NÁSTRAHY INTERNETU

aneb

informační (ne)bezpečnost

MAREK KOVALČÍK

Upozornění pro čtenáře a uživatele této knihy

V knize jsou popisovány kybernetické útoky, které se v reálném světě běžně dějí. Cílem knihy není nikoho nabádat k nelegálním činnostem, nýbrž šířit všeobecné povědomí o principech v oblasti kybernetické bezpečnosti a zvyšovat tak šance na obranu proti internetovým hrozbám. Hackování bez souhlasu majitele systému je nelegální a může vést až k zahájení trestního řízení. Autor knihy nenese odpovědnost za to, jak čtenář s předávanými informacemi naloží.

I. vydání

ISBN 978-80-11-05320-8 (pdf)
ISBN 978-80-11-05321-5 (ePub)
ISBN 978-80-11-05322-2 (Mobipocket)

Obsah

Věnováno všem, kteří se aktivně podílejí na
zlepšování úrovně kybernetické bezpečnosti ve světě.
A také těm, co si uvědomují křehkost našich systémů
a neberou ji na lehkou váhu.

Úvodní slovo autora

Není pochyb o tom, že se moderní technologie stávají stále silnější součástí našich každodenních životů. Usnadňují nám komunikaci s našimi blízkými, rodinou a přáteli. Pomáhají nám zjišťovat si informace a zefektivňují naše každodenní činnosti – od sledování dění ve světě přes zábavu a práci až po nakupování na internetu či přístup do internetového bankovnictví. Mnoho z nás bere funkčnost používaných aplikací jako naprostou samozřejmost a mnohdy nám nedochází, jak jsou všechny tyto systémy složité, propojené mezi sebou a jaká bezpečnostní rizika přináší jejich používání. Bezpečnostním rizikem mám na mysli právě situace, kdy se vám dostane někdo do vašeho e-mailového účtu, získá přístup k různým dokumentům nebo například k sociálním sítím a v tom nejhorším případě právě i do bankovnictví či k jiným velmi citlivým datům, která jsou pro vás důležitá.

Nejčastějším argumentem, se kterým se setkávám, je: „Mně se to stát nemůže, co by od mě asi tak chtěli?“ Zde si dovolím použít Murphyho zákon – „Co se může pokazit, to se pokazí“ – a aplikovat ho na tématiku

této knihy: „Co se dá hacknout, bude hacknuto.“ Mým cílem není nikoho zbytečně strašit, ale naopak šířit všeobecné povědomí o reálných hrozbách na internetu, možnostech, jak se jim efektivně bránit, a ideálně být inspirací pro další technologické nadšence, kteří uvažují o kariéře v kybernetické bezpečnosti.

Tato kniha není cílena na profesionály v oblasti informačních technologií, ale naopak se zde budu snažit vysvětlovat principy hackování tak, aby byly srozumitelné a informačně přínosné i pro „neajťáky“. A stejně tak pro lidi v oboru, co například přemýšlejí nad rozšířením svých obzorů právě do problematiky informační bezpečnosti.

Udržování a zvyšování úrovně bezpečnosti je povinností nás všech. Jedná se o velmi křehkou součást řetězce, v němž jediná chyba může vyvolat kaskádovou reakci s vážnými následky. Můžeme to vidět v praxi, kdy se i ti největší světoví technologičtí giganti často potýkají s bezpečnostními incidenty, únikem citlivých dat a nedostupností klíčových systémů. Budu se vám v této knize snažit vysvětlit, proč k hackerským útokům dochází, co je jejich příčinou a jak se jim efektivně bránit. Nečekejte zdlouhavé poučky z všeobecných materiálů, pokusím se vždy vycházet z příkladů z vlastní praxe

a předat informace, které vám pomohou nejen lépe se orientovat ve světě jedniček a nul, ale také uvažovat nad jejich významem v širších souvislostech.

Jdeme na to!

Jak jsem se stal hackerem

Odjakživa jsem měl zálibu v počítačích. Pamatuji si, že mým úplně prvním byl PC s Microsoft Windows 95. Dneska je to již kus historie, ale vzpomínám si, že při prozkoumávání systému jsem se jako malý občas dostal do bodu, kdy jsem se náhodou ocitl v terminálovém prostředí nebo počítač zobrazil „modrou smrt“ a bylo třeba se z toho nějak vymotat. Nebudu lhát, tenkrát moje IT znalosti byly nulové. Zprovoznění systému k životu tak většinou spočívalo v tom, že jsem vyrval napájecí kabel ze zdi a pak počítač opětovně zapnul.

Na základní škole pro mě začala éra počítačových her. Před osmnácti lety ještě panovala doba, kdy jsme se schovávali do virtuality před realitou. Dnes už je možná situace opačná – utíkáme do přírody před každodenním sezením u počítače. Hry byly důležitou součástí mého života. Nejen, že mě učily svižně ovládat počítač a zlepšovat se v angličtině, ale také řešit problémy. V té době ještě nebyly hry tak „dokonalé“ jako dnes, a proto jsme museli často řešit, že něco nefunguje či přestalo fungovat, a museli hledat cesty k nápravě. To, alespoň pro mě, znamenalo šťourat se v systémových

nastaveních a hledat cesty k řešení různých problémů – s připojením k síti, s ovladači grafických karet, s instalováním potřebného softwaru a tak dále. Pamatuji si také, že jsme často zkoušeli různé možnosti „cheatování“ s cílem získat výhody před ostatními hráči. Někdy se to povedlo, někdy jsem si neuváženě zaviroval počítač. I to ale pro mě byla velmi cenná zkušenost, protože jsem se naučil přeinstalovat operační systém, tenkrát ještě Windows XP.

Následoval posun na střední školu. Vybral jsem si průmyslovou střední školu v Opavě, kde jsem se vrhl do studia informačních technologií. Byl to pro mě první moment, kdy jsem se setkal s programováním, a když jsme měli v rámci projektu vytvořit jednoduchou kalkulačku, co uměla jen sčítat, odečítat, násobit a dělit, byl to pro mě úplně nový pohled na to, jak počítače fungují. Úkoly a projekty se stále komplikovaly. Měl jsem kolem sebe spolužáky, kterým to šlo mnohem lépe než mně. Nicméně jsme byli velmi dobrý kolektiv. Měli jsme motivaci se neustále zlepšovat a každý chtěl mít ve výsledku lepší projekt než ostatní. Panovala mezi námi zdravá rivalita. Kromě programování jsme se věnovali také počítačovým sítím a ve druháku jsem se poprvé setkal s Linuxem. Učili jsme se pracovat čistě

v terminálovém prostředí, konfigurovat a využívat počítačové sítě. Jednou jsme dostali za úkol pokusit se „nabourat“ do počítače spolužáka a vypnout ho. Díky spolupráci v týmu jsme na to nakonec přišli a povedlo se! Když se zpětně ohlédnu, byla to moje úplně první zkušenost s hackováním. Nemusím snad zdůrazňovat, že nás to všechny moc bavilo. Podobné experimenty minimálně ve mně stále prohlubovaly ten chtíč dozvědět se více.

Nastoupil jsem univerzitu v Brně. Bylo fajn, že řada přátel ze střední se rozhodla stejně. Začali jsme se velmi intenzivně věnovat programování, počítačovým sítím a operačním systémům. Již během studií jsem začal pracovat jako junior programátor, ale po čase mi došlo, že celodenní programování není úplně pro mě. Hledal jsem tedy dál a začal pracovat v auditní společnosti, kde jsem nabíral zkušenosti ohledně fungování velkých českých i mezinárodních organizací. Začal jsem se věnovat kybernetické bezpečnosti. Obor to byl pro mě relativně nový, o to více mě ale fascinoval. Díky podpoře ve firmě jsem mohl začít pracovat na nových a zajímavých projektech, prošel jsem řadou kurzů, získal pár certifikací. Teoretický základ ze studií mi v pracovním životě velmi pomohl, ale praxe je

nenahraditelná. V momentě, kdy jsem začal pracovat na reálných projektech – hackování IT prostředí a aplikací klientů – dostal jsem na svět okolo opět nový pohled: Hrozby na internetu jsou reálné a jsou všude okolo nás.

Nejvíce se mi líbí, že je informační bezpečnost neustále a velmi rychle se rozvíjející obor. Denně vzniká spousta nových nástrojů, metodik. Díky tomu, že se jedná o velmi atraktivní obor, kterému se začíná věnovat více a více lidí, vznikají komunity, které mezi sebou sdílejí know-how a scházejí se na různých událostech a konferencích. I po několika letech v praxi se stále učím nové věci, mimo jiné také od starších, ale i mladších kolegů, kteří často přicházejí s novými a originálními způsoby řešení různých problémů. Etický hacking je za mě velmi komplexní prací, protože slučuje techniku a jednání s lidmi. Hacker musí být kreativní, soběstačný, s dobrým kritickým myšlením. Pokud to sesumírujeme, jedná se o práci, která je různorodá a velmi naplňující, když se vám nějaký systém opravdu podaří hacknout.

I. Kdo je to hacker, co je to hacking?

Jak jsem slíbil v úvodu knihy, nechci zde opakovat žádné všeobecné poučky, které si může kdokoliv najít rychlým vyhledáváním. Místo toho se pokusím vlastním pohledem popsat, co pro mě tyto pojmy znamenají a jak je vnímám já. Hacker je podle mě kdokoliv, kdo se snaží zneužívat fungování počítačových systémů. To znamená používat je k účelům, ke kterým nebyly vytvořeny.

Vytváření podvodných webových stránek, posílání falešných e-mailů s cílem získat od uživatele citlivé informace, peníze či přístup k jeho počítači. Snaha o prolomení hesel WiFi sítí nebo vytváření různých škodlivých programů, aktivní útoky na dostupné systémy – to vše bych souhrnně označil jako hacking.

Obecně jsou hackeři velmi šikovní ajťáci, kteří zkoumají fungování a nastavení počítačových systémů s cílem odhalovat jejich chyby a slabiny. Existence těchto chyb a slabin je důvodem, proč je hackování vůbec možné. Všechny používané systémy ve světě jedniček

a nul vytvořili lidé. Člověk není tvor dokonalý a dělá chyby. Právě naše nedokonalost je důvodem, proč počítačové systémy obsahují chyby, které se mohou projevovat částečnou nebo úplnou nefunkčností. Přirovnal bych to například k učení se gramatiky. Nelze se za jeden den naučit vše, učíme se po malých krůčcích. Od jednotlivých písmenek, přes skladbu slov a vět. Trvá nám roky, než se naučíme číst a psát bez chyb. Podobné je to při tvorbě počítačových programů a systémů. První počítač byl spuštěn v roce 1944 a od dnešních moderních počítačů se velmi lišil. Zpět k analogii s gramatikou – získali jsme funkční počítač, naučili jsme se písmenka. O 25 let později v roce 1969 byla spuštěna první počítačová síť – naučili jsme se skládat věty. Systémy i počítačové sítě se od té doby velmi změnily, jsou rychlejší, výkonnější, uživatelsky přívětivější a dokážeme s nimi řešit každodenní úlohy – naučili jsme se psát souvislé texty. S narůstajícími možnostmi roste také komplexita těchto systémů a není v silách jednoho člověka ovládat všechny aspekty IT. Vznikají specializované role na vývoj, testování, management, bezpečnost. Kvůli této komplexnosti děláme i po 80 letech od uvedení prvního počítače chyby v jejich používání a vytváření. Máme písmena, skládáme slova,

věty i celé texty, ale ještě je mnoho práce před námi, než dokážeme napsat celý diktát bez jediné chyby.

Etický a neetický hacking

Existují dvě hlavní kategorie hackerů – neetičtí a etičtí. Neetický, nebo také „black-hat" hacker je ten, o kterém můžete slyšet nejčastěji. Je to ten cool chlápek z filmů a seriálů, který se během minuty naboural na servery FBI, NASA a vlastně kamkoliv, kam se mu to zrovna hodí.

V reálném světe to tak jednoduché není, ale taky to není nereálné. Nicméně hlavní charakteristikou neetického hackera je fakt, že svou činnost provádí ilegálně. Teď se možná sami sebe v duchu ptáte – „Ono existuje něco jako legální hacking?". Ano, existuje, a za chvíli se k němu dostanu.

Co je vlastně motivací black-hat hackera, proč útočí na počítačové systémy, společnosti či lidi? Hackování, to neetické, by se dalo stručně popsat jako kybernetický zločin. Motivace může být často stejná jako při jiných reálných zločinech – někoho okrást, někomu ublížit. Možná jste se již setkali s termínem ransomware?

Budu se mu detailněji věnovat v dalších kapitolách, ale ve zkratce se jedná o formu vydírání. Představte si scénář, kdy se hacker zmocní vašich digitálních účtů, získá přístup k vašim souborům a výměnou za jejich navrácení nebo příslib nezveřejnění požaduje peníze. Teď jsem vám ve stručnosti popsal princip útoku, který se v reálném světě opravdu děje. Už docela dává smysl pojmenování „neetický hacking“, že?

Na druhé straně stojí etičtí nebo také „white-hat“ hackeři. Jedná se o profesionály v oblasti kybernetické bezpečnosti, kteří provádějí svoji činnost naprosto legálně. To v praxi znamená, že cíleně a řízeně útočí pouze na systémy, ke kterým mají souhlas jejich vlastníka. Můžete se také setkat s termínem „penetrační testování“, což je vlastně činnost prováděná etickými hackery. Pravdou je, že etičtí hackeři využívají naprosto stejné techniky, nástroje a postupy jako jejich protipóly, a proto jsou schopni věrohodně simulovat reálné útoky. Nyní by se někdo mohl zeptat, proč by si někdo chtěl najímat hackera, aby útočil na jeho systém či aplikace? Jde o formu testování. Pro společnosti je mnohem lepší, když jim bezpečností chyby odhalí někdo, kdo jim je zároveň pomůže opravit, než někdo, kdo by je zneužil ve vlastní prospěch.

Z vlastní zkušenosti můžu říci, že celé hackování je taková forma hry. Hledáte chyby, které se snažíte zneužít, a vždy se pokoušíte být o krok před ostatními. Trénink etických hackerů často obsahuje různé formy soutěže, kde se účastníci mezi sebou předhánějí v rychlosti či kreativitě řešení. Někteří však zajdou dále a připravené simulace jim už nestačí. Pustí se do hackování reálných systémů, ale bez motivace někomu ublížit. Chtějí si například sami sobě nebo i ostatním dokázat, že jsou ti nejlepší. Pokud se jim povede nějaký systém úspěšně napadnout, většinou informují vlastníka a „jdou o dům dál". Takovým hackerům říkáme „gray-hat". Stojí na pomyslném prahu mezi etickými a neetickými hackery, ale v podstatě je jejich činnost také nelegální, jelikož nepracují se souhlasem vlastníka systému.

Od začátečníků po špiony

Již víme, že existuje určité dělení hackerů podle jejich cíle, ale co například podle jejich schopností či zdrojů? V různých časopisech, blozích, knihách a videích se můžeme setkat dělením do velké spousty kategorií. Pokusím se vám zde popsat ty nejčastější a nejpoužívanější.

Začátečníci, nazýváni také jako „script-kiddies“, jsou lidé, kteří se tomuto oboru teprve učí, snaží se proniknout do všech koutů informační bezpečnosti. Sice zatím nemusí rozumět všem aspektům toho, co provádějí, ale i oni mohou využívat dostupné nástroje a metody k provádění reálných útoků. Je pravda, že tyto útoky nebudou příliš sofistikované a jejich šance na úspěch v reálném světě bude mizivá, přesto se mohou někdy povést. Setkal jsem se také s případy, kdy nezkušení nadšení začátečníci omylem uškodili sami sobě. Buď si omylem infikovali vlastní počítač, nebo třeba vyzkoušeli zaútočit na reálný cíl, ale bez uvědomění si všech následků. Jak jsem již nastínil dříve, hackování bez souhlasu majitele systému je nelegální. Profesionální hackeři na rozdíl od začátečníků dokáží své aktivity dobře maskovat, aby nebyli jednoduše dohledatelní.

Setkal jsem se již i s případy, kdy si někdo snažil vyzkoušet principy nějakého útoku, ale byl rychle odhalen a musel vysvětlovat důvody svého jednání. V tomto případě se jednalo o jednoduchý a snadno odhalitelný pokus, díky tomu také nedošlo k žádným škodám a stačila pouze omluva. Nicméně to dokazuje, že hackování není pro každého a nezkušený začátečník se může dostat i do vážných problémů. Slovy strýčka Bena – „s velkou mocí přichází také velká zodpovědnost“.

Když se posuneme ve škále kousek dále, můžeme nalézt kategorii hacktivistů. Zde už se může jednat o schopné až profesionální hackery, kteří jsou internetovou obdobou aktivistů. Přestože jejich primární cíle mohou být naprosto čisté a myšlenky nevinné, i jejich počínání naplňuje podstatu nelegální činnosti. Představte si nespokojené občany, kteří se prostřednictvím internetových útoků snaží dát například najevo svůj nesouhlas s aktuálním děním ve svém státě. Politická motivace bývá v tomto ohledu nejčastější, ale obecně se hacktivisté snaží podporovat jakýkoliv názor, který oni sami považují za ten spravedlivý. Možná jste již slyšeli o skupině Anonymous, která se velmi proslavila prosazováním svobodného a otevřeného přístupu k informacím na internetu.

Úroveň hacktivistických skupin se často liší. Setkáváme se zde jak s hackery, kteří na svou cestu kyberbezpečnosti teprve nastoupili, tak i s ostřílenými profesionály.

Na dalším stupni nalezneme profesionální hackery. Zde najdeme etické „white-hat“ i neetické „black-hat“ hackery. Dá se říci, že jejich hlavní motivace bývá častokrát stejná – finanční profit. Přestože ti etičtí vykonávají svou činnost naprosto legálně, nepracují za pouhé „děkuji“. Na rozdíl od neetických hackerů není jejich cílem někoho vydírat nebo okrást, ale jelikož se jedná o velmi kvalifikované IT pracovníky, odpovídá tomu také jejich mzda.

Často se můžeme setkat ještě s jednou kategorií, státem sponzorovanými hackery. Zní vám to jako sci-fi? Opak je pravdou. Jedná se o profesionály, kteří své aktivity vykonávají pod záštitou státu. To jim dává možnost využívat neomezené podpory, financí a ochrany své země. Často můžeme v médiích slýchat o korejských, ruských nebo amerických hackerech a špionech. Nenechte se mýlit, každá vyspělá země má v dnešní době k dispozici tým trénovaných profesionálů, jejichž cílem je bránit svůj kybernetický prostor, své zájmy a své lidi.

Existuje mnohem detailnější škatulkování různých typů internetových útočníků, ale pro účely této knihy nám postačí rozdělení na začátečníky, hacktivisty, profesionály s dobrými i špatnými úmysly a špiony.

II. Chraňme si své soukromí

Člověk je tvor společenský většina z nás ke svému životu potřebuje ostatní lidi. Myslím, že nezáleží na tom, jestli je člověk extrovert či introvert, čas od času každý z nás zatouží po pozornosti či uznání ostatních. Jedním z velmi silných trendů moderní doby je sdílení – ať už informací či zážitků. Masivní využívání sociálních sítí na denní bázi, zveřejňování miliónů fotografií a příspěvků ukazujících naši aktuální náladu, mazlíčky, zajímavé dovolené. Pro mnoho lidí je velmi uspokojující vidět množství pozitivních reakcí na sdílené fotografie, což je motivuje k tomu sdílet více a více. Občas ale zapomínáme, že naše soukromí je velmi cenné a bez uvážení jej obětujeme právě za ten chvilkový obdiv ostatních. Nejde přitom jenom o fotografie na sociálních sítích, jde celkově o to, jak se na síti chováme, jak ji využíváme a jakou stopu za sebou necháváme. Rád bych vám přiblížil principy metody OSINT, což je zkratka pro „open-source intelligence“, volně přeloženo jako „zpravodajství z otevřených zdrojů“. Rozhodně není

mým cílem do vás natlačit množství různých zkratek, jde mi spíše o pochopení jejich významu.

Jedná se o metodu získávání informací o lidech, společnostech a organizacích či počítačových systémech z různých částí internetu. Myslím, že můžeme říci, že se jedná o úplně první krok, kterým hackování začíná. Když si útočník vybere svůj cíl, začne s jeho opatrným zkoumáním zpovzdálí, aby o něm zjistil nějaké základní informace, které mu pomohou vymyslet další průběh útoku.

Různé zdroje se často rozcházejí v tom, jestli je OSINT analýza legální či nelegální. V podstatně jde o shromažďování veřejně dostupných informací, které jsou volně k dispozici na internetu, a z toho by se dalo vyvodit, že na této praxi není nic nelegálního. Není to však vždy pravda. V některých státech světa může být shromažďování informací o subjektech v rozporu se zákony či regulacemi o ochraně osobních údajů. V některých autoritativnějších režimech je OSINT dokonce klasifikován jako narušení soukromí či sledování a při jeho prokázání se na něj pohlíží podobně, jako kdyby vás někdo sledoval v reálném životě.

Můžete si vyzkoušet ve svém prohlížeči ve svém oblíbeném vyhledávači zadat své jméno a příjmení,

případně zadejte ještě město, ve kterém bydlíte. Možná budete překvapeni, kolik informací o sobě najdete jen tímto velmi rychlým průzkumem. Je pravdou, že pokud se budete hledat v prohlížeči a vyhledávači, který běžně používáte pro svou každodenní činnost, je velmi pravděpodobné, že výsledky tím budou ovlivněny. Moderní prohlížeče uchovávají naši historii, aby nám pomáhali vyhledávat co nejrelevantnější obsah. Pokud byste si chtěli vyzkoušet, jaké informace jsou o vás dostupné pro ostatní lidi, doporučuji využít jiný prohlížeč, vyhledávač nebo alespoň anonymní režim, který většina moderních prohlížečů nabízí.

Neuvážené sdílení

Pojďme se nyní vrátit k úvodní myšlence této kapitoly. Zkusíme se zamyslet nad tím, proč může být sdílení většího množství informací na sociálních sítích hrozbou pro naše soukromí.

Představte si nyní, že jedete na svou vysněnou, dlouho očekávanou dovolenou. Vyrazili jste s rodinou či přáteli. Na týden, abyste si odpočinuli od práce a poznali nová zajímavá místa. Rádi sdílíte fotky na Facebooku či

Instagramu, a tak si tam hodíte příspěvek. Aby byl ještě krásnější, přihodíte k němu hudbu, pár popisků a samozřejmě označení aktuální polohy, aby se příspěvek odkazoval na místo, kde se právě nacházíte. Ideálně, když všem dáte vědět, jaké bude následující místo vaší návštěvy, aby se mohli těšit na další zajímavé příspěvky. Už asi tušíte, kam s těmihle myšlenkami směřuji, že ano?

Přestože je prvotní myšlenka naprosto čistá a nevinná, může se jednat o zásah do soukromí vás či vašich blízkých, se kterými dovolenou prožíváte. Nejen, že každý, kdo si příspěvek prohlédne, bude vědět o vaší aktuální poloze, ale může zjistit i to, kde se budete nacházet v příštích dnech. Chápu, že spoustě lidí bude tato skutečnost lhostejná, ale někdo jiný to na druhou stranu může vnímat jako zásah do svého soukromí. Je pravdou, že většinou jsou podobné příspěvky dostupné pouze pro náš okruh známých a přidaných přátel na sociálních sítích. Zkuste se však pozorně podívat do seznamu svých přátel či sledujících, jestli se tam nacházejí opravdu jen lidé, které reálně znáte.

Nedávno jsem zaslechl o dalším případu neuváženého sdílení, co může mít mnohem větší dopad než jen to, že někdo zjistí informace o vás. Je to dopad, který může mít sdílení informaci o nás a našich blízkých

na naše děti. Když se hrdý rodič rozhodne, že chce získávat uznání na sociálních sítích skrze své ratolesti, a začne sdílet jejich roztomilé fotografie, neuvědomuje si, na jaké problémy mu může zadělávat do budoucna. V tu chvíli se z jeho dítěte stává veřejně známá osobnost. Pokud vás navíc někdo na sociálních sítích sleduje delší dobu, může skrze vaše příspěvky odhalit, v jakých lokacích se nacházíte nebo jaké kroužky vaše dítě navštěvuje. Představme si nyní, že za dítětem někdo přistoupí a už jen přímým oslovením jeho jménem v něm okamžitě vzbuzuje důvěru. Učíme své děti se rozhlížet, když přechází silnici, učíme je dávat si pozor na cizí lidi, učíme je se učit. Neuváženým zveřejňováním detailů jejich dětství jim ale nechtěně můžeme zkomplikovat dospívání i dospělý život. Pomáhejme jim mimo jiné tím, že budeme chránit jejich současné i budoucí soukromí na internetu.

Jeden účet vládne všem

Většina z nás má svůj soukromý e-mail. Využíváme ho pro vytváření účtů na sociálních sítích, v internetových obchodech, na různých webových portálech a občas třeba i pro komunikaci. Pokud naše

zaměstnání obnáší práci s počítačem, je naprosto běžné, že máme ještě pracovní e-mail. Je to jedno z prvních opatření, které používáme pro oddělení soukromého a pracovního života. Málokdy nám však dochází, jak je pro nás onen soukromý e-mail důležitý. Kromě již zmíněného na něj máme navázáno například internetové bankovnictví a další důležité služby.

Je docela běžnou praxí, že stejný účet využíváme při registracích i do méně důležitých aplikací, jako jsou blogy, zpravodajství či například počítačové a mobilní hry. V úvodu knihy jsme si vysvětlili, že ani v dnešní době systémy nejsou dokonalé a občas vlivem bezpečnostních chyb může dojít k úniku informací. Součástí těchto informací může být třeba i seznam registrovaných uživatelů včetně jejich e-mailových adres. Občas k těmto únikům dochází i z vlastní vůle vlastníka blogu, zpravodajského portálu či online hry. Může mít například domluvenou spolupráci s dalšími organizacemi o poskytnutí či prodeji seznamu registrovaných uživatelů, což může vést například k tomu, že vám začnou chodit e-maily ze stránek, které jste nikdy neviděli. O tom, proč mohou být nevyžádané e-maily bezpečnostní hrozbou se budu blíže věnovat

v kapitole vysvětlující metody a nástrahy sociálního inženýrství.

Jednoduchým a efektivním bezpečnostním opatřením může být například využívání různých účtů pro různé účely. Pokud se naučíme se systémy efektivně pracovat, nemusí se jednat o tak významný zásah do našeho uživatelského komfortu, přičemž naše internetová bezpečnost se výrazně zlepší.

Jméno mazlíčka není dobré heslo

Prakticky neustále se setkávám s tím, že lidé používají jednoduchá a snadno zapamatovatelná hesla. Podle studie nazvané „Na konec jsem přidal ‚!', aby to bylo bezpečné" [1] od výzkumníků z Carnegie-Mellonovy univerzity v Pensylvánii uživatelé využívají při vytváření svých hesel nejčastěji jména a data narození členů své rodiny, mazlíčků či přátel. V těsném závěsu jsou úryvky textů či fráze z oblíbených písní. Velmi často se používají také klávesové vzory typu „qwertzuiop" či „abcde123". Často se stává, že pro „posílení" hesla uživatelé vloží nakonec či na začátek nějaký speciální znak jako například vykřičník, otazník či hvězdičku.

Dále v práci nazvané „Hesla a chování uživatelů“ [2] autoři zjistili, že až 52 % všech dotazovaných respondentů běžně používá stejné heslo ke všem svým účtům.

Tolik ke statistice a číslům, co nám z toho plyne? Bude-li někdo znát naši e-mailovou adresu a uhádne či jinak zjistí naše jednoduchá hesla, v nejhorším scénáři může získat přístup ke všem našim navázaným účtům. Na druhou stranu, důležité systémy, které opravdu uchovávají naše citlivá data, jsou většinou chráněny ještě druhým faktorem. Mám na mysli jednorázové ověřovací kódy skrze SMS zprávy či mobilní aplikace. Pokud se ale vrátíme opět k sociálním sítím, ty tento typ dvoufázového ověřování standardně nevyžadují. Může se tedy stát, že někdo převezme kontrolu nad naším účtem a bude se za nás moci vydávat. Aby nám znemožnil přístup k účtu, může i změnit heslo, e-mailovou adresu, klidně si i nastavit dvoufázové ověření svým telefonem. V takovém případě bychom mohli ztratit přístup ke svému účtu navždy, jelikož získání opětovného přístupu skrze oficiální podporu poskytovatele bývá velmi dlouhý a bolestivý proces, navíc s nejasným výsledkem.

Jak se efektivně bránit? Mimo standardní poučky o využívání dlouhých, silných uživatelských hesel bych

chtěl zdůraznit významnost právě více faktorového ověřování, a to všude, kde je to možné. Jedná se o opatření, které může ubírat na uživatelském komfortu, zato ale významně přispět k zajištění naší bezpečnosti na internetu. Velmi dobrou a v dnešním světě stále se rozšiřující praxí je využívání aplikací pro ukládání hesel – tzv. password managerů. Jedná se o aplikaci, do které se přihlašujete například pomocí otisku prstu či skenu obličeje a která je schopna generovat a uchovávat komplexní hesla i usnadnit vám jejich používání jednoduchým způsobem.

Dvakrát měř, jednou řež

Tvrzení, že co se jednou umístí na internetu, to na něm také zůstane navždy, je trochu zjednodušené. Mnoho aplikací a systémů se musí řídit různými právními předpisy, které vznikají mimo jiné také proto, aby pomáhaly chránit soukromí uživatelů. Je docela běžné, že aplikace mimo legislativní požadavky uchovávají trvale jen minimum informací, čímž se stávají pro uživatele atraktivnější.

Mějme ale na paměti fakt, že cokoliv, co zveřejníme na síti, si mohou ostatní, kteří mají k obsahu přístup, stáhnout, uložit a nakládat s tím dle svého uvážení. Existují také organizace, které se specializují na archivaci obsahu na internetu s cílem zálohovat a uchovat obsah, který by neměl být ztracen. Samozřejmě, že i tyto rozsáhlé archivy mají svá omezení, ale je klidně možné, že uchovávají informace i o nás, kdo ví.

Tou nejlepší a nejefektivnější ochranou našeho soukromí je kritické uvažování. Sdílejme pouze informace a obsah, u nějž nám nevadí, že bude dostupný v delším časovém horizontu. Pokud si třeba za den či týden uvědomíme, že již nechceme, aby zveřejněné informace o nás byly dostupné, může být pozdě.

III. Nekonečný příběh jménem sociální inženýrství

Již víme, kdo je to hacker a co je to hacking. Nyní se blíže podíváme na několik útoků, které se v reálném světě opravdu dějí. Když se řekne „hacker“, mnoho z nás si hned představí chlápka v černé mikině s kapucí v tmavé místnosti, který shrbený velmi rychle píše na klávesnici a za chvíli se na jedné z jeho obrazovek objeví zelený nápis „přístup povolen“. Okamžitě získá bez povšimnutí přístup i do těch nejstřeženějších částí sítě a má k dispozici ty nejtajnější vládní dokumenty. Přestože v realitě by podobný přímý útok na chráněné systémy vyžadoval čas a nemalou dávku zkušeností a kreativity, opravdu existuje i relativně jednoduchý způsob, jak infiltrovat cizí systémy, a to relativně rychle.

Možná jste již zaslechli o fenoménu známém jako sociální inženýrství. Jedná se o soubor metod, technik a postupů, které necílí na počítačové systémy jako takové, ale naopak na jejich uživatele. Sociální inženýrství využívá principů manipulace s lidskou psychickou s cílem zastrašit, vyvolat pocity nejistoty, štěstí či soucitu. Jeho cílem je obelstít uživatele a přimět

ho, aby klikl na podvodný odkaz a navštívil nebezpečnou webovou stránku, přímo či nepřímo útočníkovi vyzradil své přihlašovací údaje a umožnil mu tak přístup do systémů pod falešnou identitou. Další motivací útočníků může být stažení nějakého škodlivého programu do zařízení oběti s cílem jej ovládnout.

Musím říci, že se v praxi čím dál víc setkávám se společnostmi a organizacemi, které si uvědomují hrozby v kyberprostoru. Z toho důvodu vynakládají nemalé finanční prostředky na zabezpečení vlastní sítě, počítačů či serverů. Tohle úsilí velmi oceňuji, ale je třeba mít na paměti, že bezpečnost si jen tak nekoupíte. Platí, že počítačové systémy využíváme zejména pro zefektivnění našich každodenních činností, zpracovávání dokumentů, elektronickou komunikaci a tak dále. Počítačové systémy jsou vytvářeny hlavně pro používání lidmi. A zde se dostáváme k jádru věci, můžete mít sebelepší bezpečností opatření – drahý firewall, behaviorální síťové sondy, antivirová řešení nové generace, ale dokud si sami uživatelé neuvědomí svou roli v informačním řetězci a svou povinnost podílet se na zajišťování bezpečnosti, může celá dosavadní snaha přijít vniveč. Člověk je v tomto ohledu nejslabším a nejsnáze ovlivnitelným článkem.

Vychází to z naší přirozenosti – zvídavosti, lehkomyslnosti či neznalosti. Dále se vám pokusím popsat právě konkrétní metody, způsoby jejich provedení, možné důsledky, ale také efektivní způsoby, jak se jim bránit.

Phishing – podvodné e-mailové zprávy

Tak jako je rybář nejstarší známé řemeslo, je i phishing (anglicky „rybaření“) nejstarší a stále nejpoužívanější metodou sociálního inženýrství. Troufám si říci, že se každý s nás už někdy s tímto typem kybernetického útoku setkal. Jedná se stále o tu pro útočníky nejjednodušší a nejefektivnější metodu. Spočívá v odesílání e-mailových zpráv, které se snaží být věrohodnou napodobeninou legitimních zpráv, newsletterů, upozornění, reklamních sdělení. To, že člověk mohl podvrh na první pohled rozeznat díky gramatickým chybám či nevyladěné grafice, již dávno neplatí. Zvlášť v dnešní době pokročilých překladačů a systémů umělé inteligence, které i útočníkům

pomáhají vytvářet lákavé a věrohodné e-mailové šablony. Možná si teď říkáte, proč výrobci nezakážou použití inteligentních systémů pro vytváření podvodných e-mailů? Jedná se princip, na který budeme narážet v celé knize. Hackeři totiž využívají naprosto stejné nástroje jako uživatelé a administrátoři, jen k účelům, ke kterým nebyly primárně vyvinuty. V tomto konkrétním případě e-mail, překladače, obrázky, texty a vlastní kreativitu.

Lákavou a dobře vypadající e-mailovou zprávou to však nekončí. Z toho, že by si uživatel pouze prohlédl přijatý e-mail, by hacker žádný užitek neměl. Jeho cílem je do těla zprávy přidat nějaký „call to action“, něco, co po uživateli chce, aby provedl. Většinou je ve zprávě k nalezení odkaz či tlačítko, které po kliknutí přesměruje uživatele na novou webovou stránku. Tyto stránky bývají pod plnou kontrolou útočníka, což znamená, že si na ně může umístit cokoliv chce. Od přihlašovacích formulářů, které budou věrnou kopií známých internetových služeb, přes portály, kde jsou zajímavě vypadající soubory volně ke stažení, až po podvodné webové galerie, blogy a mnoho dalšího. Obsah těchto webových stránek a e-mailových zpráv, skrze které se uživatel na stránky dostal, závisí na tom, co od uživatele chce hacker získat.

Nejčastěji je útočníkovým záměrem získat uživatelovy přihlašovací údaje, aby mohl následně ukrást jeho identitu a vydávat se za něj na internetu. Často se setkávám s tím, že mi lidé na školeních a seminářích tvrdí, že když vidí ve svém prohlížeči onen „zelený zámeček“ vedle adresního řádku, který tvrdí „připojení s tímto webem je bezpečné“, jedná se o validní web a žádné riziko zde nehrozí. Opak je však pravdou. Tento „zelený zámeček“ říká pouze to, že komunikace mezi vaším počítačem a serverem, kde se webová stránka nachází, je zabezpečená, je šifrovaná. Zjednodušeně to znamená, že nikdo kromě vás a webové stránky by neměl mít možnost narušit vaši vzájemnou komunikaci s cílem vidět, co na konkrétním webu děláte. V žádném případě to ale neznamená, že samotný web je bezpečný. Je nutné si uvědomit, že webová stránka či webová aplikace je plně pod kontrolou útočníka. Tato stránka či aplikace je napsána v nějakém programovacím jazyce. My jako uživatelé vidíme pouze to, jak se prezentuje navenek, ale nemáme žádné informace o tom, jak se chová na pozadí. Blíže se tomuto tématu budu věnovat v následujících kapitolách, ale chtěl jsem tímto rychlým úvodem do bezpečnosti webových stránek poukázat na potenciální bezpečností rizika, která se k nim vážou.

Krása phishingových útoků spočívá v jejich jednoduchosti. Útočník zašle oběti e-mail s lákavým obsahem, který ji přiměje rozkliknout cílovou webovou stránku s výzvou k přihlášení. Tímto elegantním způsobem může hacker během pár minut získat přihlašovací údaje uživatele a podniknout další fáze svého zamýšleného útoku.

Jak se proti phishingu efektivně bránit? Základní ochranou, kterou společnosti a organizace implementují, jsou různá technologická opatření, která hlídají a kontrolují příchozí i odchozí poštu uživatelů. Také monitorují a blokují spojení se známými podvodnými weby. Nicméně ale ani to v praxi nestačí, jelikož založení nových e-mailových adres či vytvoření nových podvodných stránek je pro útočníky relativně jednoduché. Nejlepší obranou tedy zůstává naše kritické myšlení a schopnost podvrhy rozpoznat. Proto je velmi důležité pravidelně o aktuálních hrozbách mluvit, školit se a nespoléhat pouze na nasazená bezpečnostní opatření. Vždy se nejprve podívejte, zda e-mail přišel z vám známé adresy. Důležité je se také zamyslet, co po mně zpráva požaduje? Proč nyní? Proč ten náhlý spěch? Pokud usoudíte, že je cílem zprávy ve vás vyvolat strach, že se stane něco nepěkného, pokud nekliknete, bude se

téměř jistě jednat o phishing. Pokud je cílem zprávy ve vás vyvolat nadšení, že jste vyhráli milion korun a pro vyzvednutí výhry stačí kliknout a přihlásit se, bude se téměř jistě jednat o phishing. Kontrolujte pečlivě adresu odesílatele a text v adresním řádku prohlížečů. Většina útoků bývá úspěšná pouze kvůli nepozornosti uživatelů, kteří přehlédnou překlep v názvu webové stránky. Člověk je z pohledu bezpečnosti tím nejslabším článkem, ale člověk s dobrým kritickým myšlením je zároveň tím nejlepším bezpečnostním opatřením.

Rád bych se podělil o jeden příklad z praxe. Vytvářeli jsme kampaně s phishingovými e-maily pro klienta. Cílem bylo zjistit, jak jsou na tom lidé v organizaci se znalostmi v oblasti kybernetické bezpečnosti a jestli je vhodné organizovat školení s touto tématikou. Naším cílem bylo vytvoření několika e-mailových šablon a několika podvodných webových stránek. Samozřejmě, že jsme si dali práci s tím, aby šablony byly co nejlákavější. Strávili jsme přípravou spoustu hodin, aby výsledné e-maily byly velmi propracované. K našemu údivu jsme po vyhodnocení proběhlých kampaní zjistili, že „nejúspěšnější“, tzn. takové, na které se „nachytalo“ nejvíce lidí, byly zároveň ty nejjednodušší. Šablony s tématikou „Vyhráli jste košík

plný velikonočních vajíček“ či „Platy vedoucích zaměstnanců“ měli takovou úspěšnost, že jsme je použili ještě mnohokrát poté. Dospěl jsem tedy k osobnímu názoru, že ty nejúspěšnější útoky na bázi sociálního inženýrství cílené na lidskou psychiku nevedou přes vyvolávání strachu či nejistoty, ale naopak cílí na naši soutěživost a zvídavost.

Smishing – podvodné SMS zprávy

Pokud jste v předchozí kapitole pochopili provádění útoků s využitím podvodných e-mailových zpráv, bude pro vás porozumění technice smishing velmi snadné. V podstatě se jedná o stejný princip, jen nosným médiem se místo e-mailu stávají SMS zprávy. Také cíl zůstává stejný, přimět uživatele otevřít podvodnou webovou stránku. Velký rozdíl ale nastává v možnostech, které mají útočníci k dispozici. Zatímco při sestavování atraktivního e-mailu se dají využít barvy, obrázky i formátování textu, při odeslání SMS zprávy můžete použít jen omezené množství znaků. Dalším kamenem úrazu je fakt, že podvodná SMSka musí kromě

samotného textu zprávy obsahovat i podvodný odkaz. Jak se tedy útočníci s těmito překážkami vypořádávají?

Aby podvodné SMS zprávy působily věrohodně, nejčastěji napodobují zprávy, se kterými se uživatelé běžně setkávají. Nejběžnějšími napodobeninami bývají upozornění na vyzvednutí zásilky a výzvy k převzetí výhry v soutěži. „Vyhráli jste poukaz pro dvě osoby do našeho wellness centra, klikněte na odkaz a převezměte si výhru!“ – i takto může vypadat podvodná SMSka. Nebo například – „Váš balík budeme doručovat dnes mezi 9-11h. Svou zásilku můžete sledovat na tomto odkaze.“ První krok je tedy zřejmý – stručnou a lákavou zprávou se útočníci snaží přimět oběť kliknout na odkaz a otevřít podvodnou webovou stránku.

Pokud běžně pracujete s počítačem, tak asi víte, že URL adresa webové stránky může být velmi dlouhá a pro posílání v SMS zprávě velmi nepraktická. Existují však služby, kterým neformálně říkáme „URL zkracovače“. Jedná se o legitimní služby, které nahrazují dlouhé URL adresy mnohem kratšími. Po kliknutí na konkrétní zástupný odkaz je uživatel přesměrován na původní adresu. Jedná se o běžně používanou službu, která často bývá naprosto volně dostupná. Tenhle fakt nám docela komplikuje možnost rozpoznat podvodnou

stránku, protože na první pohled nebude možné zjistit, kam přesměrování vede. Moderní bezpečnostní řešení, prohlížeče a další běžné prvky operačních systémů počítačů i telefonů se snaží podobné hrozby odhalovat, ale i jejich možnosti jsou v tomto ohledu dosti limitované.

I zde platí, že tou nejlepší obranou je naše kritické myšlení. Očekávám podobnou SMS zprávu? Čekám nějaký balíček? Vyžaduje po mně odesílatel nějakou okamžitou akci? Je součástí SMS zprávy nějaký odkaz, který působí podezřele? Znám odesílatele? Toto jsou základní otázky, které byste si měli položit před rozhodnutím, zda na odkaz ve SMSce kliknete. I pouhé kliknutí bez nutnosti zadávat informace na webu může vést k incidentu s vážnými následky.

Vishing – podvodné volání

Je to forma útoku na bázi sociálního inženýrství, která na rozdíl od hromadných e-mailů či hromadných SMS zpráv bývá téměř vždy cílena na konkrétního jednotlivce. Vishing je metoda využívající telefonních hovorů, útočníkovy výřečnosti a umění přesvědčovat.

Představte si případ, kdy vám zavolá neznámé číslo, představí se jako někdo, komu důvěřujete – například váš bankéř – a snaží se vás přimět k nějaké akci.

Osobně tento druh útoku považuji za jeden z nejhorších, protože téměř vždy je jeho cílem získat peníze od důvěřivých a této problematiky neznalých lidí. Je smutné, že se setkává v praxi s velkou úspěšností, zejména u starších ročníků, co pak mnohdy přijdou o celoživotní úspory. Pokud si teď říkáte, že jde o velmi nelidský přístup, souhlasím s vámi. Proč vám to ale popisuji? Myslím, že je důležité dívat se na svět racionálně, bez růžových brýlí. Existují mezi námi lidé, kterým jde pouze o jejich vlastní profit a neváhají cíleně škodit ostatním, aby dosáhli svého. Tahle myšlenka mě již od počátku motivovala a motivuje k napsání této knihy, jejímž cílem je právě šířit povědomí o nástrahách internetu, způsobech, jak se mít na pozoru a jak se jim efektivně bránit.

Zpátky k vishingu a k tomu, jak může vypadat. Dovolím si navázat na příklad s bankéřem. V poslední době se jednalo o ten nejčastější scénář, kdy útočník zavolal oběti a představil se právě jako její osobní bankéř. Informoval ji, že někdo napadl její účet, a že jí pomůže tuto situaci vyřešit. Útočník nezapomene zdůraznit, že

není třeba kontaktovat policii, protože ta je již s celou situací seznámena a vyšetřování probíhá. Nyní je třeba, aby s řešením pomohl i sám uživatel. Následovat může několik variant. Falešný bankéř například informuje oběť, že v rámci řešení incidentu jí založil nový zabezpečený účet, na který je třeba převést všechny peníze, aby byly v bezpečí. Stává se také, že se útočník snaží oběť přimět vybrat hotovost a skrze vkladové bankomaty ji vložit jinam. Anebo oběť krok po kroku navede, jak peníze vložit skrze nákupní bankomaty do kryptoměn a odeslat je na „zabezpečený účet“. Může vám to znít neuvěřitelně, ale všechny tyto scénáře se běžně stávaly a stávají. Hodně lidí při podobných útocích přišlo o nemalé peníze.

Úspěšnost vishingových útoků plně závisí na ochotě oběti spolupracovat. Toho se útočníci snaží docílit výmluvnými historkami, empatií a využitím konkrétních osobních informací. Mohou pro zvýšení své důvěryhodnosti zmínit jméno členů vaší rodiny, místo, které jste nedávno navštívili, či jméno vaše mazlíčka. Informace, které mohli lehce zjistit například z vašich sociálních sítí.

Baiting – nebezpečné „flashky“

Troufám si říci, že většina z nás používá USB flash disky pro přenos či ukládání dat. Není na tom nic špatného, dělám to také. Ve většině případů se rizika spojená s „flashkami“ pojí ke ztrátě dat, která na nich máme uložená, například při ztrátě či fyzickém poškození zařízení. Z pohledu hackera mají USB „flashky“ však ještě další zajímavá využití s velkým potenciálem. Pokusím se vám vysvětlit princip baiting útoku, který se snaží infiltrovat počítač právě skrze nevinně vypadající „flashky“.

Když si představíte obyčejnou „flashku“, bude se skládat minimálně ze dvou částí – USB konektoru, kterým ji připojíte ke svému počítači, a těla, které často bývá zabaleno do nějakého elegantního plastového krytu. Velmi jednoduchý design. Co se však skrývá uvnitř flashky, je nám jako uživatelům ukryto. Když takovou „flashku“ chceme použít a zasuneme ji do svého počítače, většinou se nám po krátké chvíli otevře složka a ukáže nám uložené soubory. Krátce odbočím k ostatnímu příslušenství, které s našimi počítači běžně používáme. Mám na mysli myši, ať už drátové či bezdrátové, klávesnice, webové kamery a další. Běžně tato zařízení

používáme stejným způsobem jako USB „flashky“. Zasuneme do počítače a jednoduše je používáme.

Když to velmi zjednoduším, toto velmi elegantní a uživatelsky přívětivé použití funguje díky tomu, že zařízení počítači předá informaci ve stylu: „ahoj, jsem klávesnice a teď do tebe budu vkládat znaky“; „ahoj, jsem myš a nyní budu hýbat kurzorem a klikat na ikony“; „ahoj, jsem webkamera a můžeš mě použít pro nahrávání videa“. Počítač tuto informaci zpracuje a s připojeným zařízením takto začne pracovat. Nyní se nabízí docela zajímává otázka: co když vytvoříme takové zařízení, které počítači „zalže“ a identifikuje se jako něco jiného? Přesně tohoto principu využívá útok baiting.

Tento útok spočívá ve vytvoření zařízení, které vypadá naprosto stejně jako klasická „flashka“. Nicméně při identifikaci po zastrčení do USB portu počítači předá informaci, že není úložný disk, nýbrž klávesnice. Hacker při přípravě tohoto falešného zařízení naprogramuje sadu instrukcí, které se mají při jeho aktivaci provést. Představte si to tak, že takto připravená falešná „flashka“ začne psát za uživatele, a to velmi rychle. Počítač dokáže psát mnohem rychleji než člověk, a proto takto připravené zařízení může napsat i tisíce znaků během velmi krátké chvíle. Operační systém počítače je velmi

komplexní a dá se ovládat mnoha způsoby. Jedním z nich je grafické rozhraní, tak, jak jej zná většina uživatelů. Tím druhým způsobem je terminálové prostředí, které používají především správci, nicméně je běžně dostupné jakémukoliv uživateli. V tomto prostředí se dá velmi efektivně ovládat a konfigurovat počítač, nicméně se jedná o čistě textové prostředí bez grafické nástavby. Ideální pro někoho, kdo používá pouze klávesnici.

V momentě, kdy se falešná „flashka“ dostane do akce a přistoupí do terminálového prostředí počítače, může ho plně ovládat s právy uživatele, který je k systému aktuálně přihlášen. Možná již tušíte, kam tohle celé směřuje. V případě, že podobně připravené falešné zařízení neuváženě použije například administrátor velké společnosti, může to mít kritický dopad na celou společnost. Útočník je totiž schopen připravit velmi sofistikovaný útok, který „flashka“ provede. Může se jednat o stažení trojských koní, virů či jiných škodlivých programů. Může se jednat o smazání informací na připojených uložištích. Může se jednat o krádež citlivých dat uživatele či společnosti. Možnosti toho, co vše se s použitím baitingu dá provádět, jsou obrovské a věřte tomu, že útočníci bývají velmi kreativní.

Dalším problémem je, že proti tomuto druhu útoku není k dispozici moc efektivních ochran. Jako první se hned nabízí znemožnit uživatelům využívat USB zařízení. To v praxi ovšem není možné, uživatelé přece potřebují používat klávesnice a myši. Existují moderní bezpečnostní řešení, která provádějí velmi efektivní a chytrou ochranu koncových počítačů, ale to není téma vhodné pro tuto knihu. Zmíním tedy jen to, že pokročilé nástroje existují a v mnoha společnostech se používají. Pro domácí uživatele a počítače ale ve většině případů dostupné nejsou. Jedinou obranou, která nám zbývá, je opět náš vlastní úsudek. Pokud najdeme neznámou nevinně vypadající „flashku“, nebudeme ji bezhlavě strkat do našich počítačů. Všechna tato podvodná zařízení budou na první pohled vypadat nevinně, na žádném z nich nebude napsané „podvodná fleška, která ti hackne počítač“. Buďme tedy vždy obezřetní, a nejsme-li si jisti, co je na zařízení nahráno nebo jak jej bezpečně použít, nechejme jej radši na zemi, kde leží.

A je toho mnohem více!

Sociální inženýrství je velmi široký a zajímavý obor hackingu. Pro black-hat hackery se jedná o jednoduchý a efektivní způsob, jak získat identitu uživatele a přístup k jeho souborům. Pro white-hat hackery je to zase „práce hrou“, jelikož zde platí více než jinde, že představivosti a kreativitě se meze nekladou. Zmiňované metody v této kapitole představují jen zlomek běžně používaných technik a postupů, které hackeři na denní bázi používají. Od obyčejného fyzického odposlouchávání hovorů, koukání přes rameno oběti s cílem odhalit uživatelské heslo nebo pin ke kartě, přes vytváření falešných profilů na sociálních sítích s ukradenými fotografiemi celebrit až po reálné vydávání se za někoho jiného. Všechny metody sociálního inženýrství však mají jeden hlavní společný znak. Cílí na uživatele.

IV. Pastičky s názvem „webové stránky“

Velká část předchozí kapitoly věnovaná sociálnímu inženýrství se zaobírala technikami, jak se nás útočníci snaží přimět vykonat nějakou akci. Často jde právě o kliknutí na tlačítko či odkaz, který následně otevře webovou stránku v prohlížeči. Nyní se blíže podíváme na to, čeho tím může hacker dosáhnout, jaké dopady může i jen pouhé otevření podvodného webu mít a jestli se jedná o finální krok útočníkova plánu, anebo jen o další část řetězce, na jehož konci bude mít útočník plný přístup k uživatelově identitě a souborům. Na úvod bych zde chtěl ještě zmínit, že bezpečnost webových aplikací je velmi široké téma a pokrýt všechny její aspekty není cílem této knihy. Nechci se zde pouštět do přílišných technických detailů, naopak se vám budu snažit vysvětlit základní principy tak, aby i běžný uživatel pochopil rizika související s neopatrným přístupem na webové stránky.

Jak „webovky“ fungují

Pojďme si opět představit jednoduchý scénář. Otevřete na svém počítači nebo telefonu webový prohlížeč a do vyhledávače zadáte název či adresu své oblíbené stránky. Následně se vám zobrazí obsah webové stránky a vy máte možnost číst texty, zobrazovat si obrázky, pouštět videa, kliknout na další podstránky, zkrátka klasika. Tohle je uživatelský pohled, co se však děje na pozadí z technického úhlu pohledu?

Jako první je nutné si uvědomit, že webovou stránku někdo musel vytvořit a následně zveřejnit. K vytváření webových stránek se standardně využívají různé programovací jazyky. Ten, kdo webovou stránku či aplikaci vytváří, má možnost na ni umístit prakticky cokoliv chce. Pomineme-li nyní to, že vývojář by měl ctít autorská práva ostatních lidí a nepoužívat bez svolení jejich texty, obrázky či části kódů, je opravdu čistě na onom vývojáři, jaké prvky na stránku umístí. Mimo zobrazování textů a obrázků se velmi často setkáváme s formuláři, což jsou interaktivní prvky, do kterých může uživatel vkládat různá data. Za formulářem se vždy nachází nějaká skrytá logika, která definuje, jak jsou zadávaná data zpracovávána. I zde platí, že nad

způsobem, jakým se tato data zpracovávají, má plnou kontrolu provozovatel systému.

Ve 21. století již dávno neplatí, že každou webovou stránku vytváří programátor úplně od znovu. Využívají se různé frameworky, což je sada předpřipravených šablon a kódů, které vývojáři smí volně použít, a které jim usnadňují vytváření grafických i logických prvků aplikace. Jedná se o naprosto běžnou praxi, že jedna aplikace používá velké množství podpůrných modulů, které vytvořil někdo úplně jiný. Tato „optimalizace“ přispívá k rychlejšímu a efektivnějšímu vývoji aplikací, stejně jako ke „standardizaci“ ovládacích prvků. Když se budete pozorně koukat, zjistíte, že řada webových stránek využívá stejné nebo velmi podobné vizuální styly a funkce.

Jako uživatelé vidíme pouze finální podobu webové stránky, ale co je vše nutné pro její fungování, to nám zůstává skryto. Aby byla webová stránka pro nás kdykoliv dostupná, musí být umístěna a provozována na nějakém počítači, který běží neustále. Takovému počítači říkáme server. Většinou je nutné pro správnou funkčnost webových stránek správně nakonfigurovat vícero služeb, vícero serverů. Databázi pro ukládání a zpracovávání

dat, počítačovou síť, aby vše bylo správně propojeno a měli jste možnost se k cílovému serveru vůbec připojit, a mnoho dalšího. Proč o tom píšu? Chci, abyste pochopili, že internetový svět je mnohem složitější, než se na první pohled může zdát. Je to obrovské soukolí vzájemně propojených služeb. Za jednoduchostí používání našich každodenních aplikací stojí obrovská komplexita internetu, která s sebou přináší také mnoho bezpečnostních rizik.

Webové stránky z pohledu útočníka

Webovou stránku si může vytvořit doslova kdokoliv. Také je pravdou, že na ni může přidat téměř cokoliv chce. To samé platí pro útočníky. Cílem je přimět uživatele nejen otevřít jejich web, ale ideálně na něm také něco provést, například se přihlásit či stáhnout nějaký soubor. Hackeři běžně vytvářejí webové stránky tak, aby byly důvěryhodnou kopií známých internetových portálů. Vytvořit stránku, která bude vypadat naprosto identicky jako přihlašovací formulář nejznámějších sociálních sítí či internetových obchodů, není vůbec

těžké. Dokonce se dají najít a používat šablony, které jsou na internetu volně k dispozici.

Jedním z cílů útočníka může být právě získat uživatelovo heslo. Běžné webové stránky hesla v čitelné podobě neukládají. To znamená, že i kdyby administrátor sociální sítě chtěl, jednoduše se k vašemu heslu nedostane. Toto však neplatí pro stránky, které si vytváří útočník. Můžete na nich najít graficky identické formuláře pro přihlášení, ale v momentě, kdy se o přihlášení pokusíte, útočník odchytne vaše přihlašovací jméno i heslo a může s ním dále nakládat, jak chce.

Dalším velmi častým použitím podvodných stránek je snaha útočníků stáhnout do zařízení oběti nějaký škodlivý program. Můžeme se setkat s různými portály, kde je nabízen běžně zpoplatněný obsah, jako jsou programy, knihy, galerie, hudba či filmy a seriály, zdarma ke stažení. Vždy bychom měli být velmi obezřetní ohledně toho, co a odkud stahujeme. Rozhodně netvrdím, že pouze placený obsah na internetu je důvěryhodný, ale pokud zdroji plně nedůvěřujeme, měli bychom stránku raději opustit.

Zatímco pro počítač je přirozenější pracovat s čísly, pro lidi je obecně jednodušší pracovat s písmeny

a slovy. Na tomto principu je založená služba DNS, která mimo jiné slouží pro překlad číselných adres serverů na doménová jména. Do této chvíle jsem se záměrně vyhýbal poukazováním na konkrétní reálné aplikace či společnosti, ale pro pochopení toho, co je to doménové jméno, zde udělám výjimku. Jistě znáte webové stránky a vyhledávač společnosti Google LLC, který je dostupný na adrese www.google.com. V tomto případě je doménové jméno právě „google.com“. Doménové jméno si může registrovat kdokoliv, a to takové, které zatím nevlastní někdo jiný. S tímhle faktem se vrátím zpět k tématu nebezpečných webových stránek. Aby útočníkův web vypadal věrohodně, nestačí, aby pouze obsah stránky byl atraktivní kopií nějaké známé služby. Pro zvýšení šancí na „úspěch“ si útočníci často zaregistrují doménové jméno, které si může nepozorný uživatel lehce splést s jinou, jemu známou doménou. Například www.google.com a www.gooqle.com vypadají docela podobně, že ano? Je běžnou praxí, že si útočníci registrují domény se schválně zavedenými „překlepy“, aby k sobě nepozorného uživatele nalákali. Tato technika není nikterak nová, mnoho internetových společností se podobné podvody snaží neustále nacházet, nahlašovat a ve spolupráci s dalšími entitami i blokovat. Nicméně

každý den vzniká velké množství podvodných stránek, které jsou založeny na tomto principu. Jedná se o takový věčný souboj dobra a zla, a opět platí, že tou nejefektivnější obranou je naše obezřetnost.

I pouhé „ukliknutí“ může vést k vážným následkům

Pro pokračování si představíme následující scénář. Uživatel se dostal na webovou stránku, ať už skrze phishingový e-mail, podvodnou SMSku či z vlastní iniciativy při procházení internetem. Je ale obezřetný a po načtení stránky vyhodnotí, že se může jednat o podvod, a proto stránku raději rychle opustí.

Bohužel, i tohle stačí, aby váš počítač byl napaden. Dosud jsem vám popisoval scénáře, kdy byla od uživatele vždy vyžadována nějaká akce na podvodné stránce – zadání přihlašovacích údajů, stažení nějakého souboru. Nicméně stačí, aby uživatel podvodnou stránku jenom otevřel, a tím dal útočníkovi šanci infikovat jeho zařízení.

V předchozích částech této kapitoly jsme si zjednodušeně vysvětlili princip fungování webových stránek a víme, že aplikace i data jsou pod plnou kontrolou správce. Také víme, že programátor, který aplikaci vytváří, může libovolně upravovat její chování. Webová stránka je vytvořena v nějakém programovacím jazyce či více jazycích. V momentě, kdy na nějakou webovou stránku přistoupíme, spouští se její kód. Ten se může spouštět buď na webovém serveru nebo přímo v prohlížeči, ve kterém se stránka zobrazuje. Zaměříme se nyní na tu část, která se spouští v prohlížeči uživatele. Jedná se například o jazyk JavaScript. Pokud jste tento název nikdy neslyšeli, vůbec to nevadí, pro pochopení principu útoku to není podstatné. Důležité je pochopit, že při přistoupení na nějakou webovou stránku se na našem počítači v našem prohlížeči spouští kód, který napsal někdo jiný. Chytrá bezpečnostní řešení dokáží nebezpečný kód na stránce objevit a přístup k ní zamezit, ale pro pokračování v tomto příkladu uvažujme, že žádná bezpečnostní opatření k dispozici aktuálně nemáme.

Běžně při procházení internetem nezkoumáme, jaké všechny komponenty webové stránky využívají. A pokud to za nás nedělá ani žádné automatizované bezpečnostní opatření, tak všem stránkám slepě

důvěřujeme. JavaScript je mocná zbraň, s jejíž pomocí útočníci mohou získat přístup k vašemu prohlížeči a ovládnout jej. V případě úspěšného zneužití útočníci mohou zobrazovat vyskakovací okna, podstrkávat oběti soubory ke stažení, využívat webovou kameru či získávat snímky obrazovky. Tohle samo o sobě zní dost strašidelně, ale může být ještě hůře. Pokud stejný prohlížeč využíváte zároveň k přístupu k jiným službám, je možné určitými technikami ukrást vaše přihlášení a následně se za vás v těchto službách vydávat. Velmi nebezpečné toto může být například ve chvíli, kdy jste zároveň přihlášeni do internetového bankovnictví či jiných citlivých služeb.

Jedinou stoprocentní ochranou zde je zakázání využívání JavaScriptu v prohlížečích. Nicméně v praxi je toto nerealizovatelné. Většina moderních webových stránek tuto technologii v nějaké podobě používá, a proto by její zakázání vedlo pouze k tomu, že bychom měli k dispozici spoustu nefunkčních webů. Proto je nutné využívat různá dodatečná bezpečnostní opatření, která nás před nebezpečnými stránkami chrání. Žádná technologie není všespásná a hackeři jsou velmi kreativní. Musíme se proto mít i my stále na pozoru, do jakých částí internetu přistupujeme. Kromě kritického

myšlení je třeba zapojit i naše bystré oko, které rychle odhalí imitace originálních stránek, například i z překlepu v adresním řádku.

Zelený zámeček aneb „spojení s touto webovou stránkou je bezpečné“

V kapitole věnované sociálnímu inženýrství jsem již naťuknul téma týkající se onoho zeleného zámečku, který tvrdí, že „připojení s tímto webem je zabezpečené“. Používám označení „zelený zámeček“, protože dříve takhle použitá ikona vypadala, ale v dnešní době se může lišit. V moderních prohlížečích může vzhled i barva této ikony samozřejmě vypadat jinak, většinou ale platí, že ji najdeme nalevo od adresního řádku prohlížeče.

Se zeleným zámečkem se setkáte u většiny webových stránek, které běžně procházíte. Poznáte to také podle toho, že se v adresním řádku na začátku nachází *https* místo *http*. Tyto zkratky identifikují, že se jedná o webovou službu, a ono „s“ na konci znamená „secure“, což překládáme jako „zabezpečený“. Co tento zámeček ale znamená? Co když na stránce není? Je

připojení opravdu bezpečné? Může ho někdo nějak zneužít?

Celé toto téma souvisí s termínem kryptografie. Ze zkušenosti vím, že je pro mnoho lidí strašidelné, a proto vás hned na úvod uklidím, že zde nemám v plánu zabředávat do detailů kryptografie. Jeden její princip vám ale pro pokračování vysvětlit musím. Je to princip důvěrnosti. Představte si, že chcete někomu zaslat dopis, jehož obsah je pro vás důležitý. Jediný, kdo ho může znát, je jeho adresát. Přestože „důvěřujete“ poštovním službám a všem jejich kurýrům, chcete si být jistí, že se obsah dopisu nedostane do nepovolaných rukou. To, že dopis nikdo z doručovatelů neotevře, vám nikdo nikdy plně nezaručí. Nicméně využití kryptografie vám zaručí, že i když dopis někdo otevře a zprávu si přečte, nebude jí rozumět. Zprávu bude moct dešifrovat a přečíst pouze ten, kdo zná dešifrovací klíč. Přesně tenhle princip je využit při komunikaci s webovými službami.

Nyní aplikujeme analogii s dopisem na příklad, kdy si otevřeme webovou stránku. Na pozadí proběhne výměna klíčů, abychom byli schopni komunikaci mezi námi a serverem šifrovat. O to se samozřejmě automaticky stará náš webový prohlížeč. Pokračování je stejné jako v analogii s dopisem. Na webové stránce

například vyplníme nějaký formulář, třeba hned ten přihlašovací, a odešleme. Tomu, co se odesílá na webový server, říkáme požadavek. Tento požadavek obsahuje informace o tom, kam se snažíme přihlásit, co jsme do formuláře zadali a spoustu dalších informací. Požadavek se zašifruje a cílový webový server, na který se odesílá, bude tím „jediným“, kdo jej dokáže přečíst. Pokud jsme zadali správné přihlašovací údaje, server nám vrátí odpověď, která se nám uživatelům zobrazí například v podobě textového oznámení „přihlášení bylo úspěšné“.

Víme tedy, že komunikace mezi naším webovým prohlížečem a serverem probíhá šifrovaně, a i kdyby se tuto komunikaci někdo snažil narušit, nebude schopen ji přečíst. Nyní se možná ptáte, kdo a jak by takovou komunikaci mohl narušit? Počítačová síť je velmi komplexní a skládá se z obrovského množství počítačů a jiných zařízení. Tím vám nejbližším je pravděpodobně váš domácí router. Dále komunikace putuje k vašemu poskytovateli internetu, ten ho přesměrovává dále. Než se náš požadavek k přihlášení dostane na cílový server, projde množstvím různých zařízení. Každé z těchto zařízení může číst, případně i měnit obsah komunikace, která přes něj prochází. Aby zařízení po cestě byla schopna úspěšně dopravit náš požadavek na cílový

server, musí do požadavku vidět, nemusí však pochopit obsah toho, co konkrétně přenáší. A právě tento obsah zabezpečíme šifrováním a ujistíme se, že pouze cílové zařízení, v našem případě webový server, bude schopné obsah zprávy přečíst.

Co se však může stát, když webová stránka šifrovací mechanismy nepoužívá – využívá *http* místo *https*? Nutno říci, že v dnešní době neexistuje reálný důvod pro to, aby nějaká komunikace neprobíhala šifrovaně. Z historických důvodů se šifrování nepoužívalo pouze kvůli optimalizaci výkonu, jelikož kryptografie je matematicky i výkonově náročný proces. Musíme si uvědomit, že po cestě od našeho prohlížeče k cílovému serveru se nachází velké množství různých zařízení. Přestože většina z nich bývá legitimních, může se stát, že vaše komunikace bude protékat útočníkem. Tomuto tématu se budu věnovat v následující kapitole s názvem *Bezpečná WiFi je „jen" ta vaše.*

Většina zařízení, které jsou schopny nějakou nešifrovanou komunikaci zachytit, ji mohou také číst. Může tak jednoduše dojít k úniku čehokoli, co do webové stránky zadáváme – a to včetně našich přihlašovacích údajů. Absence šifrovacích a dešifrovacích principů na webových službách sice sama o sobě nenarušuje jejich

funkčnost, zato však narušuje bezpečnost komunikace a důvěrnost přenášených dat.

Podvodným webem to teprve začíná

Využití kombinace sociálního inženýrství a podvodných webových stránek otevírá útočníkům dveře k mnoha útokům, jejichž úspěšnost závisí především na jejich kreativitě a schopnostech. Podvodné webovky se dají využít k infikování počítače oběti či získání kontroly nad uživatelskými účty. Pro útočníky cílící na jednotlivce může jít o kýžený cíl, nicméně v praxi se hackeři soustředí spíše na firmy a organice, za kterými je skrytá vidina získání financí – ať už kontrolovanou krádeží nebo snahou vymámit z napadené společnosti výkupné za „příslib“ opětovného zprovoznění napadených systémů.

V. Bezpečná WiFi je „jen“ ta vaše

Máte rádi cestování? Sbalit kufr a vyrazit za exotikou? Nebo preferujete tuzemskou dovolenou, například s návštěvou přírodních rezervací či vinných sklepů? Tak či tak, dovolená je příležitostí chvilkově se oprostit od strastí každodenního života a užívat si pohody, poznávat nová místa i lidi. Tato kniha však není cestopis, je věnována nástrahám na internetu, a tak se zkusíme podívat na rizika cestování z trochu jiného úhlu.

S dovolenou se tradičně pojí spousta záležitostí, ke kterým informační systémy potřebujeme. Nalezení hotelu, navigace, hledání zajímavých míst v okolí, komunikace s rodinou a přáteli. Ne každý z nás tráví celou dovolenou na mobilních datech, a proto se vám pokusím popsat, jaká rizika s sebou přináší využívání cizích sítí. Může se jednat o WiFi sítě na letištích, v kavárnách, hotelích a dalších veřejně přístupných místech. Nejde však pouze o bezdrátové WiFi sítě, stejné principy budou platit, i když budete využívat drátové připojení.

Začneme však u sebe samých, v našem domově. Troufám si říct, že naprostá většina domácností má k dispozici vlastní WiFi připojení. Máme tedy k dispozici vlastní router. Tahle kouzelná krabička toho umí mnohem více, než jen zprostředkovávat přístup k internetu. Každý router je jiný, ale platí, že router vidí do naší komunikace, aby ji mohl posílat dále. Ne každý využívá plný potenciál tohoto zařízení. Klasický domácí router v sobě kombinuje funkčnost více síťových zařízení, aby pro domácnost byl jednoduchý k používání. Prakticky je ale možné, že router disponuje spoustou dodatečných nastavení, která zlepšují výkon či zvyšují bezpečnost sítě. Jedním z takových opatření může být mimo jiné filtrace nebezpečných stránek. Je to vhodný pomocník například pro rodiče, kteří svým dětem z různých důvodů chtějí omezit přístup k určitým stránkám na internetu. Většinou se jedná o pornostránky, ale prakticky je možné omezit i sociální sítě, videopřehrávače či jakékoli jiné zdroje obsahu na internetu.

Funkčnost této ochrany dokazuje, že prvky naší sítě sledují naší aktivitu a dokáží na ni reagovat. Co se stane, když se připojíme na cizí WiFi síť? Co všechno může správce, případně útočník, který je v roli správce,

vidět a nastavovat? Na tyto otázky a mnoho dalších se vám pokusím odpovědět v této kapitole.

Síť je pod kontrolou toho, kdo ji vlastní!

Pro běžného uživatele je počítačová síť taková černá skříňka, která mu umožnuje přistupovat k různým službám internetu. O tom, jak tato skříňka funguje a co všechno obsahuje, však uživatel netuší. V realitě se mohou v rámci této černé skříňky mezi vámi a webovou stránkou nacházet různá jiná zařízení. Většina z nich má za úkol zajistit požadované připojení, ale na síti se běžně nacházejí i různá bezpečnostní a monitorovací zařízení. Běžně se s nimi můžeme setkat například v zaměstnání, v našich kancelářích. Je v zájmu zaměstnavatele, abychom naši činnost vykonávali bezpečně a neohrozili nejen sebe, ale i jeho byznys. Z těchto důvodů uvědomělé společnosti nasazují různá bezpečností řešení. Firewally, které hlídají vstup a výstup do vnitřní sítě. Antivirová řešení, která hlídají nebezpečné soubory v našich počítačích. Behaviorální sondy, které hlídají naši aktivitu

na síti a hledají v ní vzorce, co by mohly ukazovat na to, že jsme byli napadeni nebo sami na někoho útočíme. A spoustu dalších opatření, o kterých jako uživatel nevíte. Proč zde ale zmiňuji bezpečnostní opatření, když se tato kniha zabývá nástrahami na internetu? Zmiňované technologie mají v rukou administrátora velkou moc, jelikož je schopen vidět vaši činnost a na základě různých kritérií ji ukládat, blokovat a sledovat. Podobné technologie mohou používat také hackeři a monitorovat a analyzovat tak chování uživatele na síti.

Tyto technologie nelze nasazovat jen tak, je třeba mít k dispozici vlastní síť, na které můžeme provádět prakticky cokoliv. Z toho důvodu se nejdřív na nějakou takovou síť musíme připojit. Proč bychom se ale dobrovolně připojili na nebezpečnou WiFinu?

Nebezpečná síť se nejmenuje „nebezpečná síť“

Vytvořit si vlastní síť není ani pro neajťáka nic extra těžkého. Stačí vám k tomu mobilní telefon a mobilní data. Vytvářeli jste někdy někomu mobilní

hotspot, aby se skrze váš telefon byl schopen připojit k internetu? Pokud je vaše odpověď „ano“, tak jste dokázali vytvořit vlastní počítačovou síť, vlastní WiFinu. Ostatní zařízení, kterým poskytnete heslo, se mohou k telefonu připojovat a skrze něj přistupovat k internetu. V tomto případě máte možnost si libovolně pojmenovat tuto síť a nastavit vlastní heslo. Vy jste v tento moment ten, kdo síť ovládá.

Při vytváření hotspotů skrze naše mobilní telefony jsou naše možnosti konfigurace značně omezené. Útočníci využívají stejný princip, jen pro zajištění připojení využívají externí síťové karty, malé snadno přenosné routery a notebooky. Dostanou tak možnost provádět pokročilé nastavování a síť si mohou upravit dle své libosti. Pokud používáte jakoukoliv formu nešifrované komunikace, bude útočník schopen vidět cokoliv, co na síti provádíte. Pokud přistupujete pouze na stránky s validním „zeleným zámečkem“, musí se útočník snažit trochu více, jelikož obsah komunikace pro něj bude nečitelný.

Existuje jeden typ útoku, který je zde obzvláště nebezpečný. Nazývá se pharming, přeloženo jako farmaření. Pamatujete na zmínku o systému DNS, který se stará o překlad doménových jmen na číselné adresy

konkrétních serverů? Rychle si to v jednoduchosti připomeneme. Systém DNS je soustava serverů na internetu, které uchovávají číselné adresy ostatních serverů, jelikož alfanumerická jména jsou pro člověka lépe zapamatovatelná než pouhá čísla. Když do adresního řádku prohlížeče napíšete například google.com, váš počítač provede dotaz na nejbližší DNS server: „Nevíš, jakou adresu má server google.com?“ V případě, že to nejbližší DNS server ví, odpoví například – „Ano, je na adrese X.X.X.X.“ Za symboly X se dosazují čísla s hodnotou 0 až 255. V případě, že jeho adresu nezná, zeptá se jiného DNS serveru a následně vám vrátí odpověď. Pokud se vám taková odpověď vrátí, váš počítač bude schopen se k vzdálenému serveru připojit.

V případě, kdy je síť pod kontrolou útočníka, může mít plnou kontrolu také nad systémem DNS. Začátek komunikace je stejný. V momentě, kdy do adresního řádku zadáte google.com, váš počítač provede dotaz na nejbližší DNS server – „Nevíš, jakou adresu má server google.com?“ – a nejbližší DNS server, který je pod kontrolou útočníka, odpoví: „Ano, je na adrese Y.Y.Y.Y.“ Za hodnoty Y opět dosadí číselné hodnoty. Nyní jsme ale dostali v odpovědi na totožný požadavek naprosto jinou adresu. V případě, že má hacker na tomto

serveru připravenou i povedenou kopii oné požadované webové stránky, naše šance na odhalení tohoto podvrhu se blíží nule. Jako uživatel na stránce totiž uvidíme stejný obsah, stejnou adresu v adresním řádku, třeba i zelený zámeček. Tohle je příklad již docela pokročilého útoku, kde útočník musí projevit nemalou dávku šikovnosti, není však neproveditelný.

Jak rozeznám podvodné WiFi sítě?

Nespoléhejte na název sítě. Ani v případě, že se nacházíte v McDonald's a k dispozici je síť s názvem „McDonald's Free WiFi". Jak již víme, název sítě si vlastník může nastavit na téměř cokoliv. Z pohledu útočníků navíc dává smysl umístit svou vlastní WiFinu do lokality a s názvem, který by důvěřivý uživatel mohl očekávat. Navíc se jedná o ten nejjednodušší trik, kdy útočník nastaví název vlastní sítě na podobný nebo klidně stejný jako jiné WiFi sítě v dosahu.

Dalším znakem podvodné sítě je to, že není dobře zabezpečená. Pokud se jedná o naprosto otevřenou síť na nějakých veřejných místech, k jejímuž připojení není potřeba žádné heslo, jedná se o dost výrazné znamení, že

je buď po kontrolou někoho se špatnými úmysly nebo se dost pravděpodobně takoví lidé na této síti nachází.

Velmi běžným případem je také využívání „captive portálů“. Jedná se o webové stránky, které na vás vyskočí při prvotním připojení k jinak otevřené síti. Běžně po vás vyžadují nějakou akci. Může se jednat o přihlášení uživatelským účtem, registraci či jinou formu interakce. Ne vždy je toto indikace nebezpečné sítě. Technologie captive portálů se běžně využívá v hotelech, restauracích či na letištích. Rád bych ale opět zdůraznil, že stejnou technologii mohou jednoduše využívat i útočníci. V momentě, kdy by po vás podobný portál vyžadoval přihlášení, správce této sítě je schopen monitorovat a sledovat přihlašovací údaje, které do captive portálu zadáváte.

Sám se už z principu nikdy nepřihlašuji k neznámým sítím. Možná je to již důsledek mé profesionální deformace, ale plně důvěřuji pouze známým WiFi sítím. Tam, kde si nejsem jistý, využívám raději mobilní data a vlastní hotspoty.

Nutně se potřebuji připojit. Jak udělat maximum pro vlastní bezpečí i na veřejné síti?

V životě může nastat mnoho situací, kdy budete zrovna velmi potřebovat připojení k internetu a nebudete mít k dispozici mobilní data. Důvodů může být velká spousta – nutnost okamžitě odeslat dokument šéfovi či klientovi, vyhledání nejbližšího zdravotnického zařízení, rodinná urgence. Nebudeme se zamýšlet nad tím, co všechno by se muselo stát, abyste byli nuceni se dobrovolně připojit na cizí WiFi síť. Pro pokračování však předpokládejme, že taková situace nastala a nacházíme se například na volně dostupné WiFině na letišti či v kavárně. Nyní již máte představu, jaké hrozby se s používáním podobných síti pojí, a proto logicky vyvstává otázka – jak minimalizovat rizika spojená s použitím cizí WiFiny?

Tím nejjednodušším a nejefektivnějším je využívání VPN systému. Možná jste se s VPNkami setkali v pracovním či studijním prostředí, kde vám umožnily přístup k interním systémům organizace třeba i z home office, z vašeho obýváku. Primárním účelem VPN je vytvoření tunelu do jiné vzdálené sítě. Po připojení se

bude váš počítač či telefon tvářit, jako by byl fyzicky v dané síti. Z toho plyne další užitečná funkcionalita využívání VPN – dokáže zamaskovat vaši reálnou polohu. VPNky mají pro běžné uživatele ještě jednu skvělou vlastnost, veškerou komunikaci šifrují. Proto, budete-li se zapnutou VPNkou přistupovat i k aplikacím, které šifrování běžně neřeší, samotná VPN se postará o zachování důvěrnosti přenášených dat.

Tato ochrana je vzhledem k jednoduchosti použití velice účinná a rozhodně vám ji doporučuji na neznámých sítích vždy používat. Existuje spousta různých řešení, bezplatných i placených. Liší se v tom, kde se servery, ke kterým tunelové spojení vytváříte, reálně nacházejí. Liší se dále v tom, jakou rychlost komunikace vám dovolí přenášet, či v intuitivnosti ovládání. Asi nejdůležitějším aspektem při zvažování VPN je vhodný výběr poskytovatele. Pokud nemáte k dispozici vlastní servery, budete odkázáni na někoho, kdo vám dovolí připojovat se k těm jeho. Je nutné si uvědomit, že opět se zde dostáváme do situace, že ten, kdo vlastní VPN server, má nad nim plnou kontrolu. Když se k němu budeme připojovat, běžně se stává, že poskytovateli slepě důvěřujeme. Velcí poskytovatelé VPN připojení slibují maskování vaší reálné polohy skrze

rozmístěné servery po celém světě, stabilní a rychlé připojení, a také to, že o vás ani vašich aktivitách neukládají žádné údaje. To poslední je velmi diskutabilní a osobně mám problém důvěřovat třetím stranám, že žádná data neukládají. Není to snad proto, že bych potřeboval něco skrývat a tajit. Jde spíše o princip – když už využívám řešení, která mi mají pomoci zvyšovat bezpečnost na internetu a chránit mé soukromí, chci využívat pouze taková, kterým plně důvěřuji. Volte proto moudře, udělejte si vlastní průzkum dostupných řešení a zvažujte jejich pro a proti.

VI. Malware – digitální podsvětí

Hackeři využívají k infikování svých cílů velkou škálu škodlivých programů a utilit. Hromadně je nazýváme malware. Tyto škodlivé programy mají spoustu podob a dělíme je do několika kategorií. Například dle účelu, ke kterému byly vytvořeny, či dle způsobu, jakým se šíří. Existuje obrovské množství malwaru, ale zde se zaměříme pouze na ty nejčastější a nejnebezpečnější typy. Pokusím se vám také vysvětlit, jak antivirová řešení bojují proti škodlivým programům a jak hackeři bojují proti antivirům. Opět nebudu zacházet do technických detailů, ale z vyšší perspektivy se vám budu snažit popsat principy, které vám pomohou rozpoznávat různé druhy malwaru a efektivně se proti nim chránit.

Trojský kůň – zadní vrátka do systému

Troufám si říct, že „trojan“ je ten nejznámější druh malwaru. Mimo jiné díky všeobecně známému příběhu o řeckých válečnících, kteří pod vedením Odyssea obelstili a nakonec dobyli Tróju. Jejich mazanost spočívala ve vytvoření návnady ve formě velkého dřevěného koně, který měl symbolizovat kapitulaci řeckých snah o dobytí města. Trójané koně zavlekli do města a v noci, když stráže byly nepozorné, vyskočili z koně ukrývající se Řekové a otevřeli brány zbytku armády, který čekal skrytý za hradbami. Díky této fintě se Řekové dostali nepozorovaně do vnitra Tróji a ve vhodný moment zaútočili. Zde ukončím svou vsuvku z historie a přesuneme se do přítomnosti, kde se princip pasti s dřevěným koněm hojně využívá i ve světě jedniček a nul.

Představte si nyní místo trojského dřevěného koně nějaký počítačový program či počítačovou hru. Mnoho programů, aplikací a her bývá placených a stává se, že uživatelé hledají cesty, jak je získat bezplatně. Začnou proto pátrat na internetu a pravděpodobně najdou portál či úložiště, kde se požadovaný obsah

poskytuje bezplatně. Tato aplikace či hra může být náhradou řeckého dřevěného koně. Součástí souborů, které si s aplikací stáhnete, může být vložený útočníkův kód. Jakmile jej nainstalujete, bude sloužit jako zadní vrátka, která je útočník schopen zneužít a získat tak přístup do vašeho počítače. V analogii s příběhem o dobytí Tróje představuje vložený škodlivý kód skupinu řeckých válečníků a váš systém město schované za hradbami.

Pokud se vám povede si do počítače nainstalovat trojského koně a přítomná bezpečností opatření jej neodhalí, může to mít několik vážných důsledků. Trojský kůň se zamaskuje do jiných procesů či souborů v počítači a stane se mnohem hůře odhalitelným. Současně s tím může provádět krádež různých citlivých údajů uložených ve vašem operačním systému nebo právě zprostředkovat nepozorovaný přístup útočníkovi. Ten může tiše převzít kontrolu nad vaším počítačem a provádět další útoky s cílem získat vaše hesla či útočit na ostatní zařízení připojená ke stejné síti.

Počítačový virus – infekce se šíří

Princip infikace zařízení počítačovým virem je mnohdy stejný jako v případě trojského koně. Uživatel si ho odněkud stáhne, a pokud jej bezpečnostní systém včas neodhalí, pak se také nainstaluje. Virus se ale od trojského koně výrazně liší ve svém chování. Trojský kůň se snaží zamaskovat a nepozorovaně poskytnout přístup útočníkovi. Virus je naopak velmi agresivní. Začne napadat ostatní soubory v systému a replikovat sebe sama do všech jeho částí. Snaží se plně infikovat systém, a když dostane šanci, bude útočit i na ostatní dostupná zařízení ve svém okolí.

Cíle počítačového viru mohou být stejné jako v předchozím případě. Krádež citlivých dat či stažení jiného malwaru, ale ve většině případů se jedná spíše o zničení dat a znemožnění používání systému. Jeho chování je tedy více destruktivní. Existují také případy, kdy se za tímto násilným přístupem schovávají sofistikované metody infiltrace jiných částí, a tato destrukční činnost funguje pouze jako kamufláž.

Některé počítačové viry jsou obzvláště chytré a kromě modifikace ostatních souborů v systému dokáží měnit i sebe sama. Je to způsob, jak se vyhýbat

detekčním mechanismům, zůstat přítomný v systému co nejdelší dobu a napáchat co možná největší škody.

Dopady úspěšné infikace počítače virem mohou být velmi nepříjemné nejen pro firmy, ale také pro běžné uživatele. Ze zkušenosti vím, že mnozí z nás si svá data pravidelně nezálohují, a proto poničení systému virem může vést k trvalé ztrátě uložených dat. Dále pak k problémům spojených s obnovou systému, která většinou obnáší kompletní přeinstalaci celého operačního systému.

Adware – nežádoucí reklamy

Škodlivé programy z rodiny adware nejsou zaměřeny na krádež uživatelských dat či znemožnění používání systému. Naopak po instalaci a uvelebení se v systému začne adware uživateli zobrazovat nechtěné reklamy. Může se jednat o legitimní i podvodné produkty a služby, pornostránky, burzy či obchody. V podstatě záleží čistě na útočníkovi, co bude adware uživateli zobrazovat. Pokročilejší varianty adware programů dokáží také sledovat aktivitu uživatele na daném zařízení a zobrazované reklamy i přizpůsobovat. Například

fyzické lokalitě zařízení či různými překlady relevantními pro uživatele. Přítomnost adwaru v zařízení značí například zvýšené množství vyskakovacích oken, různé reklamní bannery či vkládání odkazů do různých částí vaše počítače.

Běžně se při marketingových kampaních vyplácí provize tomu, kdo reklamu zprostředkovává – například za každý proklik. Právě snaha o finanční zisk bývá nejčastějším účelem šířením adware programů a snahou jejich tvůrců o získávání maximálního počtu prokliků.

Spyware – vidí každý tvůj krok

Spyware je špionážní software. První, co spyware po infikaci zařízení udělá, je to, že se důkladně v systému ukryje, aby zůstal v systému přítomný co nejdéle bez povšimnutí uživatele i bezpečnostních opatření. Následně začne sledovat vaši činnost a bude o vás a o systému sbírat informace. Opět záleží na konkrétním typu spywaru a záměrech útočníka, ale prakticky může spyware odhalovat vaše hesla, monitorovat aktivitu na internetu, analyzovat vaše chování nebo dlouhodobě sledovat, co na klávesnici píšete. Také může například

v tichosti procházet vaším operačním systémem a vyhledávat soubory s citlivým obsahem. Nasbírané informace následně různými skrytými kanály odesílá na vzdálený útočníkův server a ten je pak zneužívá pro svůj prospěch. Může je zveřejnit, použít pro vlastní potřebu či klidně prodat.

Kromě narušení soukromí mívá spyware také negativní vliv na výkon zařízení a rychlost internetového připojení. Podobně jako u adwaru se může projevovat vyskakovacími okny, změnami systémových nastavení a jiným rušivým chováním.

Červ – prokouše se sítí

Cílem počítačového červa je počítačová síť, přesněji zařízení na počítačové síti. To je významný rozdíl od předešlých typů malwaru popisovaných v této kapitole, které se zaměřovaly především na infikaci jednoho zařízení. Důležitou vlastností červa je schopnost replikace bez nutnosti zásahu uživatele. To znamená, že se sám dokáže šířit počítačovou sítí a infikovat další dostupná zařízení. Je pravdou, že cílí spíše na rozsáhlejší

podnikové sítě, ale stejně tak je jeho použití pro útočníky uplatnitelné i pro malé domácí sítě.

Počítačový červ dokáže šířit další škodlivé programy a podílet se tak na velkých útocích. Významnou roli hraje například při provádění ransomware útoků či přidávání napadených zařízení do botnet sítě. O tom, co je to ransomware a botnet, se budeme bavit v další části.

Červ, stejně jako ostatní druhy malwaru, má potenciál provádět velmi sofistikované útoky, které jsou omezeny zejména schopnostmi a kreativitou jeho tvůrce. Kromě šíření sebe sama a přídatného malwaru dokáže znatelně také přetížit počítačovou síť a omezit či úplně znemožnit přístup uživatelům k dostupným službám.

Obrana proti malwaru, co se šíří po síti, je spíše v rukách administrátorů než běžných uživatelů. Spočívá v implementaci vhodných bezpečnostních opatření, jako je například segmentace sítě do menších, vzájemně nepropojených celků. Dále pak v nasazení vhodného firewallu, nastavení komunikačních pravidel či třeba zavedení behaviorálních sond, které sledují aktivitu uživatelů a hledají v ní vzory známých útoků.

Ransomware – jak si hackeři spoří na důchod

Nyní máte docela pěkný vhled do různých typů malwaru. Ransomware je útok, který kombinuje funkce více různých typů škodlivých programů a dokáže nadělat velmi vážné škody. Zaměřuje se především na společnosti a organizace, které fungují na větších počítačových sítí, využívají více různých služeb a standardně mají mnoho uživatelů. Cílem ransomware je ovládnout všechny části počítačové sítě a legitimním uživatelům znemožnit je používat. Využívá k tomu principy kryptografie. Úspěšný ransomwarový útok zašifruje všechny dostupné systémy a data, která se tak pro své vlastníky stanou nečitelnými. Pokud společnost nemá vhodným způsobem nastavené zálohování, nebude schopná sama data a systémy obnovit. A to ani nechci zacházet do takových detailů, že i zálohy mohou být kompletně zašifrovány. Z našeho předchozího úvodu do kryptografie z kapitoly o „zeleném zámečku“ víme, že principem šifrování není data zničit, nýbrž zajistit, že pouze ten, kdo zná správný dešifrovací klíč, bude schopen data přečíst a použít. V tomto případě jediný, kdo zná dešifrovací klíč, je hacker či skupina hackerů

stojící za útokem. A zde se dostáváme k hlavnímu principu ransomware.

Název vznikl z anglického „ransom“, v překladu „výkupné“. Za většinou ransomwarových útoků stojí motivace k finančnímu prospěchu. Hackeři po úspěšném dokončení útoku svou oběť kontaktují a nabídnou dešifrovací klíč výměnou za nějakou tučnou částku, kterou si většinou vyžádají v kryptoměnách. V kryptoměnách proto, že jim pomohou zůstat jen velmi těžce dohledatelní kýmkoliv, kdo se bude pokoušet o vyšetřování tohoto incidentu.

Podle Reuters, což je zpravodajská agentura patřící společnosti Thomson Reuters Corporation, pokořila celková částka zaplacená ransomwarovým skupinám v roce 2023 jeden bilion dolarů. Navíc jsou tato čísla, včetně množství ransomwarových útoků, každým rokem vyšší. Tento trend je viditelný i přesto, že se vždy doporučuje výkupné neplatit. Nejen, že se tím přímo podporuje organizovaný kybernetický zločin, ale také si oběť musí uvědomit, že platí pouze za „příslib“ navrácení dat. Po případném zaplacení výkupného organizace spoléhá na poctivost hackerů a věří jejich slibu, že ukradená data vrátí. Důvěřuje, že na ně nezaútočí znovu a že poskytnou správný dešifrovací klíč.

Asi chápete, že se zde nachází příliš mnoho „pokud“ a celý úspěch zprovoznění našich systémů zaplacením výkupného závisí pouze na důvěryhodnosti toho, kdo nás napadl.

Jaký tedy mohou mít společnosti důvod, že vůbec zaplacení výkupného zvažují? Ransomwarový útok je velmi komplexní záležitost a jeho provedení je časově i technicky velmi náročné. Může trvat měsíce i roky, než se hackerské skupině podaří nepozorovaně infikovat celou síť. Také z tohoto důvodu si hackeři své oběti pečlivě vybírají. Znají o nich všechny veřejné informace a při své činnosti získají i spoustu interních. To pomůže hackerům mimo jiné nastavit „ideální“ výši výkupného. Bývá vybalancovaná tak, aby nebyla pro společnosti likvidační, a také tak, aby oběti došlo, že bude levnější zaplatit výkupné a okamžitě se vrátit do plného provozu, než procházet složitým procesem obnovy.

Představme si, že obětí je například obrovský výrobní podnik. Každou hodinu, kterou jeho výrobní linky stojí, narůstá ušlý zisk, mohou se kazit materiály nutné pro výrobu. Stále musí platit mzdy svým zaměstnancům a pravděpodobně má také závazky vůči svým klientům. Následně můžeme uvažovat také nad zaplacením profesionálů, kteří s obnovou pomohou,

a případnými novými licencemi pro potřebný software. Suma sumárum se částka nutná k opětovnému zprovoznění podniku může vyšplhat velmi vysoko, a proto se často zaplacení výkupného zdá jako snadnější cesta.

Ransomware je velice komplexní útok, za kterým většinou stojí více než jen jeden útočník. Je známo mnoho skupin, které tento typ útoku využívají, liší se mimo jiné ve způsobech jeho provádění. Útočníci mají mnohdy navrch a oproti svým obětem vládnou velkou výhodou. Souvisí to s vysokou mírou byrokracie a nutností schvalování, než se například nějaké bezpečnostní řešení ve firmě zavede. Útočníci jsou ve svém počínání rychlejší a flexibilnější.

Během své praxe jsme měl několik příležitostí se s ransomwarem setkat i mimo testovací laboratoře. Podílel jsem se na vyšetřování průběhu takovýchto útoků, pomáhal jsem s obnovou napadené infrastruktury. Vedl jsem také vyjednávání s hackerskou skupinou, s cílem získat čas a případné informace, které by nás mohly k útočníkům přiblížit. Z této akce jsem si odnesl jednu velmi překvapivou zkušenost. I když se jedná o organizovaný kybernetický zločin, cílem většiny skupin jsou opravdu pouze peníze. Z toho důvodu

nevídáme příliš mnoho útoků na zdravotnická zařízení, naprostá většina z nich je mířena na výrobu, rafinérie, logistiku, státní instituce. Skoro si až člověk říká, že i black-hat hackeři mají svědomí. Dále jsem zjistil, že když hackeři společnost napadnou, vždy ji zanechají jasná vodítka s návody, jak se s nimi zkontaktovat. Většinou se jedná o formu online chatu prostřednictvím dark webu. I o tomto velmi zajímavém zákoutí internetu si v knize budeme povídat.

Když jsem vyjednával se skupinou, která klienta napadla, velmi mě překvapila jejich reakční doba. Požadovali jsme například důkazy o tom, že jsou opravdu schopni naše soubory dešifrovat, načež nám do pár hodin dodali testovací dešifrovací program, který tři vybrané soubory obnovil. Odpovědi na komunikaci byly někdy okamžité. S kolegy jsme se shodli na tom, že i když neschvalujeme, co provádějí, tak s následnou komunikací fungují mnohem lépe než kdejaká IT podpora.

Botnet – farma infikovaných zařízení

Botnet je označení pro síť infikovaných zařízení, které nazýváme boti. Botnet tedy není druh malwaru, ale je s ním velmi úzce spjatý, a proto si ho dovoluji do této kapitoly zařadit. Představte si klidně milion zařízení – od serverů a počítačů přes mobilní telefony po všelijaká chytrá zařízení. Chytrá televize, kamery, různé senzory, kávovar či klidně chytrá lednička mohou být součástí botnetu. Všechna tato zařízení jsou v podstatě malými počítači, a proto abychom je mohli vzdáleně ovládat, připojujeme je k síti.

Prakticky každé z těchto zařízení může být napadnutelné. Využijeme to, co již známe. Klidně se o infekci může starat počítačový červ, který šíří infekci po síti. Může šířit například trojského koně, který útočníkům umožní vzdálené ovládání zařízení skrze připravená zadní vrátka do systému.

Víme tedy, co je to botnet, jak může vznikat a rozšiřovat se. K čemu je ale útočníkům mít k dispozici přístup k takovému množství zařízení, ze kterých jen těžko získají nějaká užitečná data? V tom případě je cílem útočníků vybudovat síť zařízení, která budou hromadně vzdáleně ovládat a využívat k dalším útokům

na různé cíle v internetu. Představte si, že těchto milion zařízení v tu samou chvíli začne útočit na nějaký webový server v internetu. Díky fyzicky geograficky odděleným zařízením a jejich distribuci v rámci planety získávají útočníci zbraň s ohromnou silou. Pokud nejsou nastavena vhodná bezpečnostní opatření, může velmi snadno dojít k přetížení a zhroucení serveru, na který se útok zaměří. Takovému útoku říkáme DDoS – „Distributed Denial-of-Service“, v překladu „Distribuované odepření služby“.

Jeho dopadem může být chvilkový, ale i dlouhodobější výpadek služeb. Velkým strašákem jsou DDoS útoky pro služby, které garantují svým zákazníkům 24/7 dostupnost. To mohou být například banky či burzy. Ve veřejném sektoru se může jednat například o systémy bezpečnostních složek či jiných služeb kritické infrastruktury státu. Docela oblíbeným cílem útoků DDoS bývá nějaká dlouho dopředu plánovaná veřejná akce. Třeba státní volby a jejich narušení mohou být kýženým cílem hackerů z různých států. Dalším častým cílem jsou například herní servery, na které se útok zaměřuje s cílem odepření přístupu ostatním hráčům. Častým cílem jsou také technologické společnosti, které například poskytují IT infrastrukturu

svým klientům, a pro které by výpadek jejich služeb mohl mít významný dopad na jejich byznys.

Mít, či nemít antivirák? To je to, oč tu běží

Obecně vzato platí, že antivirové řešení by mělo být nasazeno všude, kde je to možné. Antiviry neodhalují pouze viry, nýbrž analyzují veškerý známý malware. To, že se ve svém názvu odkazují pouze na viry, neznamená, že se se zaměřují pouze na tento typ malwaru.

Existuje velké množství antivirových řešení. Některá jsou integrována přímo do operačního systému, jiná je třeba zvlášť doinstalovat. Některá jsou bezplatná, jiná placená. Liší se svými detekčními schopnosti, přidruženými moduly i cenou. Nebudu zde doporučovat žádné konkrétní řešení, naopak vám doporučuji provést si vlastní analýzu a zjistit, které řešení je pro vás nejvhodnější.

S existencí moderních kybernetických hrozeb muselo také dojít k vylepšení detekčních technologií. Moderní bezpečnostní řešení dokáží analyzovat chování

škodlivých programů, hledat známé vzorce útoků či detekovat různé anomálie v chování uživatele či systému. Jedná se však o dost pokročilé a rozsáhlé téma, proto se vám pokusím vysvětlit, jak fungují starší typy antivirových strážců. Z pohledu technologického pokroku je lze označit za „starší“, neznamená to však, že by se v dnešním světě již nepoužívaly. Naopak se stále jedná o nejrozšířenější řešení, vzhledem k jejich jednoduchosti a efektivnosti odhalovat známý malware.

Tento typ antivirových strážců funguje na bázi takzvaných signatur. Představme si, že máme nějaký textový soubor uložený na disku ve svém počítači. Existují algoritmy, způsoby a postupy, jak vypočítat jeho signaturu. Tu nyní vypočteme. Pak uděláme náhodnou změnu v původním souboru, stačí změnit jediné písmenko. Když signaturu vypočteme znovu, bude mít jinou hodnotu. Signatura je alfanumerická hodnota, která nám pomáhá zaručit, že v souboru nedošlo k žádné změně. Je vypočtena jednosměrnou funkcí, nedá se zpětně odvodit. Výhodou je, že můžeme mít libovolně velký soubor v libovolném formátu, ale jeho signatura bude vždy alfanumerický řetězec fixní délky.

Může to znít docela složitě, ale uvažujme o souboru jako třeba o rodinném domě. Jeho signatura

bude například fotografie ve vašem telefonu. Když se na domě změní například střecha nebo barva fasády, po porovnání s originální fotkou snadno zjistíte, že nějaká změna proběhla. Jeho novou signaturu získáte tak, že fotografii pořídíte znovu.

Běžná antivirová řešení mají k dispozici miliardy signatur, které poukazují na známé škodlivé soubory. Jejich databáze se často aktualizuje, aby měly k dispozici nejnovější informace. Následně tyto antiviry kontrolují soubory v počítači tak, že spočítají jejich signaturu, porovnají její hodnotu s hodnotami ve své databázi, a pokud najdou shodu, označí soubor jako malware.

Můžete se nyní ptát – co když si vytvořím vlastní malware, budou ho tyto klasické antiviry detekovat? Co když si nějaký malware stáhnu, ale poupravím si ho? Tohle jsou naprosto skvělé otázky! Odpověď zní, že pokud to uděláte dobře, antiviry tento malware neodhalí, jelikož nebudou znát jeho signaturu. Je to jeden z důvodů, proč je pro hackery relativně jednoduché antivirová řešení obcházet.

Neznamená to však, že jsou klasické antiviry bezúčelné. Je také pravdou, že běžně se různá antivirová řešení učí od sebe navzájem a sdílejí mezi sebou informace o nových nalezených signaturách škodlivých

programů. Navíc velké společnosti zabývající se vývojem bezpečnostních řešení mají dedikované týmy, které denně pomáhají odhalovat nové hrozby. V systému mají tyto klasické antiviry svou důležitou roli, ale je nutné je doplnit o další opatření, která dokáží analyzovat kromě signatur také právě chování programů a uživatelů. V takovém případě mluvíme běžně o „next-generation AV“, v překladu antivirech nové generace.

VII. O oknech, tučňákovi a jablku

Věčný boj oken, tučňáka a jablka, který bývá mnohdy předmětem vášnivých debat ajťáků i neajťáků. Při vymýšlení názvu této kapitoly jsem si nemohl odpustit ji pojmenovat touto hantýrkou, ale věřím, že jste již poznali, že se bude zabývat operačními systémy Windows od společnosti Microsoft, macOS společnosti Apple a Linuxem, což je otevřený operační systém vyvinutý panem Linusem Torvaldsem.

Často se mě lidé ptají, který systém je nejlepší či nejbezpečnější. Někteří lidé si nekompromisně stojí za tím, že právě ten, který používají oni sami. Já si naopak myslím, že každý má své klady a zápory. Nejlepší operační systém pro vás bude takový, který splňuje vaše požadavky na funkcionalitu, výkonnost, intuitivnost, přizpůsobitelnost a mnoho dalšího.

Žádný z těchto typů operačních systémů nebyl vyvinut přes noc, naopak první verze vyšly před desítkami let a od té doby se razantně proměnily. Nebudu se zaměřovat na nějakou konkrétní verzi,

naopak bych se rád v této kapitole věnoval jejich principům a cílovým skupinám. V krátkosti se také na každý z nich podíváme. Budu vycházet ze svých osobních zkušeností a názorů. Nemusíte se bát, že bych zde kopíroval všeobecné poučky, které najdete pod prvním odkazem ve vyhledávání.

Okna (Microsoft Windows)

Operační systém Windows z dílny Redmondského gigantu je dlouhodobě nejpoužívanějším systémem na osobních počítačích. Není omezený na nějaký konkrétní hardware, je použitelný na počítačích různých výrobců. Ve svých počátcích byl velmi známý pro své chyby a neduhy, které mnohdy končily slavnou „modrou smrtí“. Jedná se o stav, kdy se systém zhroutí a není jiné možnosti obnovy, než ho restartovat. S postupem času se Windows několikrát razantně proměnil, a to vizuálně i funkcionálně. Moderní Windowsy jsou velmi pěkné a uživatelsky přívětivé systémy, které nabízí spoustu možných funkcí, aplikací a možností přizpůsobení.

V dnešní době jsou také základním prvkem většiny firem a organizací, například z důvodu snadné a efektivní integrace podnikových systémů a jejich hromadné správy.

Jablko (Apple macOS)

Pro mnohé lidi je Apple zárukou kvality a luxusu. Na rozdíl od MS Windows jsou jeho operační systémy využívány „pouze“ na Apple hardwaru. I tato mince však má své dvě strany. Na jednu stranu je zde velký potenciál vytvořit maximálně efektivní souznění hardwaru a softwaru . Na tu druhou by se dalo namítat, že se Apple tímto ochuzuje o širší rozšíření systému mezi koncové uživatele.

Zařízení a operační systémy společnosti Apple cílí především na uživatele, kteří chtějí intuitivní a spolehlivý systém, který jim bude primárně zefektivňovat jejich práci či jim bude společníkem během trávení volného času.

Tučňák (Ubuntu, Fedora, Kali,...)

Existuje spousta Linuxových distribucí, které se liší zamýšleným využitím i vzhledem. Běžně jsou zdarma dostupné a dají se nainstalovat téměř na libovolný kus hardwaru. Mají společné to, že cílí především na zkušené až profesionální uživatele, kteří mají vyšší nároky a složitější požadavky oproti běžným uživatelům. Může se jednat o vývojáře, síťové administrátory, bezpečnostní experty, hackery, studenty a jiné. Pro jejich efektivní využívání jsou nutné určité IT znalosti, jelikož často se v nich uživatel pohybuje pouze prostřednictvím příkazového řádku.

Mnoho lidí si to neuvědomuje, ale právě Linux a jeho odvozené varianty jsou tím nejpoužívanějším operačním systémem na světě. Většina serverů, které hostují webové i jiné služby, běží na linuxových systémech. Mobilní operační systém Google Android je založen na Linuxu. Dokonce kořeny macOS od Applu sahají k určité Linuxové distribuci. Je využit také v nejrůznějších chytrých domácích i firemních zařízeních. Také ve velkých superpočítačích.

Všechno je to možné díky tomu, že Linux byl a je dostupný jako otevřený systém, nad kterým má uživatel

plnou kontrolu. Může upravovat veškeré části systému. V rukách nezkušeného uživatele se může systém snadno pokazit, ale v rukách profesionála nabízí spoustu zajímavých možností.

Vyberte si správný systém dle svých potřeb

Jsem zastánce názoru, že nelze jednoduše říct, který z těchto tří systémů a jejich verzí je ten nejlepší. Záleží vždy primárně na tom, co od svého zařízení a systému očekáváte. Pokud hledáte počítač pro běžné používání, budete asi volit mezi Windows a macOS. Pokud je vaším záměrem rozjet ty nejmodernější hry, sáhnete pravděpodobně po MS Windows, jelikož je pro ně obecně nejvhodnější. Je-li pro vás důležitý maximální komfort pro práci a chcete, aby byl váš systém co nejjednodušší na používání, pravděpodobně si vyberete macOS. A když jste ajťák, co potřebuje či chce mít 100% kontrolu nad svým systémem, zvolíte některou z Linuxových distribucí.

Který z nich je ale nejbezpečnější?

Ani jeden. Kéž by to bylo tak jednoduché – vybrat si správné zařízení, správný systém a již nikdy neřešit kybernetické hrozby. Pro každý systém existují specifické druhy malwaru. Obecné útoky na bázi sociálního inženýrství jsou aplikovatelné vždy bez ohledu na používaný operační systém. Je také nutné si opět uvědomit, že tyto systémy vytvářejí lidé. Ať už omylem a neúmyslně, anebo naopak záměrně, může se v systému objevit chyba. Její úspěšné zneužití často znamená napadení systému či jeho částí. Ať už se rozhodnete pro jakýkoliv operační systém, nevěřte slepě tomu, že je nenapadnutelný. Antivirová řešení, pravidelné aktualizace a vhodné nastavení systému jsou pouze začátek. Žádné bezpečnostní řešení není všespásné, a proto velká část zodpovědnosti stále leží na našich bedrech. Na bedrech uživatelů a administrátorů.

Který OS osobně používám?

Všechny. Pro běžnou práci a zábavu využívám okna i jablka. Pro vlastní stránky, aplikace a jejich vývoj

zase různé Linuxové distribuce. Pro trénink, výzkum v oblasti kybernetické bezpečnosti a hackování využívám vlastní sítě, na kterých jsou počítače (virtuální i fyzické) všech tří typů a v různých verzích. Kromě množství funkcí, které toto diverzifikované portfolio systémů nabízí, mě experimentování s novými i staršími technologiemi velmi baví. Pokud jste také technologickým nadšencem či nadšenkyní, doporučuji si vyzkoušet práci i v nekonvenčních systémech, rozšiřovat si tak své znalosti a nabírat cenné zkušenosti. Umění do hloubky ovládat různé druhy operačních systémů je velmi cenná schopnost, která vám může pomoci i ve vašem profesním růstu.

VIII. Dark web – temná zákoutí sítě

Internet a jeho temná zákoutí. Je opravdu tak temný, jak jeho název popisuje? Co vše se dá na dark webu najít? K čemu se používá a jak funguje? Je přistupování do něj ilegální? Nejen na tyto otázky se vám pokusit odpovědět v této kapitole.

Přestože je dark web nejčastěji spojován s nelegálními aktivitami, dá se na něm najít i běžný obsah. Přistupování k dark webu samo o sobě není nelegální, i když v některých státech světa může být mnohem více regulováno. Nejprve si ale ujasníme terminologii, abychom dokázali správně definovat, co dark web je a co není. Začneme od jeho protipólu, tedy clear webu. Zde si můžete představit nejrůznější veřejně dostupné stránky a portály, pro které není potřeba žádné přihlášení. Můžeme sem zařadit internetové vyhledávače, Wikipedii, různé mediální a zpravodajské portály. Velmi často se setkáváme s vizualizací formou ledovce, jehož špička je vidět nad hladinou, ale velká část ledovce zůstává skryta pod ní. V kontextu celého

internetu je clear web právě ta špička, která je velmi jednoduše dostupná komukoliv s připojením k síti a zařízením, které je schopno zobrazovat webové stránky. Vědecké zdroje se často neshodují, jak velká tato část internetu je, ale obecně se udává, že se jedná přibližně o 4 % celkového obsahu internetu. Tyto nižší jednotky procent symbolizují právě onen vrchol ledovce, který se houpá na moři.

Po hladinou začíná oblast deep webu. Zde se nachází obsah, který je nepřihlášenému uživateli skrytý. Troufám si říci, že se během své činnosti na internetu setkáváte nejčastěji právě s tímto obsahem. Jedná se o různé sociální sítě, e-maily, bankovní systémy a jakékoliv další aplikace, které vyžadují právě vaše přihlášení. Je to část internetu, která není webovými prohlížeči indexována. To znamená, že ji běžné automatické nástroje neskenují a neprozkoumávají její obsah, aby vám ho následně nabídly při vašem vyhledávání. Dává to smysl, protože je přeci velmi nežádoucí, aby nějaký robot procházel a analyzoval váš bankovní účet, četl vaše e-maily či zprávy na sociálních sítích. Vrátíme-li se k analogii s ledovcem, který symbolizuje celý internet, většina jeho těla pod hladinou

se dá přirovnat právě k deep webu. Obecně se uvádí, že jde až o 90 % celého obsahu internetu.

Poslední kategorií je dark web, který najdeme na samém spodku našeho ledovce. Přestože existují určité vyhledávače také pro dark web, obecně se zde nachází stránky, které nenajdete jinak, než že se k vám dostane jejich adresa. Může se tak stát, že vám ji někdo přepošle nebo ji například najdete na jiných clear či deep web stránkách. Co všechno na nich ale můžeme najít, to si necháme na další kapitolku. Pozorný čtenář si však již nejspíš spočítal, že se dark web podílí na přibližně 6 % obsahu celého internetu. Ještě pozornější čtenář si uvědomil, že množství volně dostupných informací na internetu je obecně menší než množství publikovaných informací na jeho temnějších zákoutích.

Co vše se dá na dark webu najít?

V předešlých kapitolách jsme si vysvětlili, jak webové stránky fungují a proč mohou být nebezpečné. Úplně stejné principy platí pro webové stránky dostupné na dark webu. Opět platí, že vlastník stránek nad nimi má plnou kontrolu a může zde publikovat libovolný obsah. U clear webu narážíme na jednu velmi důležitou vlastnost. Vlastník webové serveru či domény je standardně známý a jednoduše dohledatelný. Navíc je pro poskytovatele internetu i různé kontrolní společnosti či organizace velmi jednoduché přístup k těmto stránkám regulovat. Narážíme zde tedy na problém možné cenzury a regulace přístupu k informacím. Také například i na to, že může být složitější provozovat na clear webu stránky anonymně.

Dark web principiálně odbourává tyto problémy. Pokud vlastník stránek chce, může svou činnost provozovat naprosto anonymně a publikovat cokoliv, co se mu zlíbí. Hlavním záměrem při tvorbě této sítě bylo dát uživatelům možnost anonymně sdílet informace, soubory, přistupovat k nim a procházet internet bez cenzury a místních omezení. Prvotní myšlenka je tedy opět čistá. Velký zájem se objevil například u autorů

a žurnalistů, kteří tímto způsobem mohli publikovat své názory veřejně, bez cenzurních opatření svého státu.

Jak už to tak ale bývá, mnozí pochopili, že jejich nová „nedohledatelnost“ v digitálním světě může nést i jiné ovoce. Objevily se proto internetové obchody s různým nelegálním zbožím, jako jsou zbraně či drogy.

Osobně jsem párkrát během svých průzkumných a výzkumných činnostech narazil na portál, kde bylo možné si zakoupit tank či vojenskou helikoptéru získanou z nějakého černého trhu. Platidlem v těchto internetových obchodech jsou zpravidla kryptoměny. Jedná se o virtuální měnu založenou na složitých kryptografických principech, do kterých v této knize nechci zabředávat. V případě onoho tanku či helikoptéry nebyla uvedena cena, ale navazovala se separátní komunikace. Řekl bych, až taková analogie k tomu, když ve firmě nakupujete nový hardware a cenu dojednáváte s přiděleným obchoďákem.

Ať už najdete e-shop s vojenským vybavením, drogami či jiným nelegálním obsahem, všechny tyto transakce mají několik společných znaků. Rozhodně se jedná o nelegální činnost, za kterou si můžete nemalou chvíli posedět v chládku, ale také se jedná o obchod s nejasným výsledkem. Obě strany, nakupující

i prodávající, vystupují anonymně, cokoliv, co si objednáte nebo dojednáte, se může a nemusí uskutečnit. Dále stojí za zmínku, že nemalé procento podobných obchodů je provozováno vládními složkami z různých států s cílem bojovat proti rozšiřování, nejen, kyberzločinu.

Z pohledu hackerů, ať už etických či neetických, je dark web velmi zajímavým místem. Je na něm dostupná široká škála nástrojů, návodů a materiálů, které mohou být běžně skryté. Také se zde nachází fóra, kde jsou zveřejňované nové zranitelnosti a diskutované metody jejich zneužívání. Podobné portály se nachází také na clear webu, ale na jeho temné straně se setkáváme také s obchody, kde se prodávají ukradená data, přihlašovací údaje nebo třeba i přístupy skrze vystavěná zadní vrátka do úspěšně napadených systémů. Nejen pro hackery, ale také pro bezpečáky jsou tato fóra a obchody zajímavé. Existují metody a nástroje kontinuálního monitoringu takovýchto stránek, s cílem upozornění administrátorů, že například právě jejich systém byl úspěšně hacknut a přístupy se prodávají na dark web e-shopu za zlomek bitcoinu.

Velkou částí obsahu na temném webu je bohužel také nelegální pornografie. Dále záběry či objednání

různých forem násilí. Rozhodně není mým cílem kohokoliv k podobným činnostem navádět, ale myslím si, že stojí za zmínku. Minimálně proto, abychom se na svět nekoukali skrze růžové brýle. Uvědomit si, že stejně jako existují kriminální skupiny v reálném světě, existují a působí „kyberkriminální“ skupiny v tom digitálním.

Jak je možné, že funguje? Proč ho vlády nevypnou?

Stránky na dark webu jsou dostupné skrze adresu, která se standardně skládá z dlouhého řetězce znaků i číslic následovaného koncovkou *.onion*. Ano, cibule, za chvíli se dostaneme k tomu, proč zrovna cibule. Je to alternativa k dalším doménovým koncovkám, které běžně potkáváte, jako *.com, .eu, .cz, .org* a tak dále. Pokud se pokusíte nějakou *.onion* stránku otevřít z klasického prohlížeče ve svém běžném prostředí, tak to nepůjde. Potřebujete se nejdřív připojit k TOR síti, což je zkratka pro „The Onion Router“. A zase ta cibule, pojďme si tedy vysvětlit tuto analogii.

Pokud jste někdy krájeli cibuli, tak víte, že se skládá z množství vrstev. Uvažujme nyní o každé z těchto vrstev jako o počítači či routeru. Když přistoupíte k nějaké stránce na dark webu, tak je váš požadavek směrován přes několik náhodně vybraných vrstev cibule, než se dostane k cílovému webovému serveru. Při přechodu do nové vrstvy je požadavek šifrován a vrstva neuchovává teoreticky žádné informace o tom, odkud požadavek přišel nebo co obsahuje. Jakmile požadavek doletí skrze celou cibuli k cílovému serveru, ten odešle odpověď ve formě zobrazitelné webové stránky skrze jinou cestu napříč vrstvami cibule. Tento složitý mechanismus zajišťuje, že informace o původním či cílovém počítači jsou prakticky nedohledatelné.

Jedna věc nám však může vrtat hlavou, když se nad principem fungování TOR sítě blíže zamyslíme. Vícevrstvá architektura nám sice zajišťuje jistou míru anonymizace, ale vstupní bod dark webu může lehce zjistit, odkud reálně přicházíme. Stejně tak výstupní bod cibule může relativně jednoduše zjistit, kde se cílový webový server nachází. Tento systém je komplexní a dokáže nám pomoci chránit si naše soukromí na internetu, ale musíme tomu také přispět my sami. Jak? O tom se budeme bavit v následující podkapitole.

Pokud se mi podařilo vám srozumitelně popsat fungování TOR sítě, tak nyní víte, že se jedná o nástroj, který nám nabízí možnost surfovat internetem anonymně. Je to možné také díky tomu, že je celý tento projekt řízen komunitně, nejedná se o komerční projekt. Je decentralizovaný. Každý uzel TORu, každá vrstva cibule je počítač, který někdo připojil s cílem rozšiřovat a budovat tuto síť. Tohle je také má odpověď na jednu z počátečních otázek – když má tolik nelegálního obsahu, proč ho vlády nevypnou? Nemohou, jelikož není pod jejich kontrolou. Moc rád na různých školeních používám jednu analogii s klasickým autem. Tato analogie je obecně aplikovatelná na všechny principy hackování. Automobil je pouze nástroj a je pouze na každém řidiči, jak jej bude používat. Jestli bude dojíždět z bodu A do bodu B, nebo jestli bude vjíždět na chodník a přejíždět lidi. Stejně jako v dnešní době nemůžeme zakázat používání aut, nemůžeme v digitálním světě zakázat používání legitimních nástrojů. To, že tyto nástroje jsou používány k nelegitimním účelům, je záležitost úplně jiná.

Kdy už brouzdat, tak hlavně bezpečně

Otevřít dark web a začít v něm hledat není nic obtížného. Je to dokonce tak jednoduché, že běžnému uživateli stačí nainstalovat jeden specializovaný prohlížeč, který jej připojí k TOR síti a dá mu možnost vyhledávat. Je to nejjednodušší, ale nejméně bezpečné řešení. Již víme, že webové stránky mohou obsahovat škodlivý kód, který se spouští v našem prohlížeči – JavaScript. Je vhodné upravit si nastavení TOR prohlížeče tak, aby zakazoval spouštění takového kódu. Stránky na dark webu jej stejně běžně nepoužívají, jedná se většinou o jednoduché stránky. Také kvůli tomu, že s množstvím nasazených anonymizačních opatření klesá rychlost načítání dark web stránek. Je naprosto normální, že tyto stránky nereflektují moderní standardy uživatelských rozhraní, zde se jedná hlavně o obsah.

Webové stránky dokáží zjistit mnoho zajímavých informací o vašem operačním systému i použitém hardwaru. Jako je jeho typ a verze systému, rozlišení použité obrazovky a mnoho dalšího. Sám nikdy nepřistupuji k dark webu z počítače, který používám pro běžnou činnost. Místo toho využívám operační systémy, které lze využívat přímo z USB Flash disku. Jejich

obrovskou výhodou je, že si neukládají uživatelská data a po každém vypnutí a zapnutí jsou ve výchozím režimu. Navíc skrze TOR síť směřují nejen webový, ale veškerý síťový provoz. Jedná se o velmi dobré opatření pro zajištění bezpečnosti a anonymity při brouzdání dark webem.

Pokud jste technologický nadšenec stejně jako já, určitě vám padne do okna systém, který byl vytvořen pro uživatelskou bezpečnost i anonymitu a zároveň nabízí možnost fungovat jako klasický operační systém. Nechci zde jmenovat konkrétní produkty, ale existují operační systémy, které rozdělují svůj disk do několika operačních domén, které jsou logicky oddělené. Ano, tato varianta již vyžaduje určitou dávku zkušeností s linuxovými systémy, ale rozhodně vás nebude nudit.

Dalším velmi dobrým a jednoduše implementovatelným opatřením je použití VPNky. O těch již v této knize byla řeč. Hlavní dvě funkcionality VPN spojení jsou zpřístupnění zdrojů jiné sítě, čímž se zamaskuje aktuální poloha, a přidání další vrstvy šifrování, která chrání důvěrnost i jinak nezabezpečené komunikace. S ohledem na připojování se k nezabezpečeným kanálům nás dosud zajímala právě funkcionalita dodatečné vrstvy šifrování. Asi již tušíte, že

v případě ochrany identity nás zajímá v prvé řadě ono maskování polohy. VPN sítě nám dokáží jednoduše poskytnout maskování reálné polohy, ale je nutné si uvědomit, že opět vkládáme důvěru v onoho poskytovatele VPN spojení.

Ať už používáte jakékoliv bezpečnostní opatření, které vám pomůže chránit vaši aktivitu a soukromí i na temnějších částech internetu, berte v úvahu, že žádné z nich není stoprocentní. Opět je vždy nutné se kriticky zamýšlet nad tím, jaké stránky chci navštívit, jaký je jejich obsah, kam a jaké zadávám své osobní údaje. Dark web je velmi zajímavé, ale také nebezpečné místo, kde se chyby neodpouští a neznalost neomlouvá.

IX. Internet je dobrý sluha, ale zlý pán

Síť je divoké místo. Obsahuje miliardy uživatelů a ještě více zařízení. Ne každý je hodný a je pravdou, že se zde nalézá spousta individuí, která sledují pouze své vlastní zájmy a neváhají porušovat zákony a etiku, aby svých cílů dosáhla. Počítače s internetem se staly natolik důležitou součástí našich životů, že je již nemyslitelné se od nich oprostit. Ani by to nemělo být naším cílem, jelikož žijeme v informačním věku a přístup k informacím je pro nás zásadní. Velmi nám usnadňuje vzdělávání, práci a komunikaci. Měli bychom se učit na internetu správně chovat a bezpečně jej využívat.

Stejně jako v realitě si hlídáme své klíče od domu, měli bychom si chránit hesla od svých účtů. Stejně jako se rozhlížíme při přecházení silnice, měli bychom se zamýšlet, jaké stránky a služby na síti navštěvujeme. Stejně jako při konverzaci s ostatními lidmi při osobních setkáních, i na internetu bychom si měli dávat pozor na to, komu a jaké informace sdělujeme prostřednictvím e-mailů či sociálních sítí. A v neposlední řadě, stejně jako

ochraňujeme své blízké ve fyzickém světě, měli bychom dbát na jejich ochranu i v tom digitálním. Jedním z účinných opatřeních je společně o tématech nástrah na internetu mluvit. Šířit všeobecné povědomí o kyberbezpečnosti i mezi lidi, kteří k počítačům nemají blízko, přesto moderní technologie využívají. Aniž si to mnohdy uvědomují, i oni se mohou stát obětí kyberútoku.

Osobně si myslím, že by vysvětlování principů bezpečnosti mělo být samozřejmost již od prvních chvílí, kdy počítače začínáme používat. Setkal jsem se s mnoha případy, kdy malé děti ještě neumí psát ani číst, ale ovládat tablet či telefon jim nedělá žádný problém. Opět může nastat scénář, kdy omylem infikují ono zařízení nějakým malwarem. V případě, že stejné zařízení používají rodiče ke svým běžným činnostem, může být úspěšně napadeno. Jaké důsledky mohou nastat, to víme z předešlých kapitol. V tomto konkrétním případě by byla vina na straně rodičů, jelikož nedokázali své zařízení vhodně zabezpečit.

Vrátím se ale zpátky k dětem. Dřív nebo později nastane moment, kdy budou schopné používat počítače i k jiným účelům než jen k zábavě, například k plnění domácích úkolů. To zahrnuje většinou vyhledávání na

internetu a vytváření dokumentů. Tohle je moment, kdy je podle mého názoru ideální čas začít mimo jiné také s učením se bezpečného využívání sítě. Nejsem pedagog a nehodlám si na něj ani hrát. Je ale to můj názor a upřímné přání, jelikož pak budou mladí lidé opouštět základní školy s širokými znalostmi o informačním světě a budou se stávat mladými technickými experty. Vnímám toto jako nezastavitelný trend, kterému můžeme přispět tak, že budeme všichni diskutovat a řešit témata bezpečnosti. Koneckonců, bezpečnost je povinností a odpovědností nás všech.

Možná je to ale pouze utopie, nebo ne?

Hacking je cool, chci vědět více!

Jelikož jste dočetli až sem, troufám si hádat, že vás témata ze světa hackingu a informační bezpečnosti zaujala. Tato kniha si kladla za cíl jednoduchým a srozumitelným způsobem šířit povědomí o hrozbách a nástrahách na internetu, bez zacházení do přílišných technických detailů. Jestli chcete vědět více, není nic jednoduššího než začít vlastní průzkum internetu, objevovat zajímavé blogy, lidi, videa, přednášky či záznamy z různých konferencí.

Můžete si dokonce vyzkoušet hackování na vlastní kůži! Nebudu jmenovat, ale existuje řada online výukových platforem, kde si v simulovaném prostředí můžete vyzkoušet provádět reálné útoky na připravené cíle. Mnoho z nich praktikuje učení hrou, kdy je cílem získat vlajku ukrytou uvnitř systému a tím pádem dokázat jeho úspěšné napadení. Často podobné platformy bývají dostupné zdarma, a proto vám nic nebrání nabírat zkušenosti a třeba se stát i velmi úspěšným hackerem či hackerkou.

O autorovi

Marek Kovalčík je odborníkem v oblasti kybernetické bezpečnosti, hackování a penetračního testování. Podílel a podílí se na zakázkách pro klienty ze soukromého sektoru i pro veřejné subjekty různých velikostí, jak v České republice, tak i v zahraničí. Po absolvování studia informačních technologií na Vysokém učení technickém v Brně rozšířil své znalosti studiem risk managementu na Ústavu soudního inženýrství, čímž získal komplexní pohled na technologické a právní aspekty digitální sféry.

Ve svých kariérních začátcích se věnoval programování, ale brzy ho zlákaly oblasti s širším záběrem, jako jsou operační a informační systémy, počítačové sítě a komunikace, se zvláštním důrazem na jejich bezpečnostní aspekty.

Marek je držitelem několika prestižních certifikací, včetně CISSP (*Certified Information Systems Security Professional*) a CEH (*Certified Ethical Hacker),* což dokládá jeho odbornost a závazek k budování bezpečnosti informačních systémů.

Literatura

[1] Ur, Blase & Noma, Fumiko & Bees, Jonathan & Segreti, Sean & Shay, Richard & Bauer, Lujo & Christin, Nicolas & Cranor, Lorrie. (2015). "I added '!' at the end to make it secure": Observing password creation in the lab.

[2] Hussain, Tehreem & Atta, Kiran & Bawany, Narmeen & Qamar, Tehreem. (2018). Passwords and User Behavior. Journal of Computers. 13. 10.17706/jcp.13.6.692-704.

NÁSTRAHY INTERNETU

aneb. informační (ne) nebezpečnost

Když se řekne "hacker", mnoho z nás si hned představí chlápka v černé mikině s kapucí v tmavé místnosti, který shrbený velmi rychlé píše na klávesnici. Po chvíli se na jedné z jeho obrazovek objeví zelený nápis "přístup povolen". Okamžitě získá bez povšimnutí přístup i do těch nejstřeženějších částí sítě a má k dispozici ty nejtajnější dokumenty.

Přestože v realitě by podobný přímý útok na chráněné systémy vyžadoval čas a nemalou dávku zkušeností a kreativity, nejedná se o sci-fi. Hrozby na internetu jsou reálné a jsou všude okolo nás.

Vydal:

Marek Kovalčík
www.nastrahy-internetu.cz