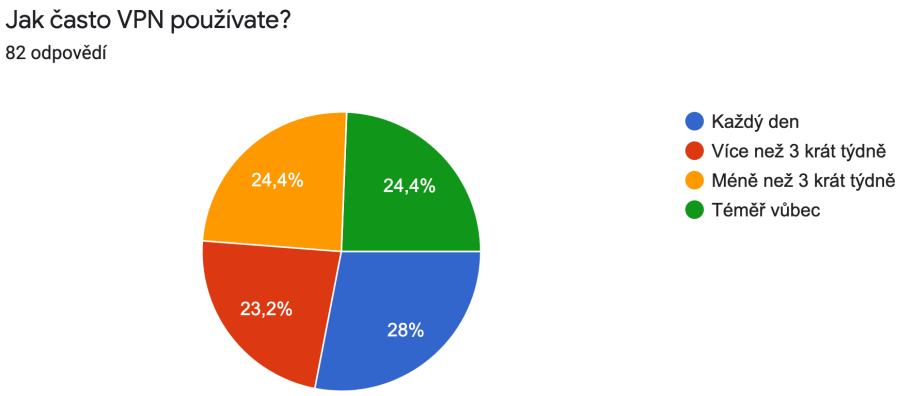


Otázka číslo 6„Používáte nebo jste někdy použili VPN?“

U této otázky bylo možno vybrat ze čtyř odpovědí. Nejčastěji respondenti odpověděli „rozhodně ano“, tedy že VPN spíše již někdy použili, takto odpovědělo 29 z celkem 92 žáků. Druhou nejčastější odpovědí bylo „spíše ano“, tedy že VPN spíše občasně využívají, což uvedlo 28 respondentů. Další nejčastější odpovědí bylo „spíše ne“, tedy že VPN požívali nebo požívají zřídka, což uvedlo 25 respondentů. Nejméně častou odpovědí pak bylo „rozhodně ne“, tedy že VPN rozhodně nepožívají a nikdy v životě jej nepoužili. Tuto odpověď uvedlo pouze 10 respondentů. Podmínkou pro zobrazení této otázky bylo zodpovězení otázky „víte co je VPN“? Pakliže respondent odpověděl „rozhodně ne“, byl automaticky odkázán na dokončení dotazníku.

[70]Vlastní:Graf č.6: Používáte nebo jste někdy použili VPN?

Graf č.7:Jak často VPN používáte?[71]



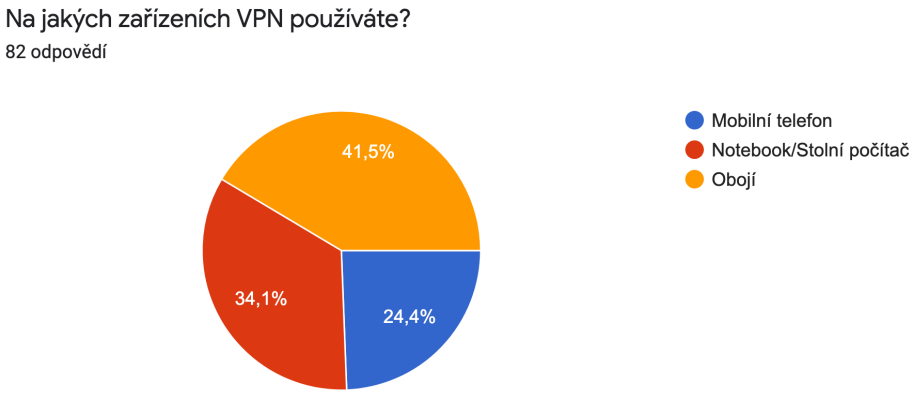
Otázka číslo 7 „Jak často VPN používáte?“

Na tuto otázku měli respondenti možnost zvolit si ze čtyř následujících odpovědí. První možnou odpovědí bylo, že respondent užívá VPN každý den, druhou že vícekrát jak 3krát týdně, třetí možnost pak byla méně než 3krát týdně a poslední možnou odpovědí bylo, že VPN neužívá téměř vůbec. Z grafu č.7 vyplývá, že nejčastěji respondenti VPN používají každý den, tuto odpověď zvolilo 23 z celkových 82 respondentů. Na druhém a třetím místě se shodným počtem respondetů a to 20, byly odpovědi “méně než třikrát týdně” a “témeř vůbec”. Poslední nejméně častou odpovědí pak bylo “více než třikrát týdně”, tuto odpověď zvolilo 19 respondentů. Je vidět, že využití VPN je u nekterých uživatelů velice individuální. Mnoho uživatelů jej využívá právě jen ke streamovacím službám nebo na dané aktivity. Zajímavé je, že uživatelé, kteří si soukromí na internetu cení, což představuje každodení surfování na internetu s použitím VPN, tvoří pouze 28% respondetů.

Graf č.8:Na jakých zařízeních VPN používáte?[72]

[71] Vlastní:Graf č.7:Jak často VPN používáte?

[72] Vlastní:Graf č.8:Na jakých zařízeních VPN používáte?



Otázka číslo 8 „Na jakých zařízeních VPN používáte?“

Na tuto otázku jsme měli 3 možné odpovědi, ze kterých si mohli žáci vybrat. První možností odpovědi je mobilní telefon, druhou notebook/stolní počítač a poslední možností je užívání VPN na obou zařízeních, tedy jak na mobilním telefonu, tak na notebooku. Celková četnost odpovědí u této otázky je 82. Z grafu vyplývá, že nejčastěji respondenti užívají VPN na obou zařízeních, tedy jak na mobilním telefonu, tak na notebooku/stolním počítači, tuto odpověď uvedli respondenti 34krát. Druhou nejčastější odpovědí byl notebook/stolní počítat, na což odpovědělo 28 respondentů. Nejméně častou odpovědí pak bylo užívání VPN pouze na mobilním telefonu, tuto odpověd uvedlo pouze 20 z celkových 82 respondentů

Otázka č.9 „K čemu VPN používáte?“

Na poslední otázku dotazníku měli respondenti na výběr z několika možných odpovědí a měli možnost uvést několik odpovědí zároveň.

Nejčastěji udávanou odpovědí, kterou udalo 81,7% respondentů bylo, že VPN používají k ochraně soukromí na veřejné wifi síti. Tato odpověď nebyla příliš překvapivá, na veřejných wifi sítích může někdo snadněji sledovat, co uživatel na zařízení dělá a získat z toho pro něj prospěšné informace, jejiž zneužitím může uživateli nemálo uškodit. Dálé byla tato možnost první volbou, což mohlo respodentům ulehčovat odpověď’ v případě, že si nebyli jisti co zvolit.

Druhou nejčastější odpovědí byla bezpečná komunikace a to s podílem 65,9%. Zde se samozřejmě jedná o uživatele, kterým záleží na tom, aby jejich komunikace byla

dostatečně dobře šifrována.

Dále mnoho respondentů uvedlo, že VPN používají k anonymnímu prohlížení. Tato odpověď nebyla nijak překvapivá, protože to je přesně to, co se od tohoto softwaru očekává. Dále se dá očekávat, že pokud si někdo nebyl zcela jistý tím jakou odpověď zvolit, s největší pravděpodobností si vybral právě tuto nejvíce obecnou a řekněme také logickou odpověď. Pro tuto odpověď se rozhodlo 64,6% dotázaných.

Polovina odpovědí byla snaha skrýt aktivitu před státem. Tuto odpověď udalo 48,8% respondentů. Zřejmě někteří uživatelé internetu nedůvěřují státu v tom, jak by mohl nakládát s jejich osobními daty získanými v kyberprostoru.

Další nejčastější důvod pro užívání VPN je snaha skrýt aktivitu prohlížení před poskytovatelem internetu, tuto odpověď udalo 46,3% respondentů. Připojení k domácí síti je sice rozhodně bezpečnější než veřejná síť, přestože sice nehrozí takové riziko napadení jako na veřejné wifi síti, je zde ale riziko zneužití dat a to právě ze strany poskytovatele internetu. Tuto odpověď udalo 46,3% respondentů, je tedy vidět, že si toto riziko uživatelé dobře uvědomují.

Dalším důvodem byl přístup na stránky s omezeným přístupem. Některé stránky jsou v ČR běžným prohlížečem nedohledatelné a jsou dohledatelné jen v určité zemi, proto VPN díky změně geolokace dovoluje změnu polohy a to je důvodem, proč 42,7% dotázaných odpovědělo, že jej využívá.

Dalším, již ne tak často udávaným důvodem užívání VPN, je získání lepší zábavy (hry, stream, apod.), tuto odpověď udalo 39% dotázaných. Navzdory tomu, že se jedná o žáky středních a vysokých škol, kteří v jejich věku zábavu na internetu vyhledávají, nebyla tato odpověď překvapivě tak častá.

Co se získání slev při nákupu online týče, tuto možnost zvolilo 37,8% dotázaných. To je způsobeno tím, že rozdíly cen mezi Českou republikou a světem nejsou tak markantní.

Předposlední důvod užívání VPN byl přístup k prohlížeči Tor, tedy 26,8% dotázaných. Tito uživatelé využívají v nejvíce případech kombinaci VPN a Toru k dosažení

nejlepšího možného bezpečí. Avšak někteří uživatelé se pouze seznamují se softwarem Tor.

Posledním důvodem uvedeným pro používání VPN je přístup na stránky v práci, což uvedlo 17,1% respondentů. Takto slabému výsledku se ale nelze divit vzhledem k průměrnému věku respondentů mezi 15ti-26ti lety. Většina z nich pravděpodobně není zaměstnaných.

8.8 Interpretace dat

Cílem této bakalářské práce bylo zjistit znalosti a způsoby užívání virtuálních privátních sítí žáků vybraných středních a vysokých škol v Jihočeském kraji z pohledu kybernetické bezpečnosti. Na počátku výzkumu této bakalářské práce byly stanoveny tři hlavní výzkumné hypotézy. Výzkumná hypotéza H1, „Virtuální privátní sítě užívají pro svou bezpečnost více muži než ženy" ,se potvrdila. To znamená, že Virtuální privátní sítě užívají pro svou bezpečnost opravdu více muži a to s výsledkem 55,6% dotazovaných mužů, kteří odpověděli na otázku „používáte VPN a už jste je někdy použili ?" „rozhodně ano" a „spíše ano". a na druhou otázku „Jak často VPN používáte?" kde byla stanovena podmínka odpovědí „více než 3 krát týdně" nebo „každý den",kdežto žen odpovědělo na tuto modelovou variantu pouze 26,6% .

Uživatelé nevyužívají VPN, ačkoli chtějí mít zabezpečená data. Takto zněla hypotéza H2, kdy jsme předpokládali, že vzhledem k tomu, jak je v dnešním světě kybernetické technologie ochrana soukromí důležitá, tak i přes to více než třetina uživatelů IT technologií nevyužívá možnosti zabezpečení VPN. Tato hypotéza tedy potvrzena nebyla vzhledem k tomu že se nejednalo o více jak polovinu respondetů. Pro tuto hypotézu byly stanoveny následující otázky „Je pro vás soukromí na internetu důležité?" zde odpovědělo možností „rozhodně ano" a „spíše ano" 91 ze 101 dotazovaných respondentů, nicméně ti, kteří odpoveděli na otázku „Používáte VPN nebo jste ji někdy použili ?" „rozhodně ne" a „spíše ne" a zároveň v předchozí otázce souhlasilo s tím, jak je pro ně soukromí důležité, bylo 31, ke kterým musíme připočítat 3 respondenty, kteří i přes jejich potřebu soukromí nedokázali odpovedět na otázku „Víte co je virtuální privátní síť (VPN)?" zvolili proto odpověd „rozhodně ne".

Výzkumná hypotéza H3: Žáci středních škol mají menší povědomí o problematice virtualních privatních sítí, než žáci vysokých škol. Ta představovala vědět co je VPN, před čím VPN může chránit a vysvětlit princip fungování VPN. Tato hypotéza byla dostatečně potvrzena. Aby bylo možné určit, zda se v bezpečnosti vyznají lépe středoškoláci či vysokoškoláci, bylo zapotřebí zodpovězení tří otázek s odpovědí „rozhodně ano" a „spíše ano". Otázky byly nasledující a to „Víte co je virtuální privátní síť (VPN)?" jako další „Věděli byste před čím vás VPN může chránit?" a jako poslední „Dokázali byste vysvětlit princip fungování VPN?". Z celkového počtu až 50% dotazovaných středoškoláků má povědomí o této problematice. U vysokoškoláků tomu bylo velice podobně a to 53,5%. Nicméně zajímavostí bylo, že když se vyhledávali žáci, kteří této hypotéze 100% rozumí, tedy ti, kteří odpověděli na všechny tři otázky „rozhodně ano" byli to naopak žáci středních škol, kterých bylo 20,8% ze všech dotazovaných, kdežto žáků vysokých škol s těmito znalostmi bylo pouze 11,3%. Na závěr je tedy důležité říci, že polovina žáků středních i vysokých škol má s touto problematikou dostatečné znalosti. To se potvrdilo u 50 ze 101 respondentů, kde u otázek „Víte co je Virtuální privátní síť (VPN)?" a „Věděli byste před čím vás VPN může chránit?" odpovědelo „rozhodně ano" a „spíše ano" a u otázky „Jak by jste popsali Vaše znalosti ohledně bezpečného užívání internetu?" byla jejich odpověd „pokročilý" a „zkušený".

Závěr

Tématem bakalářské práce byly virtuální privátní sítě neboli VPN, z pohledu kybernetické bezpečnosti a jaké zkušenosti mají s virtuálními privátními sítěmi žáci vybraných středních a vysokých škol v Jihočeském kraji. Cílem této bakalářské práce bylo tedy zjistit znalosti a způsoby užívání virtuálních privátních sítí žáků vybraných středních a vysokých škol v Jihočeském kraji z pohledu kybernetické bezpečnosti. Na počátku výzkumu byly stanoveny tři věcné hypotézy. První hypotéza H1:Virtuální privátní sítě užívají pro svou bezpečnost více muži než ženy se potvrdila. Jako další H2: Uživatelé nevyužívají VPN ačkoli chtějí mít zabezpečená data, tato se bouhužel nepotvrdila. Jako poslední stanovenou hypotézou byla H3: Žáci středních škol mají menší povědomí o problematice virtualních privatních sítí, než žáci vysokých škol. Tato hypotéza byla potvzena. Z důvodu silně rostoucího marketingu ohledně VPN, jsou na tom dotazovaní žaci se znalostmi VPN lépe, než uvádí světové statistiky. Co se bezpečnosti na internetu týče, jsou žáci vcelku uvědomělí a není tedy potřeba jakýchkoliv seminářů týkajících se bezpečnosti soukromí na internetu.

Kybernetický prostor je dnes zřejmě tím nejdůležitějším článkem našeho života, představa dnešních mladých lidí bez přístupu k internetu je proto již dnes nepředstavitelná. Internet je dnes bezpochyb nejrozsáhlejší počítačovou sítí světa. Tato světová síť se extrémně rychle rozvíjí a jak je vidět, stejně tomu tak je i u uživatelů, kteří mnohem více dbají o své soukromí. Uživatelé nejsou převážně dospělí jak tomu bylo dříve, patří mezi ně čím dál více dětí a mladistvých. Bezpečnost na internetu je velmi diskutovaným tématem, v dnešní době je extrémně důležité se na tomto místě chránit. Virtuální privátní sítě jsou z pohledu kybernetické bezpečnosti jedním z nejdůležitějších prvků, které mohou uživatele internetu na tomto místě chránit. Dnešní internet je totiž místo, kde hrozí uživatelům narušení soukromí nejen ze strany útočníka v podobě hackera, ale i poskytovatele internetu nebo Policie. To jsou hlavní důvody, proč je potřeba se na internetu chránit. Soukromí na internetu je totiž jednou z nejcennějších věcí, kterou zde vůbec máme.

V teoretické části práce byly k dizpozici informace o virtuálních privátních sítích z pohledu kybernetické bezpečnosti. Na začátku bylo nutné čtenáře dostatečně seznámit

se základními pojmy, které byly nezbytné k pochopení VPN. Další kapitola byla zaměřena na limity kyberprostoru, tedy na kybernetickou bezpečnost. V jedné z dalších částí zde byl historický vývoj virtuálních privátních sítí, následně samotní uživatelé virtuálních privátních sítí. K závěru teoretické části práce zde byly komplexně popsány formy připojení virtuálních privátních sítí a jako posledním rozbor kladů a záporů virtuálních privátních sítí. Co se praktické části týče bylo zde její stručné představení s formulací výzkumného problému bakalářské práce. Jako další byly k dizpozici výzkumné otázky a hypotézy. Následovaly metody výzkumu a sběru dat. Další podrobné informace byly uvedeny i ve výzkumném souboru. Následovala realizace výzkumu a způsob zpracování dat. Na závěr praktické části byla k dispozici interpretace dat, ve které bylo odpovězeno na předem stanovené hypotézy

Na závěr by bylo dobré zmínit, že virtuální privátní sít' je také, autorem bakalářské práce používána. Samotné zjištění, že povědomí o virtuálních privátních sítích mezi žáky středních a vysokých škol v Jihočeském kraji je velice vysoké, bylo velice překvapivé zjištění. Kdy u otázky číslo 3 „Víte co je VPN?“ odpovědělo kladně více než tři čtvrtiny respondentů. Autor je tedy rád, že si dnes mladí lidé nebezpečí, jenž hrozí na internetu uvědomují a chrání se. Před výběrem a řešením této dané problematiky bakalářské práce na téma virtuální privátní sítě z pohledu kybernetické bezpečnosti, bylo její pojetí velice optimistické. Na toto téma člověk naráží ve své podstatě každý den. Nicméně až po několika hodin čtení všech možných knih a článků, bylo vůbec možné proniknout do složitosti tohoto tématu. Asi tím nejtěžším bylo právě ono pochopení a samotné porozumění tohoto směru a to z toho důvodu, že se dlouho nedařilo sestavit správnou strukturu, která byla nezbytná pro úplné pochopení této problematiky.

Seznam použitých zdrojů

Literární zdroje

ATKINSON, R. L. *Psychologie*. Vyd. 1. Praha: Portál, 2003.ISBN: 751-80-7178-640-3.

BÍMOVÁ, A. Počítačová kriminalita a naše doba. Praha: IDG Czechoslovakia, 1990. 137 s. ISBN 80-900872-2-1.

DĚDIČEK, D. *Facebook: jednoduše*. Brno: Computer Press, 2010. Naučte se za víkend (Computer Press). ISBN 978-80-251-3196-1

DOSTÁL, J. *Hardware moderního počítače*. Olomouc: Univerzita Palackého v Olomouci, 2011. ISBN 978-80-244-2787-4.

ECKERTOVÁ, L a D. DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5.

GLENNY, M. *Temný trh: kyberzloději, kyberpolicisté a vy*. Praha: Argo, 2013. Zip (Argo: Dokořán). 263 s ISBN 978-80-7363-522-0.

JIRÁSEK, P., NOVÁK, L., POŽÁR, J., Cyber security glossary, Praha: Policejní akademie ČR v Praze, AFCEA, 2015, 242 s. ISBN 978-80-7251-436-6

JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

KABELOVÁ, A a DOSTÁLEK L. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008 483 s. ISBN 978-80-251-2236-5.

KMOCH, P. *Informatika a výpočetní technika: pro základní školy*. Praha: Computer Press, 1997. Učebnice pro základní školy. ISBN 80-7226-015-4.

KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. 522 s. ISBN 978-80-88168-15-7.

KOŽÍŠEK, M., PÍSECKÝ V. Bezpečně na internetu. Průvodce chováním ve světě online. Praha : Grada Publishing, 2016. 176 s. ISBN 978-80-247-5595-3

KRČMÁŘ, P. Linux: postavte si počítačovou síť. Praha: Grada, 2008. Průvodce (Grada). 184 s. ISBN 978-80-247-1290-1.

MCCARTHY, L a WELDON-SIVIY D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, [2013]. ISBN isbn:978-80-904248-6-9.

SATRAPA, P. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011. CZ.NIC. 409 s. ISBN isbn978-80-904248-4-5.

SKLENÁK, V. Data, informace, znalosti a Internet. Praha: C.H. Beck, 2001. C.H. Beck pro praxi. 507 s. ISBN 80-7179-409-0.

SMEJKAL, V. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

ŠEVČÍKOVÁ, A. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6.

ŠULC, V. Kybernetická Bezpečnost. Plzeň: Čeněk A., 2018. 148 s. ISBN 978-80-7380-737-5.

VYHNÁNKOVÁ, E., LOSEKOOT, M., Jak na sítě (Ovládněte čtyři principy úspěchu na sociálních sítích), Brno: Jan Melvil Publishing, 2019, 328 s. ISBN 978-80-7555-084-2

YONAZI, J. J., SEDOYEKA, E., ARIWA, E., EL-QAWASMEH, E. e-Technologies and Networks for Development. Heidelberg: Springer, 2011. 366 s. ISBN 978-3-642-22729-5.

Elektronické zdroje

Deep web. *Comparitech* [online]. [cit. 2022-2-9]. Dostupné z:https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/

Formy VPN Client to site. *Rantdriven* [online]. [cit. 2022-3-1]. Dostupné z:https://rantdriven.com/the-difference-between-the-client-to-site-and-site-to-site-vpn-models/

Formy VPN site to site. *Rantdriven* [online]. [cit. 2022-3-1]. Dostupné z:https://rantdriven.com/the-difference-between-the-client-to-site-and-site-to-site-vpn-models

Formy VPN. *Paloaltoneworks* [online]. [cit. 2022-3-1]. Dostupné z:https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

Hardware VPN. *Macpaw* [online]. [cit. 2021-12-10]. Dostupné z:https://macpaw.com/how-to/hardware-vpn-vs-software-vpn

Hardware. T*cholidays* [online]. [cit. 2021-12-10]. Dostupné z:https://www.tcholidays.com/hardware-and-software-a-professionally-written-essay-sample

Historie(1) VPN. *Csijax* [online]. [cit. 2022-2-9]. Dostupné z:https://csijax.com/a-brief-history-of-vpn/

Historie(2) VPN. *Cactusvpn* [online]. [cit. 2022-2-9]. Dostupné z:https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/

Historie(3) VPN. *Le-vpn* [online]. [cit. 2022-2-9]. Dostupné z:https://www.le-vpn.com/history-of-vpn/

I VPN může sledovat. *SecurityGladiators* [online]. [cit. 2022-4-3]. Dostupné z:https://securitygladiators.com/vpn/advantages-disadvantages/

IP adresa. *Geeksforgeeks* [online]. [cit. 2022-1-20]. Dostupné z: https://www.geeksforgeeks.org/what-is-an-ip-address/

Kvalitní VPN stojí peníze. *SecurityGladiators* [online]. [cit. 2022-4-3]. Dostupné z:https://securitygladiators.com/vpn/advantages-disadvantages/

Kybernetická bezpečnost. *VládaČR* [online]. [cit. 2022-2-9]. Dostupné z:https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

Kyberprostor. *Technopedia* [online]. [cit. 2022-1-20]. Dostupné z:https://www.techopedia.com/definition/2493/cyberspace

Limity podnikové VPN. *SecurityGladiators* [online]. [cit. 2022-4-3]. Dostupné z:https://securitygladiators.com/vpn/advantages-disadvantages/

Limity VPN. *Forbes* [online]. [cit. 2022-4-2]. Dostupné z:https://www.forbes.com/advisor/business/software/why-use-a-vpn/

MAC adresa. *Alphr* [online]. [cit. 2022-2-9]. Dostupné z:https://www.alphr.com/does-using-a-vpn-change-your-mac-address/

NÚKIB(1). *Centrumkyberbezpečnosti* [online]. [cit. 2022-2-9]. Dostupné z:https://centrumkyberbezpecnosti.cz/novym-reditelem-nukib-se-stal-brig-general-karel-rehka/

NÚKIB(2). *NÚKIB* [online]. [cit. 2022-2-9]. Dostupné z:https://www.nukib.cz/cs/o-nukib/

Ochrana osobních dat od poskytovatele internetových služeb *Vittana* [online]. [cit. 2022-4-3]. Dostupné z:https://vittana.org/16-major-advantages-and-disadvantages-of-a-vpn

Ochrana osobních údajů. *Cookielawinfo* [online]. [cit. 2022-4-2]. Dostupné z:https://www.cookielawinfo.com/gdpr-fines-biggest-gdpr-violation-examples/

Ochrana osobních údajů z aplikací a služeb VPN. *Forbes* [online]. [cit. 2022-4-2]. Dostupné z:https://www.forbes.com/advisor/business/software/why-use-a-vpn/

Osobní údaje. *Dtest* [online]. [cit. 2022-2-9]. Dostupné z:www.dtest.cz/clanek-8588/jak-je-to-s-osobnimi-udaji-na-internetu?subscribe=292

Právní aspekty. *Fakulta informatiky Masarykovy univerzity* [online]. [cit. 2022-2-9]. Dostupné z:https://is.muni.cz/do/ics/el/sitmu/law/html/pravni-aspekty.html

Představení VPN. *Geeksforgeeks* [online]. [cit. 2021-12-10]. Dostupné z: https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/

Protokoly(1). *Geeksforgeeks* [online]. [cit. 2022-1-20]. Dostupné z:https://www.geeksforgeeks.org/types-of-internet-protocols/

Protokoly(2). *Tomsguide* [online]. [cit. 2022-1-20]. Dostupné z: https://www.tomsguide.com/features/how-does-a-vpn-work

SSL-TLS. Master [online]. [cit. 2022-6-6]. https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod/

Software VPN. *Macpaw* [online]. [cit. 2021-12-10]. Dostupné z:https://macpaw.com/how-to/hardware-vpn-vs-software-vpn

Tunelování(2). *Cybernews* [online]. [cit. 2022-1-20]. Dostupné z:https://cybernews.com/what-is-vpn/split-tunneling/

Užívání VPN OBR. *Vpnmentor* [online]. [cit. 2022-2-9]. Dostupné z:https://cs.vpnmentor.com/blog/jsou-vpn-legalni/

Užívání VPN. *Vpnmentor* [online]. [cit. 2022-2-9]. Dostupné z:https://cs.vpnmentor.com/blog/vpn-101-vpn-prirucka-pro-novacky-od-vpnmentor/

Uživatelé VPN. *Dataprot* [online]. [cit. 2022-2-9]. Dostupné z:https://dataprot.net/statistics/vpn-statistics/

Výhody a nevýhody VPN . *Vittana* [online]. [cit. 2022-4-3]. Dostupné z:https://vittana.org/16-major-advantages-and-disadvantages-of-a-vpn

Výhody a nevýhody VPN. *Forbes* [online]. [cit. 2022-4-2]. Dostupné z:https://www.forbes.com/advisor/business/software/why-use-a-vpn/

Legislativní dokumenty

181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění účinném k 1.9.2021 © AION CS 2010-2019 [cit. 4. 5. 2022].Dostupné z: https://www.zakonyprolidi.cz/.

Seznam zkratek

Dos:Denial of Service

DDos:Distributed Denial of Service

IKEv1 Internet Key Exchange

FTP:File Transfer Protocol

HTML:Hyper Text Markup Language

IP: Internet Protocol

IPv4: Internet Protocol verze 4

IPv6: Internet Protocol verze 6

IPsec: Internet Protocol Security

L2TP: Layer 2 Tunneling Protocol

LAN: Local Area Network

NAS: Network Attached Storage

NAT: Network Address Translation

PPP: Point-to-Point Protocol

PPTP: Point-to-Point Tunneling Protocol

RDP: Remote Desktop Protocol

SSL: Secure Sockets Layer

SSTP: Secure Socket Tunneling Protocol

TCP: Transmission Control Protocol

TCP/IP: Transfer Control Protocol/Internet Protocol

TLS: Transport Layer Security

VNC: Virtual Network Computing

VPN: Virtual Private Network

WAN: Wide Area Network

Seznam tabulek a grafů