Život s internetem

Vrbenský Jan P1A

Obsah

1. Úvod 3

2. Komunikace na internetu 3

3. Netiquette 3

4. Nástrahy internetu 4

4.1. Spam 4

4.2. Hoax 4

4.3. Physhing 4

4.4. Malware 4

4.4.1. Počítačové viry a červy 4

4.4.2. Trojský kůň 4

4.4.3. Rootkit 4

4.4.4. Backdoor 5

4.5. Ransomware 5

4.5.1. Šifrovací ransomware 5

4.5.2. Nešifrovací ransomware 5

5. Jak se chránit 5

5.1. Antivir 5

5.2. Firewall 5

5.2.1. Paketový filtr 5

5.2.2. Aplikační brána 6

5.2.3. Stavový paketový filtr 6

5.2.4. Stavový paketový filtr s kontrolou známých protokolů a IDS 6

6. Závěr 6

7. Zdroje 7

Úvod

Můj referát bude o životu s internetem, protože ten se stává čím dál tím víc součástí našeho života. V tomto referátu bych chtěl psát o nebezpečí na internetu, jak se správně chovat na internetu. Také se zmíním o různých škodlivých softwarech. Na druhou stranu se budu zmiňovat o zabezpečovacích programech, jako jsou antiviry, nebo firewall.

1. **Komunikace na internetu**

Komunikace na internetu má své výhody, ale i nevýhody. Mezi výhody bychom mohli počítat to, že se můžeme spojit s lidmi z celého světa, anonymita, svobodné vyjadřování. Mezi nevýhody bychom mohli zařadit falešné identity, setkání s lidmi, se kterými bychom normálně nemluvili, kyberšikana, kyberkriminalita atd. Komunikaci na internetu můžeme rozdělit na 2 druhy. Na komunikaci asynchronní a synchronní.

A) Asynchronní komunikace je jednoduše řečeno komunikace při které nepotřebujeme okamžitou odpověď od člověka, kterému píšeme. Stačí nám odpověď třeba i do pár dní. Mezi asynchronní komunikaci můžeme zařadit e-mail.

B) Synchronní komunikaci volíme, pokud potřebujeme odpověď co nejdříve. K takové komunikaci se nejvíce hodí různé chatovací aplikace, jako je třeba facebook, instagram, messenger, které jsou všechny vlastněné facebookem, nebo třeba dnes již téměř nepoužívaný skype.

1. **Netiquette**

Netiketa (netiquette) je soubor pravidel správného chování, stejně jako etiketa, až na to, že internetu. Vzhledem k tomu, že na internetu tráví lidé dost času, proto vznikla pravidla, jak se chovat, ty pravidla jsou:

1. Nezapomeň, že na druhém konci je člověk, ne počítač.
2. Dodržuj pravidla slušného chování, stejně, jako v reálném světě.
3. Slušně si zjisti, s kým mluvíš
4. Ber ohled na druhé
5. Je dobré psát s diakritikou
6. Pomáhej v diskuzích
7. Nerozpoutávej „internetové války“ (modré, nebo zlaté šaty)
8. Respektuj soukromí ostatních
9. Nezneužívej svojí moc a vědomosti
10. Odpouštěj ostatním, pokud chybují
11. Nerozesílej hoax
12. Nerozšiřuj spam/reklamu
13. Neporušuj autorská práva

1. Nástrahy internetu
   1. Spam

Spam je druh sdílení ve velkém měřítku. Většinou jde o reklamu, která nám chodí do e-mailu, nebo je v komentářích na sociálních sítích. V Evropě je možné postihnout firmu, která šíří spam, ale pouze pod podmínkou, že daná firma sídlí v EU.

* 1. Hoax

Jde o druh zprávy na internetu, která je ale falešná. Většinou šíří nepravdivé, nebo falešné zprávy. Toto může být potencionálně nebezpečné pro lidi, kteří nevědí, že se jedná o hoax. Může obsahovat špatnou radu, jak se něčeho zbavit, nebo naopak vylepšit, ale ve skutečnosti se vše pouze zhorší. Hoax ale nemusí být vždy chtěný. Před asi půl rokem jeden zpravodajský web zveřejnil spoustu článků o úmrtí celebrit, které byli stále na živu. Hned po zjištění, co se stalo, se všechny tyto články stáhly z webu.

* 1. Phishing

Phishing je druh internetového podvodu. Lidé, co tuto techniku používají, se snaží získat citlivé informace, jako jsou třeba informace o kreditní kartě, hesla, informace o internetovém bankovnictví atd. Podkategorie phisingu by byl catphishing, při kterém se člověk na internetové seznamce vydává za druhé pohlaví. Ale cíl je stále stejný, získat citlivé informace.

* 1. Malware

Je hromadné označení pro škodlivé programy, které provádějí akce, které nejdou povolené uživatelem. Typy malwaru:

* + 1. Počítačové viry a červy

Jde asi o nejznámější typ malwaru. Počítačový virus se po spuštění softwaru začne šířit na další spuštěné aplikace, kde většinou poškozuje, Počítačový červ je rozdílný od viru v tom, že se přenáší automaticky, nepotřebuje zásah uživatele.

* + 1. Trojský kůň

Pomocí trojského koně se dá docela dobře šířit škodlivý software, protože se maskuje, jako něco jiného. Trojský kůň se maskuje, jako jiný, třeba i užitečný program, ale po nainstalování se ukáže, že jde o škodlivý program, který nám může mazat soubory, nebo nainstalovat jiný škodlivý software.

* + 1. Rootkit

Jde o sadu programů, které maskují škodlivý software, aby zůstal skrytý.

* + 1. Backdoor

Je metoda, obcházení zabezpečení. Může se stáhnout jeden, nebo více backdoorů, ty usnadňují budoucí přístup k zařízení.

* 1. Ransomware

Je jeden z dalších škodlivých softwarů. Tento typ softwaru blokuje zařízení, anebo šifruje soubory, data v něm uložené. Po oběti tohoto softwaru se většinou chce výkupné. Byl velice populární v Rusku, ale postupně se rozšířil i globálně.

* + 1. Šifrovací ransomware

Poprvé se objevil v roce 1989. Tento software přesvědčoval, že počítači vypršela licence a zašifroval všechny soubory na disku, dokud uživatel nezaplatil za odemknutí zařízení.

* + 1. Nešifrovací ransomware

Tento ransomeware pouze zobrazoval obrázky, kterými zamezoval přístupu k zařízení. Následně vyžadoval zaslání SMS zprávy za cenu asi 10 dolarů. Poté se zařízení opět zpřístupnilo, protože obrázky zmizely.

1. Jak se chránit
   1. Antivir

Antivirové programy jsou počítačové softwary, které slouží k rozpoznání a zneškodnění počítačových virů a jiného malwaru.

K zjištění malwaru se požívají 2 techniky:

1) Prohlížení souborů v paměti, pokud se nějaký nepodobá nějakému známému viru, nebo jinému malwaru.

2) Detekce podezřelého chování programů, jestli náhodou není nakažený virem, či jiným malwarem.

* 1. Firewall

Je zařízení, které zabezpečuje síťový provoz. Funguje, jako kontrolní body, které definují pravidla mezi sítěmi, které odděluje.

Firewall měl během vývoje spoustu kategorií:

* + 1. Paketový filtr

Nejjednodušší forma. U tohoto firewallu pravidla přesně určí, z jaké adresy se můžeme kam dostat. Není tak bezpečné zabezpečení, ale dokáže přenést rychle velké množství dat.

* + 1. Aplikační brána

Uživatel se přepojoval pomocí aplikační brány, takže šlo v dvojí spojení. Kontrola připojení se provádí na sedmé, aplikační, vrstvě. Oproti paketovým filtruj je mnohem bezpečnější, ale jsou také mnohem pomalejší.

* + 1. Stavový paketový filtr

Je podobný paketovým filtrům, až na to, že již objevené trasy mezi servery, se mohou vyhodnotit, jako bezpečné, takže bude přechod rychlejší a bezpečnější. Má také mnohem snažší konfiguraci, než paketové filtry, nebo aplikační brány. To snižuje možnost chybného nastavení.

* + 1. Stavový paketový filtr s kontrolou známých protokolů a IDS

Pracují podobně, jako antiviry, dokáže odhalit útok. Jsou schopny kontrolovat spojení procházejících dat mezi protokoly a aplikací. Mají velice vysokou úroveň bezpečnosti, relativně snadnou konfiguraci. Je složitější, než ostatní firewally a je pomalejší.

1. Závěr

Děkuji za pozornost, doufám, že jste si vzali něco z tohoto referátu a budete si na internetu dávat větší pozor, protože jak vidíte, na internetu je spousta nástrah. Podle mého názoru je internet jeden z nejlepších, ale zároveň nejhorších vynálezů, které lidstvo vytvořilo, protože je to místo, kde je mnohem větší svoboda, než v reálném světě. Na internetu si toho každý dovolí víc, než v reálném světě, proto bychom si měli dávat na internetu pozor, s kým se bavíme a co děláme.

Zdroje

**CZ.NIC. 2016.** Neboj se internetu. *nebojseinternetu.cz.* [Online] 2016. https://www.nebojteseinternetu.cz/page/3416/on-line-komunikace/.

**Wikimedia Foundation, Inc. . 2021.** Wikipedia. *cz.wikipedia.org.* [Online] 6. Prosinec 2021. https://cs.wikipedia.org/wiki/Antivirov%C3%BD\_program.

**Wikimedia Foundation, Inc. 2021.** Wikipedia. *cz.wikipedia.org.* [Online] 26. Listopad 2021. https://cs.m.wikipedia.org/wiki/Netiketa.

**Wikimedia Foundation, Inc. 2021.** Wikipedia. *cz.wikipedia.org.* [Online] 2. Prosinec 2021. https://cs.wikipedia.org/wiki/Malware.

**Wikimedia Foundation, Inc. 2021.** Wikipedia. *cz.wikipedia.org.* [Online] 25. Prosinec 2021. https://cs.wikipedia.org/wiki/Phishing.

**Wikimedia Foundation, Inc. 2021.** Wikipedia. *cz.wikipedia.org.* [Online] 26. Prosinec 2021. https://cs.wikipedia.org/wiki/Ransomware.

**Wikimedia Foundation, Inc. 2021.** Wikipedia. *cs.wikipedia.org.* [Online] 10. Březen 2021. https://cs.wikipedia.org/wiki/Firewall.

**Wikimedia Foundation, Inc. 2021.** WIkipedia. *cz.wikipedia.org.* [Online] 21. Listopad 2021. https://cs.wikipedia.org/wiki/Hoax.

**Wikimedia Foundation, Inc. 2020.** Wikipedie. *cz.wikipedia.org.* [Online] 26. Únor 2020. https://cs.wikipedia.org/wiki/Komunikace\_v\_kyberprostoru.