Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze diplomové práce

Útoky a hacking v online prostředí a ochrana před nimi

Bc. Lukáš Gregora

1 Souhrn

Diplomová práce je zaměřena na útoky a hacking v online prostředí a ochranu před nimi. V přehledu řešené problematiky byl definován pojem hacking a s ním spjaté pojmy, včetně rozdělení hackerů podle chování a smýšlení. V dalších částech byl zachycen historický, aktuální a budoucí vývoj hackingu s důležitým pohledem na právní legislativu, která je z hlediska právních systémů odlišná. Za využití aktuálních a hackery využívaných technologií, byla provedena sumarizace aktuálních typů útoků a u zvolených typů byla provedena jejich implementace v rámci izolovaných webových stránek s následným souhrnem možných ochran. Praktická část je zaměřena na využití zařízení WiFi Pineapple k analýze současné situace uživatelů využívajících veřejných Wi-Fi sítí a jejich zařízení. Za využití výše zmíněného zařízení, byl proveden výzkum formou pokusných měření a na základě jejich statistické a analytické analýzy bylo zjištěno, že až 17 % zaznamenaných zařízení je potencionálně napadnutelných zvolenou formou útoku. V rámci následné analýzy bylo provedeno vyhodnocení stanovených hypotéz, očekávání a předpokladů, které byly zaměřeny na vliv okolních aspektů a hodnoty zařízení na využívání veřejných Wi-Fi sítí.

Klíčová slova: útoky, hacking, bezpečnost, ochrana, online, internetové technologie, WiFi

2 Cíl práce a metodika

Hlavním cílem diplomové práce je definování a simulace útoků v online prostředí a možné způsoby jak se jim bránit.

Součástí dílčích cílů je:

- sestavení uceleného přehledu historického, současného a budoucího vývoje hackingu a technologií, které se v online prostředí využívají,
- sumarizace možných forem útoků v online prostředí a jejich četností, které budou implementovány na izolovaném prostředí s názornou ukázkou možných způsobů ochrany,
- zachycení aktuálního pohledu na hacking v online prostředí z právního hlediska,
- vytvoření příkladů využití zařízení, které umožňuje sledovat provoz Wi-Fi sítí.

Na základě zjištěných poznatků, bude provedena diskuse a výsledky pozorování. Formulace závěrů.

2.1 Metodika

Teoretická část diplomové práce je založena na studiu odborných informačních zdrojů. Praktická část je zaměřena na sestavení uceleného přehledu metod použitých k útokům v online prostředí, způsoby ochran před nimi a srovnání jejich četností. Útoky budou simulovány na izolovaných webových stránkách, které budou záměrně obsahovat bezpečnostní nedostatky, na kterých budou demonstrovány formy útoků. K testování, simulaci a ověřování některých útoků bude využito zařízení WiFi Pineapple, které umožňuje monitorovat provoz Wi-Fi sítě. Na základě získaných poznatků ze simulací a praktického využití uvedeného zařízení bude provedena analýza výsledků, diskuze stavu zabezpečení sítě Wi-Fi a chování uživatelů.

3 Výsledky a diskuse

Výzkum, který spočíval v analýze zařízení a chování uživatelů veřejných WiFi síti, byl proveden za využití zařízení WiFi Pineapple a spolupracujících dílčích částí, které vytvořily mobilní jednotku pro sběr kvantitativních a kvalitativních dat. Data byla dále vyhodnocena, analyzována a verifikována za použití statistických (*SAS*) a analytických nástrojů (*QlikView* a *Microsoft Excel*), které poskytly hlubší pohled na zkoumanou problematiku a umožnily vyhodnotit stanovené hypotézy, očekávání a předpoklady.

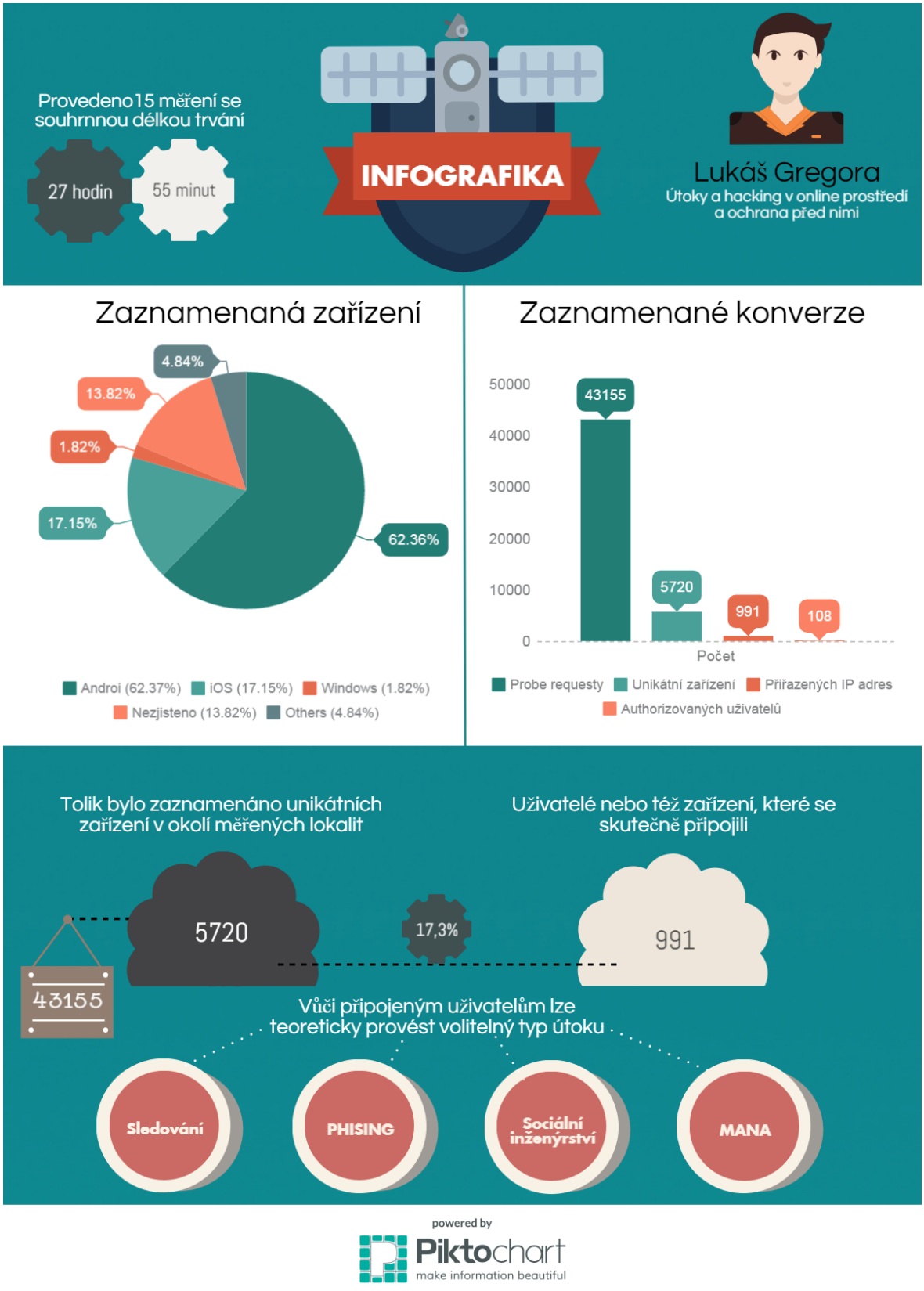
Sběr dat probíhal v prvním čtvrtletí roku 2017 za nepříliš příznivých klimatický podmínek, které následně byly zohledněny i v analýze okolních vlivů na výsledky měření. Data byla shromažďována v několika konverzních úrovních, které závisely na úrovni aktivity připojujícího se uživatele. Konverze jsou prezentovány v rámci analýzy naměřených dat a jsou členěny na úrovně: počet zachycených požadavků o připojení, počet unikátních zařízení, počet skutečně připojených zařízení a počet autorizovaných uživatelů. Z analýzy konverzí bylo zjištěno, že k vysílané skupině veřejných Wi-Fi přípojných bodů, se připojilo až 17 % ze zachycených okolních zařízení, které v okolí zařízení vysílaly požadavek o připojení k Wi-Fi síti (*probe request*). Jedná se o poměrně znepokojující procentuální hodnotu, která v konečném důsledku vyjadřuje počet zařízení, vůči kterým by mohl být veden útok formou sociálního inženýrství, sledování síťové komunikace nebo jinou sofistikovanou formou. Je třeba zdůraznit, že se jedná o aktivity, jejichž provozováním v reálném provozu se útočník dopouští jednání, které je v rozporu se zákonem a autor práce se s nimi neztotožňuje ani neposkytuje návod k jejich realizaci. Z tohoto důvodu byl výzkum prováděn takovou formou, která nikterak nepoškozuje připojené uživatele, pouze jim poskytuje možnost připojení k internetové síti prostřednictvím přípojného bodu veřejné WiFi sítě a to na základě jejich potřeb.

Následný soubor analýz, založený na statistických a analytických verifikací odhalil, že naměřené hodnoty jsou značně ovlivňovány okolními faktory, které byly za pomocí metody váženého bodového součtu z oboru vícekriteriální analýzy variant znormovány, aby umožnily objektivní znázornění jejich vlivu na měřené hodnoty. Analýza byla provedena formou proporcionálního bublinového grafu, na kterém byla na osu *X* nanesena funkce užitku, na osu *Y* datum měření a pro znázornění proporcí počet připojených

uživatelů. Následnou analýzou, která byla založena na testování normality cenové hladiny připojených zařízení, která byla doplněna o běžné ceny použitých zařízení, bylo v rámci grafického znázornění *boxplotu* možné pozorovat odlehlé hodnoty, které vylučují normální rozdělení výběru. Protože ale byl použit výběr, který má větší množství měření než 30, proto bylo použito *Kolmogorovova-Smirnovova* testu. Použitý test nezamítnul (potvrdil) nulovou hypotézu, která vyjadřovala, že výběr pochází z normálního rozdělení a na základě které bylo možné stanovit, že hodnota zařízení nemá vliv na využívání veřejných Wi-Fi sítí.

Zařízení byla analyzována z hlediska použitého operačního systému a aktuálnosti jeho verze. Při analýze typu operačního systému, došlo k prakticky identické shodě rozložení použitých zařízení s jejich rozdělením na trhu, které vycházelo z analýzy společnosti *Net Applications.com*. Detailnější rozbor zaměřený na verzi operačního systému poukázal na fakt, že změřená mobilní zařízení disponují poměrně aktuálními verzemi operačního systému a tím i větší bezpečností zařízení. Důležitou roli zde zastupuje fakt, že mobilní zařízení jsou spotřební elektronikou, která se pod tlakem výrobců neustále obměňuje, a tím se převážně dostávají nové verze operačního systému do oběhu.

Analýzou zabezpečení veřejných Wi-Fi sítí bylo zjištěno, že bezpečnostní nedostatky, kterými disponují, jsou technického charakteru a jejich případné úpravy by postihly celkovou funkcionalitu sítí. Uživatel se může v rámci veřejných Wi-Fi sítí bránit útokům na základě prevence, která je založena na jejich nevyužívání a orientovat se směrem k mobilnímu připojení třetí a čtvrté generace (sítě druhé generace jsou prostřednictvím falešných telefonních věží napadnutelné – downgrade šifrování). Z hlediska aktivní ochrany se jako účinná jeví využívání VPN, případně přistupovat k zabezpečeným webovým stránkám s prohlížečem podporujícím HSTS.



Obrázek 1 - Infografika provedeného výzkumu

4 Vybraná bibliografie

1) **BEAVER, Kevin, DAVIS, Peter T**.. Hacking Wireless Network For Dummies. 5. vydání. Vydavatel: John Wiley & Sons, Inc, 2005. ISBN 978-0764597305.
2) **CLARKE, Justin**. SQL Injection Attacks and Defense. 2. vydání. Vydavatel: Syngress, 2012. ISBN 978-1597499637.
3) **CHAUHAN, Sudhanshu, PANDA, Nutan Kumar.** Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. 1. vydání. Vydavatel: Syngress, 2015. ISBN 978-0128018675.
4) **DVORSKÝ, Marek.** Základy bezdrátových komunikací pro integrovanou výuku VUT a VŠB-TUO. [Online] Ostrava : Vysoká škola báňská - Technická univerzita Ostrava, 2014. ISBN 978-80-248-3557-0.
5) **KONDA, Matt a CURIEL, Johanna**. OWASP. [Online] OWASP Foundation, 2016. [Citace: 8. 11 2016.] Dostupné z: https://www.owasp.org.
6) **KÜMMEL, Roman**. Cross-Site Scripting v praxi. 1. vydání. Vydavatel: SOOM, 2011. ISBN 978-80-86062-34-1.
7) **KÜMMEL, Roman a KLUBAL, Martin**. SOOM.cz. SOOM.cz. [Online] SOOM.cz, © 2017. [Citace: 21. 10 2016.] Dostupné z: www.soom.cz. ISSN 1804-7270.
8) **LECKY-THOMSON, Ed a NOWICKI, Steven D**. PHP 6 Programujeme profesionálně. Brno : Computer Press, 2010. ISBN 978-80-251-3127-5.
9) **Parlament ČR**. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Sbírka zákonů. [Online] 2014. [Citace: 15. 2 2017.] Dostupné z: https://www.nbu.cz/.
10) **PASSERI, Pablo**. Cyber Attacks Statistics. HACKMAGEDDON. [Online] 2017. [Citace: 12. 3 2017.] Dostupné z: http://www.hackmageddon.com.
11) **SCAMBRAY, Joel, McCLURE, Stuart, KURTZ, George**. Hacking bez tajemství. 1. vydání. Vydavatel: Computer Press, 2001. ISBN 80-7226-549-0.
12) **SCAMBRAY, Joel, SHEMA, Mike**. Hacking bez tajemství - Webové aplikace. 1. vydání. Vydavatel: Computer Press, 2003. ISBN 80-7226-769-8.
13) **TRIGAUX, Robert**. A history of hacking. St. Petersburg Time. [Online] 2010. [Citace: 24. 10 2016.] Dostupné z: http://www.sptimes.com.