Univerzita Pardubice
Fakulta ekonomicko-správní

Etický hacking a bezpečnost

Bakalářská práce

2021 František Bartoš

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**František Bartoš**
Osobní číslo:	**E17637**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Téma práce:	**Etický hacking a bezpečnost**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je zpracovat několik případových studií pro zabezpečení proti různým formám etického hackingu s hodnocením možných dopadů na vybraný subjekt.

Osnova:
- prostudování zdrojů a zdokumentovaných případů etického hackingu
- zpracování případových studií pro vybraný subjekt
- zhodnocení možných dopadů

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

SCAMBRAY, Joel a Mike SHEMA. Hacking bez tajemství: Webové aplikace. Brno: Computer Press, 2003. ISBN 978-80-7226-769-9.
SIMPSON, Michael T., Kent BACKMAN a James E. CORLEY. Hands-on ethical hacking and network defense. Boston, MA: Course Technology, 2016. ISBN 978-13-0548-068-1.
SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.
ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2020**
Termín odevzdání bakalářské práce: **30. dubna 2021**

LS.

prof. Ing. Jan Stejskal, Ph.D. v. r.

prof. Ing. Jan Stejskal, Ph.D.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v. r.

RNDr. Ing. Oldřich Horák, Ph.D.
vedoucí ústavu

V Pardubicích dne 1. září 2020

Prohlašuji:

Práci s názvem Etický hacking a bezpečnost jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 14. 5. 2021

František Bartoš v. r.

PODĚKOVÁNÍ

Tímto bych rád poděkoval svému vedoucímu práce RNDr. Ing. Oldřichu Horákovi, Ph.D. Zejména za jeho čas a trpělivost, cenné rady, odbornou pomoc a připomínky, které mi pomohly při tvorbě mé bakalářské práce.

ANOTACE

Práce se zaměřuje na etický hacking a potenciál, který v oblasti kybernetické bezpečnosti má. Práce má demonostrovat, jaké hrozby podnikům hrozí, jak se jim lze ubránit a jakou roli v tomto procesu hraje etický hacking a sociální inženýrství. Aby bylo možné tohoto cíle dosáhnout, byly vytvořeny tři případové studie. Ty se soustředí na fiktivní podniky, které operují na jiných trzích a zpracovávají jiná data. Právě jejich rozdílné zaměření však jasně ukazuje na skutečnost, že etický hacking a pochopení sociálního inženýrství má potenciál ve všech oblastech a všech podnicích.

KLÍČOVÁ SLOVA

etický hacking, hacking, bezpečnost, sociální inženýrství

TITLE

Ethical hacking and security

ANNOTATION

This bachelor thesis focuses on ethical hacking and the potential it has in the field of cybersecurity. The thesis demonstrate which threats companies face, how they can be defended, and what role ethical hacking and social engineering play in this process. To achieve this goal, three case studies have been developed. These case studies focus on fictitious companies that operate in different markets and process various types of data. However, it is their differences that clearly indicate the fact that ethical hacking and understanding of social engineering has potential in all areas and in all companies.

KEYWORDS

ethical hacking, hacking, security, social engineering

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

ACL	Access Control List
API	Application Programming Interface
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
AT&T	American Telephone and Telegraph
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name System
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology / Informační technologie
IPS	Intrusion Prevention Systems
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HTML	Hypertext Markup Language
MITM	Man in the Middle
NIDS	Network-Based Intrusion Detection System
NIPS	Network-Based Intrusion Prevention System
PING	Packet InterNet Groper
RIPE	Réseaux IP Européens
SMS	Short Message Service
VPN	Virtual Private Network
WHOIS	Who Is

ÚVOD

Dynamický vývoj a rozšiřování informačních technologií spolu s růstem jejich využívání je signifikantním aspektem dnešní doby. Tyto faktory také způsobují, že informace nabývají na hodnotě a jejich únik představuje velkou hrozbu. Zároveň vystavuje vlastníka těchto dat řadě bezpečnostních rizik. Horálek a kol. (2017) hovoří o tom, jak i nepatrná chyba v algoritmu dokáže umožnit útočníkovi napadnout systém, získat data či šířit danou chybu po síti. Právě tato rizika jsou důvodem, proč je kladen důraz na kryptografii, proč je nezbytné mít spolehlivý šifrovací systém a proč je důležité vyvíjet stále nové a lepší algoritmy, které počítače a sítě ochrání.

Chyby v systémech však nejsou to jediné, co ohrožuje data, které podniky zpracovávají. Klíčový je lidský faktor, který svým jednáním může způsobit selhání nástrojů, která data chrání. K této chybě může dojít jak v online, tak v offline prostředí. Právě na to offline prostředí pamatuje prostřednictvím sociálního inženýrství, jelikož s ním spojené útoky stojí na selhání lidského faktoru.

Tato bakalářská práce se soustředí na etický hacking a přínos, který podnikům nabízí. Cílem práce je na příkladu tří případových studií demonstrovat, jaké hrozby podnikům hrozí, jak se jim lze ubránit a jakou roli v tomto procesu hraje etický hacking a sociální inženýrství. Práce nejprve definuje, co je hacking, jaké druhy útoků existují a jak se před nimi lze bránit. Zmíněna je kybernalita a legislativa, která se touto trestnou činností zabývá. Kapitola práce zaměřená na metodologii seznamuje čtenáře s tím, co je to případová studie a jaké parametry byly definovány pro tuto práci. Na tuto kapitolu navazují samotné případové studie, které byly vytvořeny pro e-shop, jazykovou školu a psychologickou poradnu. Všechny tyto podniky operují na jiných trzích, zpracovávají jiná data a v jiném rozsahu. Jejich rozdílné zaměření však jasně ukazuje na to, že etický hacking a pochopení sociálního inženýrství má potenciál ve všech oblastech a všech podnicích.

1 HACKING, DRUHY ÚTOKŮ A OCHRANA PŘED NIMI

Tato kapitola se věnuje otázce etického hackingu. Nejprve jsou představeny relevantní základní pojmy a poté platformy pro útok. Kapitola popisuje jednotlivé druhy útoků, a to jak pasivní, tak aktivní.

1.1 Základní pojmy

Kovalčík (2020) definuje hacking jako *„neautorizovaný přístup k počítačům, sítím, emailům či jiným zařízením za účelem získat či měnit data, ke kterým nemá mít daný člověk přístup“*. Hackování je tedy nelegální aktivita, za jejíž provozování může v některých případech pachatel skončit ve vězení. A právě aktivity těchto hackerů daly vzniknout tzv. etickým hackerům. Ti *„používají naprosto stejné metody a nástroje jako klasičtí a s povolením majitele systému se snaží odhalit bezpečnostní chyby, které by mohly být zneužity k infiltraci jeho systému“* (Kovalčík, 2020).

Hacking

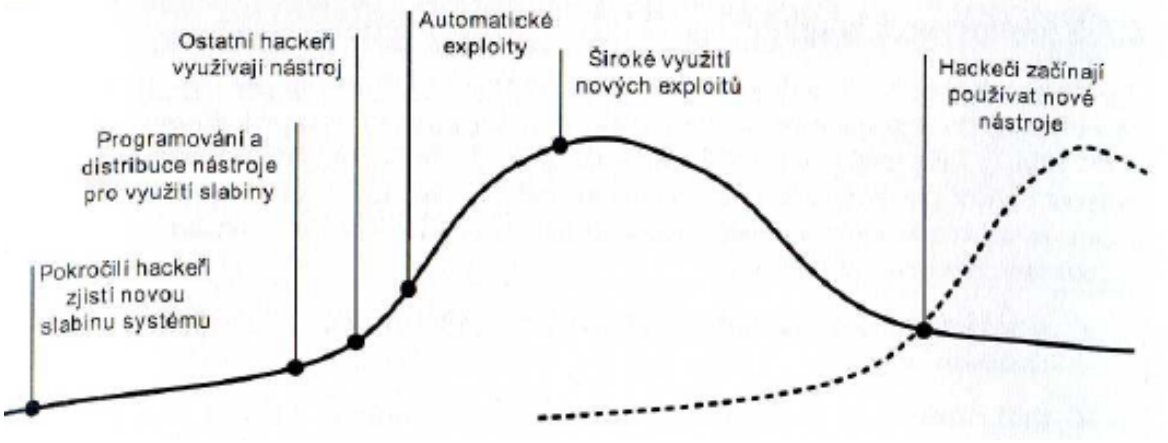
Termíny „hacker“ a „hacking“ vznikly přibližně v padesátých letech minulého století. Tehdy jím byl označen *„šikovný, technicky nadaný jedinec, schopný hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače“* (Jirovský, 2007, s. 47). To, jak je hacking znám dnes, se však do povědomí dostalo až přelomem šedesátých a sedmdesátých let. Tehdy technologičtí nadšenci využili nedokonalosti telefonní sítě, aby uskutečňovali nezpoplatněné dálkové telefonní hovory. Jedním z nich byl John Draper, známý jako „Captian Crunch“. K prvním hackerským pokusům o útok došlo v dálkové komunikační síti firmy AT&T skupinou hackerů označovanou jako „phreakers“.

Jinou definici hackera přináší Jargon File: The New Hackers Dictionary, který hackera chápe jako člověka, *„kterého baví zkoumat detaily programovatelných systémů a hledat metody, jak je vylepšit“* (Jirovský, 2007). Tato definice se výrazně liší od té, kterou přinesl Kovalčík.

Hackeři pro své aktivity využívají různé technologie, které lze dělit na:

- *„hardwarové nástroje, kam patří např. techniky hledání bezpečnostních děr v čipových kartách,*
- *softwarové neboli programové nástroje, které v hackerské komunitě převažují,*
- *sociální inženýrství neboli techniky zneužití lidského elementu“* (Jirovský, 2007, s. 59).

Vývoj hackerských nástrojů kopíruje vývoj softwarů, rovněž je ovlivňován novými bezpečnostními politikami, které začínají vstupovat v platnost. Obecně platí, že exploit, tedy program pro využití slabin daného systému, nemá dlouhou životnost. Životní cyklus zachycuje Obrázek 1.



Obrázek 1: Životní cyklus exploitu

Zdroj: Jirovský, 2007

1.2 Platformy pro útok

Základem každého moderního počítače je jeho operační systém. Ten zajišťuje komunikaci mezi hardwarovým rozhraním a uživatelem. Před nástupem operačních systému, které se začaly rozvíjet na počátku 60. let, musel programátor s počítačem komunikovat pomocí nul a jedniček (Janák, 2002). V následujících podkapitolách budou popsány základní informace o Windows, Linux a MacOS.

1.2.1 Windows

MS-DOS byl prvním operačním systémem, který společnost Microsoft vyvinula pro osobní počítače IBM. MS-DOS i IBM počítače byly uvedeny na trh v roce 1981. Systém měl však celou řadu nedostatků, které se pokusila odstranit verze Windows 2.0 představena v prosinci 1987 (Janák, 2002). Dnes jsou uživatelům k dispozici Windows 10.

Windows 10 má v současnosti již ve svém základu kompletní sadu funkcí pro zabezpečení zařízení. Obsahuje antivirus, firewall, ochranu proti ransomwaru a internetové funkce (Microsoft, n.d.). Alzahrani a kol. (2017) připomínají, že Windows se stává častým cílem pro různé ransomware útoky. Často dochází k tomu, že hackeři přepíšou nebo smažou originální soubory používané Windows API nebo Windows Secure Delection API.

1.2.2 Linux

Linux je rovněž operačním systémem, jehož licence však dovoluje uživatelům Linux i jeho software kopírovat dalším osobám. Linux je zároveň k dostání zdarma a vývojářům poskytuje zdrojové kódy programů, které mohou následně rozvíjet. Linux Expres (n.d.) definuje Linux jako *„jádro operačního systému, které spolu s ostatními programy tvoří operační systém“*.

Linux nabízí celou řadu aplikací, které jsou pro uživatele zdarma a v plné verzi. Systém je navržen tak, aby se do něj nikdo nepovolaný nemohl dostat. Disponuje antivirovými programy a firewall, přičemž poskytuje aktualizace systému zdarma a včas (Linux, n.d.).

1.2.3 MacOS

Firma Apple přišla s operačním systémem iOS, který je k dispozici pro zařízení iPhone a iPad, a také s macOS, tedy operačním systémem pro macbooky. Ten historicky existoval pod jménem Mac OS X a vyznačuje se svou intuitivností. Jeho ovládání si uživatel může usnadnit např. za pomoci jednoduchých gest. Jeho další výhodou je stabilita a velké množství programů či aplikací, které jsou s macOS kompatibilní (iWant, n.d.).

Macbooky se v poslední době stávají stále častěji vyhledávaným terčem hackerů. Často rozšířeným omylem byl předpoklad, že operační systém macOS je před viry a nebezpečnými kódy automaticky kompletně chráněn (Jelič, 2021).

1.3 Druhy útoků

Tato kapitola se bude věnovat jednotlivým útokům, a to jak aktivním, tak pasivním. Poslední podkapitola bude věnována malwaru. Běžný postup útočníka zachycuje Tabulka 1.

Tabulka 1: Postup útoku

Krok	Popis	Příklady
Průzkum	Aktivní nebo pasivní sběr informací o síti.	Odposlech síťového provozu, odposlechy obecně (pasivní), prohledání databází ARIN a WHOIS, průzkum HTML kódu webových stránek firmy, sociální útoky (aktivní).
Skenování	Nalezení systémů a služeb, které na nich běží.	Hromadný ping, skenování portů.
Získání přístupu	Zneužití nějaké známé bezpečnostní díry k získání přístupu do systému.	Zneužití přetečením bufferu nebo uhodnutí hesla hrubou silou.
Udržení přístupu	Nahrání softwaru, který se postará o útočníkův budoucí přístup k počítači.	Instalace zadních vrátek.
Zametání stop	Zamaskování činnosti, kterou útočník v systému provádí.	Smazání nebo úprava dat v systémovém protokolu a aplikačních protokolech.

Zdroj: Harris a kol., 2008

1.3.1 Pasivní útoky

Mezi pasivní patří odposlech a skenování portů. Všechny tyto varianty budou na následujících řádcích představeny.

Odposlech sítě

Harris a kol (2008, s. 131) definují programy pro odposlech sítě jako programy, které *„umí z nějakého síťového média zachytit síťové rámce“*. Autoři upozorňují na fakt, že programy pro odposlech sítě mají různé podoby. Některé mohou být jednoduché řádkové programy, jiné jsou grafické aplikace disponující vzdálenou správou a podporou databází.

Mezi programy, které umožňují odposlech síťové komunikace patří unixové knihovny libpcap a WinPcap (port pro Windows).

Skenování portů

Skenování portů odesílá pakety na cílový server s cílem identifikace spuštěných služeb. Při tomto skenování se zjišťuje, zda služby na portech „naslouchají“. Právě identifikace portů je stěžejní pro zjištění zranitelnosti systému (Plašil, 2015), jelikož hacker v danou chvíli zjistí, na kterých IP adresách jsou funkční systémy dostupné z internetu. Právě kvůli tomu, že hacker zjistí, přes kterou službu daný port běží, může cíleně nasměrovat útok (Scambray a kol., 2003).

1.3.2 Aktivní útoky

Mezi aktivní patří modifikace dat, spoofing, phising, pharming, replay attak, Man in the Middle (MITM), DoS, DDoS, brute force a rainbow tables.

Spoofing a phishing

Pojmem spoofing se označují všechny způsoby, kterými dochází k falšování identity (Management Mania, 2015). Spoofing e-mailů znamená, že osoba, která daný e-mail odesílá, předstírá, že je někým jiným. K vytvoření těchto falešných zpráv dochází za pomoci nepravých záhlaví, které disponují nepravdivými směrovacími informacemi. Právě falešné adresy jsou klasickým námětem při phishingu. Phishing je podvodná technika, jejímž cílem je získat informace. Často se jedná např. o údaje z kreditních karet (McCarthy a Weldon-Siviy, 2013). Tyto podvodné e-maily však dokážou také např. nainstalovat malware do počítače (Kaspersky, n.d.).

Pharming

Pharming je kombinací slov „phishing“ a „farming“. Jedná se o techniku podobnou phishingu, kdy dochází k manipulaci s provozem webových stránek a ke krádeži důvěrných informací. Pharming stojí na využívání základu fungování internetového prohlížení – posloupnost písmen, která tvoří internetovou adresu, musí být převedena na IP adresu serverem DNS, aby bylo možné s připojením pokračovat. Právě to se stává předmětem útoku (Kaspersky, n.d.).

Replay attack

V tomto případě se jedná o situaci, kdy hacker zachytí zabezpečovanou síťovou komunikaci, kterou podvodně zpozdí nebo znovu odešle tak, aby odesílatel udělal to, co chce hacker. Nebezpečí je o to vyšší, že hacker nepotřebuje pokročilé dovednosti pro dešifrování zprávy poté, co ji ze sítě zachytil (Kaspersky, n.d.).

Man in the Middle

V obvyklém scénáři Man in the Middle útoku vystupuje hacker jako třetí strana komunikace mezi klientem a serverem. Jinými slovy hacker tuto komunikaci zachytí a zneužije (Nayak a Samaddar, 2010). Cílem útoku je snaha získat informace o kreditních kartách, přihlášení apod. Proto jsou častým cílem klienti finančních aplikací a webové stránky, u kterých je vyžadováno přihlášení (Mallik, 2018).

DoS a DDoS

Zkratka DoS znamená „Denial of Service“, tedy potlačení služby. Podstatou těchto útoků je snaha zaútočit na spojovací cesty v případě, že hacker není schopen zaútočit na cílový stroj.

Mezi metody, které lze pro DoS využít, patří zahlcení příkazu ping do sítě cílového stroje, zahlcení volných systémových prostředků a také DDoS – zahlcení odesíláním jalových paketů z více strojů, tedy „Distributed Denial of Service“. V tomto případě hacker kompromituje dostatečné množství strojů, aby díky složení jejich přenosových kapacit převýšil přenosovou kapacitu kanálu, kterým je daný cílový stroj připojen. Z kompromitovaných strojů následně začne odesílat pakety na IP adresu cíle, čímž zahltí přístupový kanál, který se stane nepoužitelným (Jirovský, 2007).

Brute force

Brute force stojí na metodě pokus-omyl, kdy se útočník snaží uhodnout přihlašovací údaje, šifrovací údaje nebo najít skryté webové stránky. Hackeři využívají různé kombinace ve snaze uhodnout tu správnou. Tyto útoky se nazývají „brute force“ právě proto, že vynakládají nadměrné množství energie ve snaze vynutit si cestu do daného soukromého účtu. Tyto útoky se stávají stále populárnějšími (Kaspersky, n.d.).

Rainbow tables

Rainbow tables se využívají pro rozbití otisku hesla s cílem toto heslo zjistit. Pokud má hacker přístup k databázi hesel, která jsou uložena v hash formě, může tento typ útoku využít (Horálek a kol., 2017). Rainbow tables útoky se snaží šifrovat hesla před jejich přidáním do databáze, což umožňuje rychlejší rozbití hesel než například brute force metoda. Útok funguje tak, že zatímco dochází k zašifrování hesel pomocí klíčů, hackeři odpovídají funkcím, které jsou k ochraně daných hesel používány. Toto nebezpečí nastane v momentě, kdy hacker identifikuje, jaká „rainbow table“ je využívaná pro šifrování hesel uložených v dané databázi. Tu lze využít k prolomení všech uložených hesel (Techslang, n.d.).

1.3.3 Malware

Malware je *„programový kód vyvinutý k tomu, aby poškodil počítač nebo data v něm“* (McCarthy a Weldon-Siviy, 2013, s. 32). Tato podkapitola popisuje exploit kit, adware, backdoor, dialer, keylogger, ransomware, scareware, hoax, spyware, trojský kůň, virus, červ, spam a rootkit.

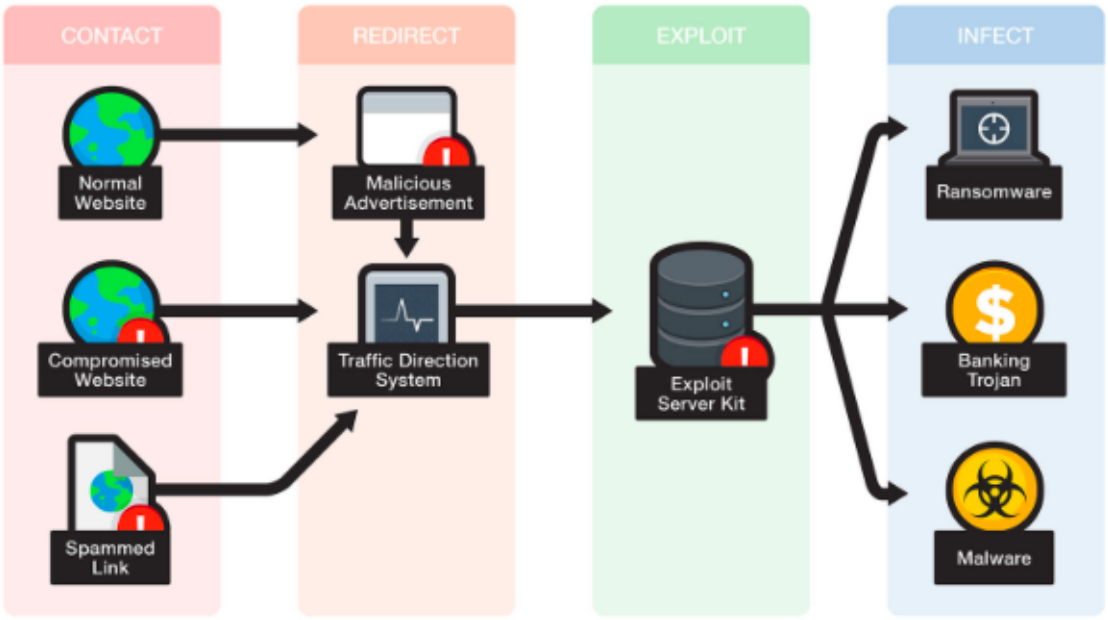
Adware

Adware může být *„buď legální komerční program, nebo je to malware, který přistane v systémech uživatelů bez jejich vědomí, nebo bez skutečně informovaného souhlasu“* (McCarthy a Weldon-Siviy, 2013, s. 65). Adware dodává do webového prohlížeče reklamu, proto ho inzerenti využívají k tomu, aby mohli takříkajíc behaviorálně zacílit. Jinými slovy, adware je *„program, který uživatelům poskytuje cílený reklamní obsah, často tak, že v počítači*

shromažďuje informace o tom, co uživatel na síti dělá, a které stránky navštěvuje“ (McCarthy a Weldon-Siviy, 2013, s. 65). Problém nastává ve chvíli, kdy uživatel s jeho fungováním nedal souhlas a do počítače se dostal bez jeho vědomí.

Exploit kits

Exploit kits se využívají pro útok na zranitelná místa v systémech, což umožňuje hackerům provádět škodlivé činnosti či infikaci malwarem. Exploit kits jsou vybaveny exploity, které umožňují zacílit na běžně nainstalované softwary, mezi které patří Adobe Flash, Java nebo Microsoft Silverlight. Exploit kits obvykle obsahují kontakt pro správu, což hackerům útok usnadňuje (Trend Micro, n.d.). Obrázek 2 zachycuje fáze tohoto útoku.



Obrázek 2: Exploit kit - fáze útoku

Zdroj: Trend Micro, n.d.

Backdoors

Backdoors, tedy zadní vrátka, představují *„kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení“* (Jirovský, 2007, s. 63). Tento způsob je mezi hackery velice oblíbený, proto se snaží o instalaci backdoors, jakmile objeví bezpečnostní díru. Takto napadené počítače umožňují útok na další stroje a zároveň kryjí hackera před odhalením. Pokud jsou backdoors vytvořena kvalitně, je velice těžké je odhalit, zvlášť v případě, že je hacker často nevyužívá.

Keylogger

Keylogger se rovná odposlechu klávesnice a bývá součástí adwarových a spywarových programů. Tento program zaznamenává každý úhoz klávesy, ke kterému při psaní na počítači dochází. Zaznamenává tedy citlivé údaje, např. uživatelské jméno a heslo pro přístup do internetového bankovnictví, čísla platebních karet, rodné číslo apod. Za zmínku stojí rovněž fakt, že tyto programy jsou prodávány rodičům ke sledování aktivit jejich dětí (McCarthy a Weldon-Siviy, 2013).

Ransomware

Ransomware je taková *„forma malwaru, při které jsou soubory na počítači uživatele zašifrovány nebo je systém (či mobilní zařízení připojené na Internet) vyřazen z provozu, dokud není zaplaceno výkupné“* (McCarthy a Weldon-Siviy, 2013, s. 74). Nejčastější formou je nástavba falešného bezpečnostního programu. V takovém případě si uživatel nainstaluje malware v reakci na nepravdivou zprávu o spywaru nebo viru.

Scareware

Scareware je falešným antivirovým programem. Takováto aplikace *„používá neetické marketingové praktiky k tomu, aby uživatele svedla k zaplacení a stažení bezcenného nebo škodlivého programu maskujícího se jako bezpečnostní počítačový program“* (McCarthy a Weldon-Siviy, 2013, s. 70). Nejčastěji se opět jedná o falešnou poplašnou zprávu, že počítač byl napaden spywarem. Tato zpráva bývá velice věrohodná, často s logem bezpečnostního programu, který má uživatel na svém počítači nainstalovaný.

Spyware

Spyware je zlehka odlišný případ, jelikož některé společnosti prodávají takové programy legálně. Například programy rodičovské kontroly fungují na stejném principu, a uživatele prakticky špehují. To je podstata spywarů. Hackery využívané jsou programy instalované bez vědomí uživatelů, které spotřebovávají systémové zdroje, kradou důvěrné informace a ovlivňují výkon počítače. Spyware může také sledovat, jaké stránky uživatel napadeného počítače sleduje a co na nich dělá. V některých případech může také zahrnovat keyloggery (McCarthy a Weldon-Siviy, 2013).

Trojský kůň

Ve vztahu k počítačům má trojský kůň podobný cíl jako v řecké mytologii, odkud tento název pochází, tedy *„zakamuflovat se jako něco neškodného nebo žádoucího, poté otevřít dveře a pustit dovnitř útočníky“* (McCarthy a Weldon-Siviy, 2013, s. 52). Klíčové tedy je, aby se trojský kůň vydával za něco lákavého, co upoutá uživatelovu pozornost.

Poté nechává „zadní vrátka“, což mu umožňuje snadný návrat s cílem ovládat napadený počítač, procházet jeho soubory a získávat důvěrná data. V některých případech může být napadený počítač za pomoci trojského koně využit k útoku na někoho dalšího.

Virus

McCarthy a Weldon-Siviy (2013, s. 41) definují virus jako *„sadu počítačových pokynů, které se samy replikují“*. Může se jednat o úplný program nebo část kódu. Pro virus je typické, že vytváří své vlastní kopie, ovšem existuje jich celá řada. Některé z nich se šíří pouze za určitých okolností, jiné s sebou nesou náklad. To znamená, že cílem viru je způsobit škodu, např. vymazat soubory nebo zaútočit na jiné systémy. Virus je schopný zabrat veškerou dostupnou operační paměť zasaženého počítače, a to velice rychle.

Červ

Červ představuje *„malwarový program, který se v sítích sám kopíruje“* (McCarthy a Weldon-Siviy, 2013, s. 47). Je obvykle samostatným programem, který se sám přenáší mezi počítači v dané síti. Rozdíl mezi virem a červem je tedy v tom, že červ se *„kopíruje spíše na jiné počítače než do jiného souboru na stejném počítači“* (McCarthy a Weldon-Siviy, 2013, s. 47). Počítač může napadnout kvůli bezpečnostní chybě a proniknout do počítače z Internetu.

Spam

Spam představuje nechtěné e-mailové zprávy. McCarthy a Weldon-Siviy (2013) připomínají, že vysoké množství spamů se soustředí na výrobky, které jsou ilegální nebo se pohybují v šedé zóně. Některé spamy jsou protizákonné, jiné ne. Vymezení rozdílu je v tomto směru velice náročné. Shodným faktorem je to, že jsou obtěžující pro uživatele. Problematická je rovněž snaha o odhlášení zasílání těchto spamových zpráv. Aby toho uživatel docílil, musí buď navštívit webové stránky spammera, nebo mu zaslat e-mail. V tu chvíli spammer ví, že uživatelova e-mailová adresa je platná a zprávy na ni odchází. Pokud daný spammer postupuje dle zákona, zasílání ukončí. Pokud ne, prodá uživatelovu e-mailovou adresu.

Rootkity

Rootkity jsou techniky, které se využívají pro skrývání činností, které jsou prováděny na operačním systému. Jirovský (2007) připomíná, že se jedná o podmnožinu backdoors, proto je také jejich funkce velice podobná. Rozdíl spočívá v tom, že rootkity zůstávají po kompromitaci účtu stále v utajení. Jedná se o běžně užívané programy, které byly modifikovány, což hackerovi umožňuje mít neomezený přístup k zasaženému počítači a administrátor nic netuší.

1.4 Ochrana proti útokům

Tato podkapitola je věnována jednotlivým druhům ochrany proti útokům, které byly přiblíženy na předchozích stránkách. Zmíněn bude antivirus, firewall i IDS/IPS.

1.4.1 Metody ochrany

McCarthy a Weldon-Siviy (2013) připomínají, že pro bezpečnost na internetu je klíčový antivirus, antispyware, osobní firewall a bezpečnostní záplaty. Otázce antiviru a firewallu se budou věnovat následující podkapitoly.

Za zmínku však rovněž stojí možnosti přechodné ochrany. Mezi ně patří např. klepání na porty. Jedná se o defensivní techniku, která je ideální pro malý počet uživatelů. Harris a kol. (2008, s 382) popisují klepání na porty jako *„tajný síťový zámek“*, kdy *„port chráněné síťové služby je zavřený do té doby, dokud klient správným způsobem nezaklepe“*. Toto zaklepání je posloupností portů, *„na kterou se klient pokusí připojit ještě před připojením k samotné síťové službě“*. Tato technika pouze komplikuje přístup k chráněným síťovým službám, ale nezamezuje mu.

Další přechodnou ochranu představuje přechod na jiný software. To může být v některých případech nejrozumnější variantou, a jak připomíná Harris a kol. (2008), vždy je potřeba tuto možnost vzít do úvahy při reakci na bezpečnostní problémy. Tato varianta je však velice komplikovaná, jelikož nemusí být k dispozici alternativní aplikace nebo tento přechod může vyžadovat také změnu hostitelského operačního systému.

Jako poslední bude popsáno záplatování. Děravá aplikace se dá zabezpečit pouze jejím vypnutím či záplatováním. Záplata může být vytvořena buď výrobcem dané aplikace, nebo svépomocí. To je jednoduší v případě, že je k dispozici zdrojový kód, neboť ten je záplatován. Harris a kol. (2008) dodávají, že jednoduché záplatování není nutně také dobré. Při záplatování je také důležité sledovat, aby nezpůsobilo další chyby v programu.

1.4.2 Antivirus

Jak podotýká Genc a kol. (2021), většina uživatelů se dnes při ochraně svých počítačů spoléhá na antivirový software. Ve svých počátcích antivirové programy detekovaly a odstraňovaly viry ze zasaženého zařízení. Díky tomu zabránily dalšímu šíření škodlivého kódu. Dnešní antiviry disponují řadou bezpečnostních vrstev, které poskytují ochranu před celou řadou hrozeb. Právě tato vícevrstvá ochrana brání krádeži účtů a hesel, zašifrování souborů pomocí ransomwaru, krádeži citlivých osobních údajů, spamu, neoprávněné těžbě kryptoměn, podvodům a celé řadě dalších forem kybernetických útoků (ESET, n.d.).

Vohanková (2020) zmiňuje, že antivirus je *„nejdůležitějším prvkem v ochraně před viry“*, jelikož jim brání ve vstupu do počítače a zároveň je klíčový pro prevenci. Zároveň dodává, že se dnes nejčastěji šíří např. přes sociální sítě. Typicky se jedná o situaci, kdy uživatel otevře škodlivý odkaz.

Antivirus je schopen nejen detekovat škodlivý kód, ale také nalézt aplikace, které představují potenciální nebezpečí. Tyto aplikace se označují jako potenciálně nechtěné a na jejich seznam se řadí např. aplikace zobrazující nevyžádaný obsah či takové, které snižují výkon zařízení (ESET, n.d.).

1.4.3 IDS/IPS

IDS

IDS, neboli Intrusion Detection System, je zkratkou pro detekci narušení. Jinými slovy IDS představuje soubor nástrojů, které pomáhají identifikovat a hlásit nepovolené síťové aktivity. Úkolem IDS není detekovat narušení, ke kterému došlo, ale monitorovat takové aktivity, které by se narušením stát mohly. Z toho vyplývá, že IDS není systémem ochrany ale spíše prevence. Existují tři verze, a to NIDS, HIDS a hybridní. NIDS se soustředí na analýzu síťových paketů, ze kterých dedukuje napadení. HIDS za pomoci instalace softwaru skenuje aktivitu uzlových zdrojů. Logicky vyplývá, že hybridní verze kombinuje NIDS i HIDS, tudíž umožňuje jak sledovat události, ke kterým dochází v uzlovém systému, tak monitorovat síťový provoz (Endorf a kol., 2005). Detailní výčet rozdílů obsahuje Tabulka 2.

Tabulka 2: Rozdíly mezi HIDS a NIDS

HIDS	**NIDS**
Úzké použití (hlídá pouze specifické činnosti hostitele).	Široké použití (hlídá všechny síťové činnosti).
Složitější nastavení.	Jednodušší nastavení.
Vhodnější pro detekci interního napadení.	Vhodnější pro detekci externího napadení.
Dražší implementace.	Lacinější implementace.
Detekce je založena na tom, co může zaznamenat každý jednotlivý hostitel.	Detekce je založena na tom, co může být zaznamenáno v celé síti.
Ignoruje hlavičku paketu.	Přezkoumává hlavičku paketu.
Odezva je obyčejně až tehdy, co byl zaznamenán podezřelý vstup v logovacím souboru.	Odezva téměř v reálném čase.
OS specifický.	Nezávislý na OS.
Detekuje lokální útok dříve, než je napadena vlastní síť.	Síťový útok detekují jako důsledek analýzy užitečné zátěže.
Verifikuje úspěch nebo selhání útoku.	Detekuje neúspěšné pokusy o útok.

Zdroj: Endorf a kol., 2005

IPS

IPS, tedy Intrusion-Prevention System, je systémem prevence proti narušení. IPS je umístěn v chráněné síti, kterou sleduje. V případě narušení přijme opatření. IPS byl vytvořen z IDS, je jeho vylepšenou variantou (Endorf a kol., 2005). Srovnání obou systémů zachycuje Tabulka 3.

Tabulka 3: Srovnání IDS a IPS

IDS	**IPS**
Instalují se na segment sítě (NIDS) a uzel (HIDS).	Instalují se na segment sítě (NIPS) a uzel (HIPS).
V síti jsou pasivním prvkem.	Jsou zařazovány sériově (nejsou pasivní).
Nemohou analyzovat šifrovaný provoz.	Vhodnější pro ochranné aplikace.
Centrální správa řízení.	Centrální správa řízení.
Výstrahu vydávající produkt (reaktivní).	Blokující produkt (proaktivní).

Zdroj: Endorf a kol., 2005

1.4.4 Firewall

Firewall je pro bezpečnostní ochranu zařízení nepostradatelný, přesto je však nezbytné instalovat i další bezpečnostní produkty. Firewall může *„chránit proti hackerům a dohlížet na dodržování bezpečnostních pravidel“* (McCarthy a Weldon-Siviy, 2013, s. 245). Firewall upozorňuje na to, že program usiluje o přístup do počítače přes porty, nebo pokud se program spuštěný na daném počítači pokouší získat přístup na internet. Jinými slovy, firewall *„kontroluje typ přenosů, který je mezi sítěmi povolen“*, čili pracuje jako zámek. Jeho hlavní funkcí je kontrolovat přenos na internet a z internetu.

Další schopností firewallu je dohled nad dodržováním pravidel bezpečnosti a poskytnutí ochrany zevnitř ven. Např. knihovna může nastavit takový firewall, který návštěvníkům nedovolí prohlížet stránky s určitým obsahem. Pokud se uživatel snaží firewall obejít, program to je schopen zaznamenat. Co však firewall neumí je ochránit před útoky, které jsou vedeny pomocí dat. Typicky se jedná o malware, který se stáhnul do počítače.

Firewall uživatele chrání tak, že:

- *„povoluje nebo odmítá požadavky k odesílání dat z počítače a na něj,*
- *monitoruje požadavky na přístup k portům“* (McCarthy a Weldon-Siviy, 2013, s. 248).

2 ETICKÝ HACKING

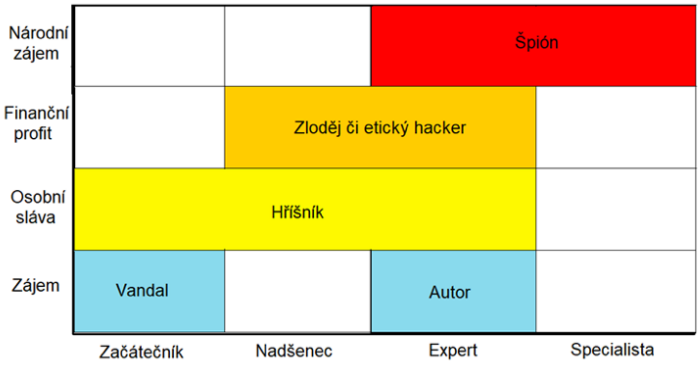
Aby byly firmy schopny se před útoky bránit, musí vědět, jak k nim dochází a jaké riziko pro ně tyto útoky představují. Úkolem etického hackingu tedy je najít síťové nebo počítačové služby ve firmě a posoudit, jak je může útočník zneužít (Harris a kol., 2008). Faily (2014) připomíná, že narůstající počet kybernetických útoků zvyšuje potřebu vzdělávání v oblasti kyberbezpečnosti. Etický hacking je jeden z nástrojů, který je k této výuce využíván.

Mezi přínosy etického hackingu patří možnost systémy reálně otestovat. Přestože přinese takový test negativní zjištění, je stále lepší být proaktivní než čelit reálnému útoku. Etický hacking zároveň umožňuje systém otestovat do větší hloubky, a to včetně slabin celé sítě, ne pouze operačních systémů (Sahare a kol., 2014).

2.1 White-hat, Black-hat, Grey-hat

Kovalčík (2020) hovoří o třech typech hackerů, pro které se nejčastěji využívá rozlišení pomocí barev. Černí hackeři (Black-Hat) napadají počítačové systémy s cílem krádeže dat nebo jiné nelegální aktivity. Za jejich aktivitami stojí nejčastěji finanční profit. Bílí hackeři (White-Hat) hledají bezpečnostní chyby a snaží se najít vhodná opatření. Mezi těmito dvěma protipóly se nachází šedí hackeři (Grey-Hat), kteří své aktivity provozují pro osobní slávu či zábavu. Jejich cílem není ukrást data, přesto však porušují zákon, jelikož nemají pro svou činnost souhlas majitele daného systému.

Dělení podle úmyslů však není jediné, které lze na hackery aplikovat. Kovalčík (2020) dělí hackery také dle jejich schopností a cílů, jak zachycuje Obrázek 3. Do druhé úrovně se řadí většina šedých hackerů, naproti tomu černí hackeři se nachází v kategorii třetí. Sem však spadají také etičtí hackeři, jelikož i oni mají ze svých aktivit profit. Ten v jejich případě znamená finanční odměnu za vykonanou práci.



Obrázek 3: Dělení hackerů

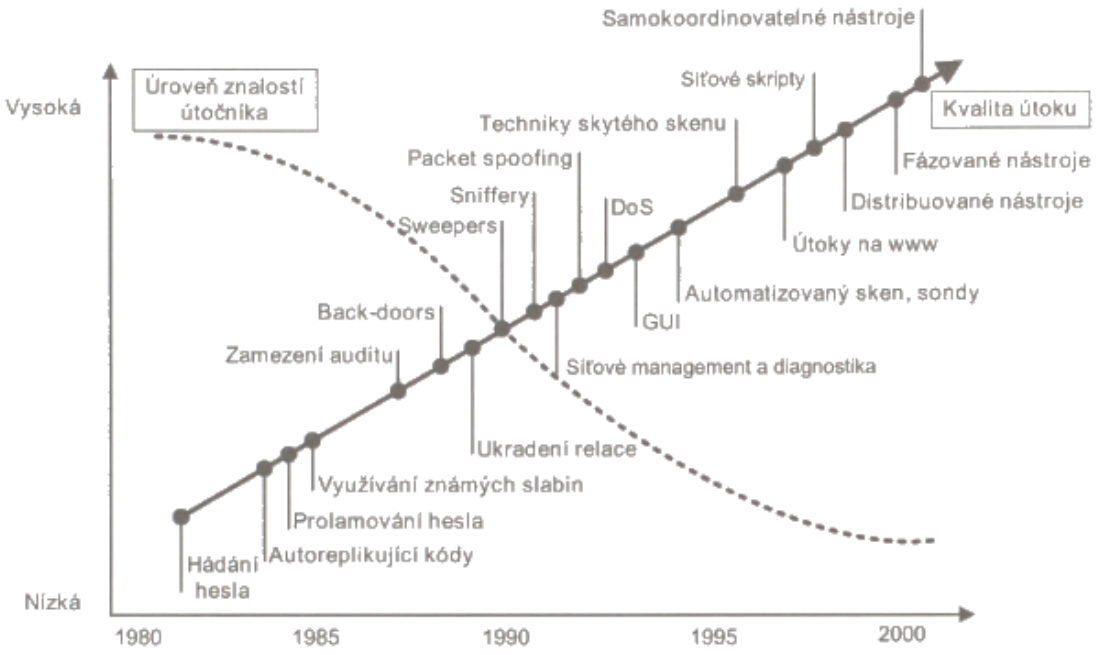
Zdroj: Kovalčík, 2020

Další typologii dělení podle nejvýznamnějších skupin hackerů uvádí Jirovský (2007, s. 54):

- *Kriminální hackeři (crackeři)* – jsou motivováni ziskem za každou cenu. Jejich cíle zahrnují většinou servery velkých firem nebo institucí. Často se jedná o organizované a izolované skupiny spojené s kriminálním podsvětím. Řadí se sem i hackeři najímaní korporacemi s cílem provádět průmyslovou a obchodní špionáž u konkurence.
- *Profesionální hackeři* – sem patří již zmínění „White Hats“, „Grey Hats“ a „Black Hats“ (tzv. klobouky).
- *Nespokojení zaměstnanci* – jde o jednu z nejnebezpečnějších skupin hackerských aktivit.
- *Ideologičtí hackeři* – jsou fanaticky zaměřené skupiny internetových aktivistů používajících Internet k prosazování svých politických nebo ideologických cílů. Aktivity, na kterých se podílejí, souvisí s nějakou významnou událostí ve světové politice nebo ekonomice. Označují se také jako „haktivisté“ a často jsou zahrnováni do kyberteroristických skupin.
- *Script-kiddies (lammers, loosers)* – nejmladší skupina hackerů, která si však označení hacker nezaslouží. Jde o skupinu s minimálními technologickými znalostmi. Využívají nástrojů a informací hackerské komunity, aniž by byli schopni docenit jejich dopady a následky. Jejich případný neuvědomělý zásah může být o to více zničující. Nevytvářejí vlastní programy, jen je stáhnou z internetu jako hotový nástroj a použijí je pro své zviditelnění.
- *Nevyužití dospělí hackeři* – jsou původní „skript-kiddies“, kteří nenašli odpovídající uplatnění. Touží po uznání v hackerské komunitě.

2.2 Nástroje

Hackerské nástroje se neustále zdokonalují a automatizují. Nejdůležitější součástí hackerského útoku je přesto stále sama osoba hackera. Jsou to jeho nabyté vědomosti, znalosti a dovednosti, které určují úspěšnost útoku (Jirovský, 2007). Obrázek 4 znázorňuje vývoj hackerských nástrojů a technik.



Obrázek 4: Vývoj hackerských nástrojů a technik

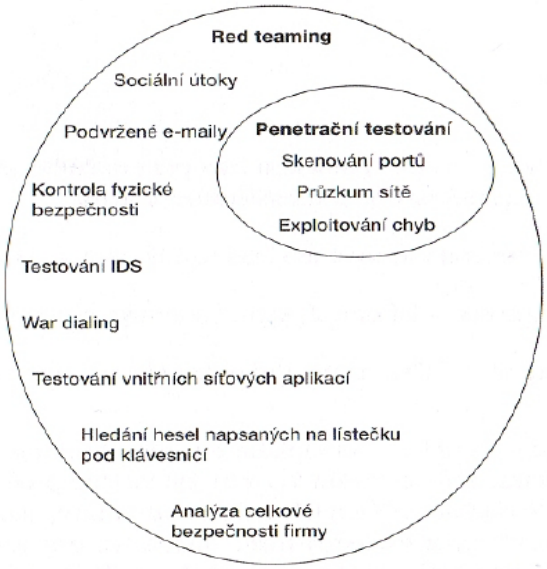
Zdroj: Jirovský, 2007

Na následujících odstavcích budou představeny nástroje etického hackingu, mezi které se řadí penetrační testování, systémové testy, Kali Linux a sociální inženýrství.

2.2.1 Penetrační testování

Penetrační testování představuje moment, kdy dochází k testování bezpečnosti sítě. Jeho primárním cílem je získat kontrolu nad celou sítí. Sekundárním cílem je získat tuto kontrolu co nejvíce způsoby, aby bylo možné vytvořit seznam chyb v síti. Penetrační testování je tedy ideální metodou k vyzkoušení efektivity bezpečnostních opatření a k identifikaci hluchých míst v obraně sítě (Harris a kol., 2008). V souvislosti s testováním bezpečnosti sítě se pojí také red teaming. Do této analýzy patří kromě skenování portů a průzkumu sítě také testování IDS, testování internetových aplikací, útoků ze sociálních sítí a identifikace dalších bezpečnostních problémů. Rozdíly mezi red teaming a penetračním testováním zachycuje Obrázek 5. Detailnější informace o penetračním testování a jeho fázích nabízí následující podkapitola.

V praxi se lze setkat s celou řadou softwarů pro penetrační testování. Patří mezi ně Kali Linux, Metasploit, Wireshark, w3af, John The Ripper, Nessus, Nmap, Dradis nebo BeEF (Denis a kol., 2016).



Obrázek 5: Srovnání Red teamingu a penetračního testování

Zdroj: Harris a kol., 2008

2.2.2 Systémové testy

Pro systémové testy neexistuje předem daný postup, proto vyžadují, aby hacker přišel s více nápady než jen s penetračním testováním. Další rozdíl oproti penetračnímu testování spočívá v tom, že systémové testy dovolují hackerovi soustředit se pouze na jeden program, což se pojí s omezeným počtem možných útoků a jejich směrů (Harris a kol., 2008).

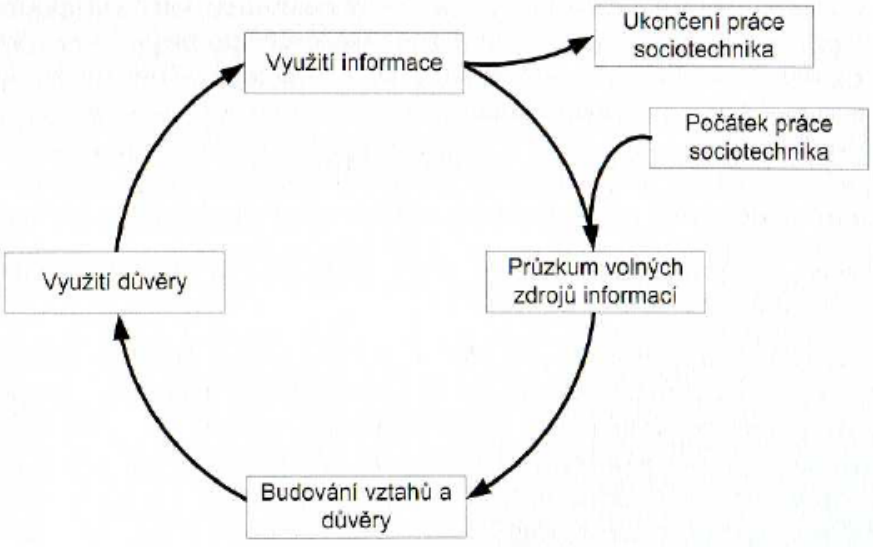
Harris a kol. (2008) rozlišují dvě hlavní části systémových testů. První z nich je ohledání povrchu, během kterého se hacker snaží identifikovat všechna místa, ve kterých je aplikace v kontaktu s vnějšími daty. Toto je klíčové pro celý zbytek testu. Druhou částí je cílené hledání chyb. V tento moment již hacker disponuje seznamem vektorů útoku, který prochází a hledá v něm ten správný způsob, jak testovaný systém napadnout. Útočit může přes soubory, pojmenované roury, registr systému, slabá ACL nebo může provést síťové útoky.

2.2.3 Kali Linux

Kali Linux je linuxová distribuce, která slouží pro forenzní analýzy a penetrační testování. Kali Linux disponuje celou řadou integrovaných penetračních a exploatačních nástrojů. Hacker si proto nemusí nástroj vytvářet sám, což představuje časovou úsporu. Kali Linux funguje na různých platformách. Celkem obsahuje více než 600 nástrojů pro penetrační testování, je zcela přizpůsobivý a dodržuje Filesystem Hierarchy Standard. Ten uživatelům umožňuje vyhledávat podporované soubory, binární soubory či knihovny. Kali Linux rovněž podporuje řadu bezdrátových zařízení a má vícejazyčnou podporu. O Kali Linux se často hovoří jako o platformě, jelikož pro jeho instalaci je nezbytné využít virtuální stroj, např. VMware (Denis a kol., 2016).

2.2.4 Sociální inženýrství

Útoky spojené se sociálním inženýrstvím jsou umožněny selháním lidského faktoru. Sociotechnik, který je původcem útoku, nejprve získává a zkoumá volně dostupné informace. Na jejich základě si buduje vztah s vytipovanými osobami v daném podniku a jejich důvěru zneužije pro získání informací. Jeho sociotechnické útoky pobíhají na dvou úrovních, fyzické a psychologické (Jirovský, 2007). Obrázek 6 zachycuje sociotechnický cyklus, Tabulka 4 potom taktiku těchto útoků a obranu proti nim.



Obrázek 6: Sociotechnický cyklus útoku

Zdroj: Jirovský, 2007

Tabulka 4: Sociotechnické útoky, taktika a obrana

Oblast útoku	Sociotechnické taktiky	Obrana
Telefon (help desk)	Předstírání identity, přesvědčování	Zaměstnanci nesmí vydávat svá hesla a důvěrné informace
Vchod do budovy	Vniknutí v převleku	Průkazy, ostraha, trénink zaměstnanců
Kancelář	Nahlížení přes rameno	Hesla psát pouze s jistotou, že se nikdo nedívá
Kancelář	Procházení budovy a hledání odemknutých kanceláří	Každý host by měl být eskortován
Serverové místnosti	Pokus o logování, odstranění vybavení, nahrání trojského koně, který získává data	Serverové místi musí být pořád zamčené, měl by být veden inventář vybavení
Telefonní ústředna	Kradení linek a přesměrování	Kontrola meziměstských a mezikontinentálních hovorů
Odpadkové koše	Prohledávání odpadků	Odpadkové kontejnery v zabezpečené a monitorované oblasti, skartovat všechny důležité dokumenty, bezpečné mazání magnetických médií
Intranet-Internet	Software na odchytávání hesel	Sledování programového vybavení počítačů
Kancelář	Zcizení dokumentů	Hierarchie důvěrnosti dokumentů a adekvátní zacházení s nimi

Zdroj: Jirovský, 2007

2.3 Nástroje penetračního testování

Proces etického hackingu je vcelku jednoduchý. Je ohledán cíl, nalezeny chyby, ty jsou zneužity pro získání přístupu do systému a výsledek tohoto testu je sdílen se zákazníkem (Harris a kol., 2008).

Fáze penetračního testování

Aby mohl být proces, který byl v předchozím odstavci představen realizován, je zapotřebí učinit několik kroků - fází. Za zmínku stojí také fakt, že existuje řada mezinárodních kurzů a certifikací pro provádění penetračního testování. Mezi ně patří např. Certified Ethical Hacker, Certified Information Systems Security Professional, OSSTMM Professional Security Tester nebo Licensed Penetration Tester (Gregr, 2015).

Sběr informací – enumerace

Sběh informací neboli průzkum, je prvním krokem penetračního testování. Jeho záměrem je získat co nejvíce informací o potenciálních cílech bez využití jakýchkoliv interních informací. Tento postup je klíčový, neboť napodobuje kroky hackera, který by se o útok pokoušel. Poté, co bylo anonymně získáno co největší množství informací, je přistoupeno k invazivnějším technikám. Jejich cílem je identifikovat všechny „živé“ systémy ve vytipované síti (Harris a kol., 2008).

Odhalování zranitelnosti

Jak připomíná Harris a kol. (2008), fáze hledání chyb je invazivnější než fáze předchozí. Výsledkem této fáze by měl být seznam systémů, které je možné kvůli bezpečnostní chybě ovládnout. Ve snaze nalézt chyby se hacker snaží odhalit bannery síťových služeb, odposlechnout autentizační údaje v síti a identifikovat nezáplatované části daného operačního systému.

Exploitace

V momentě, kdy byl vytvořen seznam potenciálních systémů, které obsahují nějakou bezpečnostní díru, je nezbytné tyto díry ověřit. Pro penetrační testování platí, že je důležité se nabourat do největšího počtu systémů a získat co nejvyšší práva. Toto vychází z cíle penetračního testování, tedy odhalit mezery v zabezpečení. Důkaz o tom, že se podařilo hackerovi ovládnout všechny systémy v síti, a že získal přístup k citlivým informacím, je maximální možné splnění tohoto cíle (Harris a kol., 2008).

Report

Konečnou fázi penetračního testování představuje report. Ten shrnuje výsledky těchto předchozích testů a informuje o nich vedení společnosti, která si je objednala. Cílem této fáze je přinést zákazníkovi kvalitní závěrečnou zprávu, která má potenciál zlepšit bezpečnost firmy (Gregr, 2015).

3 KYBERNALITA

Jirovský (2007, s. 19) popisuje kybernetickou kriminalitu neboli kybernalitu jako *„činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti“*. Jedná se o situace:

- namířené přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod.,
- počítač vystupuje jen pouze jako nástroj pro páchání trestného činu,
- počítačová síť a k ní připojená zařízení jsou prostředím, v kterém se tato činnost odehrává.

Sledování projevů kybernality v prostředí je objektivně velmi obtížně vnímatelné. Prostředí kyberprostoru můžeme pozorovat pouze pomocí strojů a přístrojů, které nám takový přístup umožní (Jirovský, 2007).

3.1 Základní pojmy

Hrozba

Hrozba je cokoliv, co může jakýmkoliv způsobem vést k nežádoucí změně informace, chování systému nebo ovlivnit jeho parametry (Jirovský, 2007).

Hrozba představuje nějaké potencionální narušení *důvěrnosti*, *integrity*, *dostupnosti* nebo *legálnosti* použití systému. Hrozba zahrnuje:

- osoby,
- prostředky,
- události,
- myšlenky (Jirovský, 2007).

Útok

Jde o faktickou realizaci hrozby.

Ochrana

Ohranou se rozumí *„veškeré fyzické mechanismy, definované politiky nebo procesy, které mají sloužit k ochraně systému nebo obecně majetku před hrozbou nebo útokem“* (Jirovský, 2007, s. 20). Jakákoliv ochrana se vyznačuje zranitelností. Jsou to většinou slabá místa ochrany nebo její naprostá absence.

Riziko

Míra rizika se vztahuje k hodnotě chráněného majetku v případě, kdy dojde k úspěšnému útoku ve zranitelném místě systému. (Jirovský, 2007)

Klasifikace hrozeb

Hrozby můžeme klasifikovat na (Jirovský, 2007):

- *úmyslné* – např. průnik útočníka do systému,
    - *pasivní* – např. monitorování provozu, který zjišťuje obsah předávaných informací, aniž by byl obsah měněn.
    - *aktivní* – např. útok je realizací aktivní hrozby, která zahrnuje změnu přenášené informace. Příkladem je třeba změna částky při finanční transakci.
- *neúmyslné* – např. ohrožení systému, které vzniká chybou operátora, uživatele nebo samotného systému.

Základní skupiny hrozeb

Základní hrozby odrážející hlediska bezpečnosti informačního systému (Jirovský, 2007):

- *Únik informace* – případ, kdy je informace důvěrného charakteru prozrazena neautorizovanému subjektu či je jím odhalena. Tato situace pak může vést k přímým útokům se značným dopadem.
- *Narušení integrity* – porušení konzistence dat, které může vést k vytvoření nových dat či změně nebo vymazání stávajících dat neautorizovaným subjektem.
- *Potlačení služby* – případ, kdy je úmyslně bráněno přístupu legitimního subjektu k informacím nebo jiným systémovým zdrojům. Příkladem jsou právě útoky DoS.
- *Nelegitimní použití* – případy, kdy je zdroj používán neautorizovaným subjektem nebo neadekvátním způsobem. Příkladem je průnik do systému a používání placených služeb bez faktického vyúčtování nebo zaplacení služby.

Aktivační hrozby

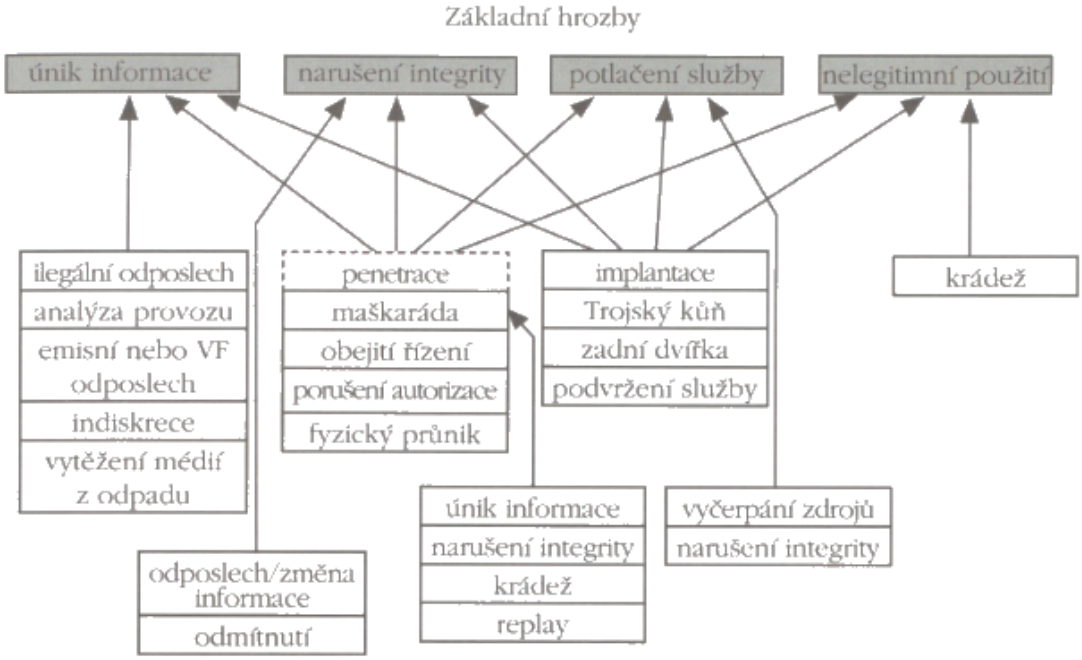
Realizace aktivačních hrozeb vede k bezprostřednímu vytvoření základní hrozby a přímému ohrožení bezpečnostních parametrů systému. Jirovský (2007) rozděluje aktivační hrozby na:

- *Penetrační hrozby*:
    - *Maškaráda* – jedna entita (osoba nebo systém) se vydává za jinou entitu
    - *Obejití řízení* – útočník využije systémové nebo bezpečnostní slabiny k získání neautorizovaných práv nebo privilegií.
    - *Narušení autorizace* – zneužití autorizovaného přístupu ke zdroji pro neautorizované účely.
- *Implantační hrozby*
    - *Trojský kůň* – software obsahuje nepozorovatelnou část, která po spuštění naruší bezpečnostní prvky systému.

- *Zadní vrátka* – část systémového software, která umožňuje při poskytnutí specifického datového řetězce na svůj vstup, obejít nástroje bezpečnostní politiky systému.

Podkladové hrozby

Hrozby, které jsou podkladem pro realizaci až několika základních hrozeb označuje Jirovský (2007) jako „podkladové hrozby“. Vztah mezi základními hrozbami a podkladovými hrozbami uvádí Obrázek 7, popis je uveden v příloze A.



Obrázek 7: Vztah základních a podkladových hrozeb

Zdroj: Jirovský, 2007

Typické hrozby

Příloha A zahrnuje všechny známé způsoby útoku, nezahrnuje však jejich metody. Například viry nebo červi současně patří do kategorie „obejití řízení“ a „maškaráda“, tedy jsou jen realizací kombinovaného útoku (Jirovský, 2007).

Základní stavy hrozby

- *Zastrašovací moment* – potencionální hrozba formulovaná útočníkem není dokonána a k dosažení daného efektu u cíle má samotné vyjádření hrozby postačující efekt.
- *Realizace hrozby* – útočník se nespokojí s formulací hrozby vůči cíli a hrozbu uskuteční nebo se ani s formulací hrozby neobtěžuje a provede ji bez předběžného ohlášení (Jirovský, 2007).

3.2 Legislativa

Kolouch (2016) uvádí, že Internet nemá právní subjektivitu. Jde o informační a telekomunikační systém, který se skládá z různých právních subjektů a to v podobě fyzických a právnických osob, tedy uživatelů, poskytovatelů veřejných či neveřejných služeb a podobně. Internet jako takový není nikým vlastněn. V případě internetu nejde o fyzickou ani právnickou osobu. Jednotliví poskytovatelé připojení k Internetu mají přímý vztah k určení právní povahy Internetu a vymezení působnosti jednotlivě zainteresovaných osob.

Internet tvoří jednotlivé počítačové sítě, které jsou navzájem propojeny. Tyto menší počítačové sítě pak typicky vlastní nějaká fyzická či právnická osoba. Často se jedná o ISP neboli o poskytovatele připojení k síti (Internet Service Provider). Vlastníkem, ale může být i stát, či jakákoli jiná fyzická či právnická osoba. Tyto sítě je možné považovat za věc, dle § 489 zákona č. 89/2012 Sb. Občansky zákoník, ve znění pozdějších předpisů (Kolouch, 2016).

Internet není možné definovat, jako věc nehmotnou. Podle § 496 odst. 1 OZ se věcí nehmotnou rozumí *„práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty.“* Toto v případě Internetu není možné uplatnit, protože Internet není právem a zároveň to ani není věc bez hmotné podstaty. Internet, bez hmotné podstaty, tedy informačních a komunikačních technologií a jednotlivých počítačových systémů, nemůže existovat. Internet je pevně svázán s hmotnou podstatou, tedy s hmotnou věcí, kterou někdo vlastní (Kolouch, 2016).

Kybernetická trestná činnost v mezinárodních dokumentech

Chceme-li se zabývat otázkou případné odpovědnosti za protiprávní jednání, musíme využít nejen prostředků vnitrostátních (ať trestněprávních či občanskoprávních), ale i mezinárodních (Kolouch, 2016). Činnost, která je v jedné zemi trestná, nemusí být v druhé zemi vůbec zahrnuta do legislativy nebo může být legální. V globálním rozměru kybernality se nedostává potřebných nástrojů. Mimo nedostatek zákonných norem neexistuje dostatek zákonných precedentů nebo judikátů (Jirovský, 2007). Seznam mezinárodních dokumentů zabývajících se kybernetickou trestnou činností je uveden v příloze C.

Právní normy ČR

Právní normy, které se zabývají hackingem a kybernalitou v rámci České republiky jsou uvedeny v příloze D.

4 METODOLOGIE

Tato bakalářská práce předkládá případové studie zaměřené na etický hacking. V této kapitole je nejprve vysvětlen samotný pojem „případová studie“, posléze jsou čtenáři seznámeni s procesem jejich tvorby.

4.1 Případové studie

Jak poznamenává Mareš (2015), pojem „případová studie“ není jednoduché definovat, jelikož zahrnuje řadu koncepčních přístupů, aspektů, typů studií apod. Společné budiž to, že se jedná o celostní přístup, který se snaží poznat dopodrobna daný případ, zachytit ho v kontextu reálného života a dospět k důkladnému porozumění. Případové studie mohou být jednopřípadové, neboli individuální nebo studie s více než jedním případem. Pro označení „multiple-case study“ neexistuje v češtině žádné jednotné označení. Jejich dělení zachycuje příloha B.

4.2 Tvorba případových studií

Při tvorbě případových studií je potřeba mít na paměti ještě jednu definici, kterou přináší Brablec (2021), a to že *„případová studie je do detailu rozebrané a popsané dodání konkrétního produktu nebo služby zákazníkovi“*. Případová studie umožňuje jejímu autorovi popsat, jak potenciálnímu zákazníkovi, pro kterého je případová studie určená, lze pomoct s daným problémem, na který se studie zaměřuje.

Stěžejním atributem případových studií jsou fakta. Čím přesnější, detailnější a věrohodnější, tím lépe. Druhým klíčovým aspektem je kontext – detailní vykreslení situace, možných problémů i přínosů zasazují fakta do „kompaktního celku“. Brablec (2021) přinesl popis struktury případové studie, která je orientovaná na klienty. Taková studie musí obsahovat:

- *informace o klientovi* – představení jeho aktivit a potenciálních problémů, kterým čelí,
- *řešení* – jakým způsobem by měl být představený problém řešen, jak se o tomto řešení správně rozhodovat, jak toto řešení uvést do praxe,
- *výsledek* – co navržené řešení přináší.

Roubal a kol. (2019) identifikovali a popsali čtyři fáze sestavování případových studií:

- *odhodlání* – tato fáze pomáhá zodpovědět řadu otázek, např. proč je daná případová studie přínosná a proč se vyplatí se dané problematice věnovat,
- *příprava* – identifikace otázek, kterým se bude věnovat již konkrétní případová studie,
- *sběr dat* – sebraná data pomáhají odpovědět na otázky, které byly sestaveny v předchozím kroku,
- *zpracování a sepsání* – základem je kritické prozkoumání a systematické porovnání získaných dat, hledání odpovědí na stanovené otázky.

Ilinčev (n.d.) dodává, že případová studie může být krátká nebo dlouhá. Krátká má rozsah 500–1 000 slov, zatímco dlouhá 1 500-2 000 slov. Studie by dle autora měla ukázat, jaké problémy umí její autor vyřešit (pokud se zaměřuje na klienty), jak identifikuje problém a jaká nabízí řešení. Důležité je také zmínit, jak identifikovat, jaké řešení je správné a jak ho uvést do praxe.

Případové studie v této bakalářské práci byly vytvořeny tři, každá z nich se zaměřuje na jiný podnik. Zvolené podniky, označené A, B a C, provozují svou činnost v odlišných oborech. Z toho vyplývá, že zpracovávají a uchovávají různá data, a to v různém objemu. Oblast podnikání byla zvolena tak, aby demonstrovala nebezpečí, která v souvislosti se zneužitím dat hrozí. Je zde patrný rozdíl mezi krádeží jména, bankovních údajů, zdravotních záznamů apod.

Každá případová studie demonstruje, jak důležitá je počítačová síť pro fungování podniku, zda se někdy objevil útok a jak se podniky snaží svá data zabezpečit. Důraz je kladen na sociální inženýrství, proto je sledována jak počítačová síť, tak offline prostředí. Identifikovány jsou možné hrozby s cílem navrhnout možná zlepšení.

5 PŘÍPADOVÉ STUDIE

Případové studie byly vytvořeny pro fiktivní podniky v různých odvětvích s cílem identifikovat, jakou roli v jejich fungování hraje počítačová síť, s jakými daty pracují a jak je nástroje etického hackingu mohou ochránit. Tyto podniky byly rozděleny do tří kategorií dle dat, které získávají a uchovávají. Detaily obsahuje Tabulka 5.

Tabulka 5: Rozdělení zkoumaných podniků

Podnik	Riziko	Zdůvodnění	Role počítačové sítě
A	střední	Podnik zpracovává veliké množství osobních údajů, které však nepatří mezi citlivé osobní údaje.	Klíčová
B	vysoké	Podnik zpracovává citlivé osobní údaje ve velkém rozsahu.	Klíčová
C	vysoké	Podnik zpracovává citlivé osobní údaje ve velkém rozsahu.	Klíčová

Zdroj: vlastní

5.1 Případová studie I

V první případové studii figuruje podnik A, který patří svou velikostí mezi malé (Czech Invest, n.d.) a který operuje v oblasti e-commerce. Bližší informace obsahují následující podkapitoly.

5.1.1 Základní specifika podniku

Podnik A je e-shopem, který se zaměřuje na obchod s potřebami pro zvířata. Nabízí širokou škálu produktů od krmiv, přes vodítka, postroje, hračky až po doplňky stravy a jiné přípravky zaměřující se na zdraví domácích mazlíčků. Většina produktů, které podnik A na svých webových stránkách nabízí, je určena pro psy, kočky a drobné hlodavce. Nabídka pro chovatele koní a hospodářských zvířat je omezená.

Podnik A zaměstnává celkem 17 zaměstnanců včetně ředitele. Deset z nich pracuje ve skladu, ve kterém jsou drženy zásoby e-shopu. Tito zaměstnanci jsou zodpovědní také za fyzickou přípravu a expedici objednávek zákazníků, jeden zaměstnanec spravuje webové stránky e-shopu a řeší IT záležitosti. Dva pracovníci mají na starosti administrativu, dva další potom fakturaci přijatých objednávek. Poslední zaměstnanec pracuje jako asistent ředitele. Z těchto 17 osob pracuje 13 z nich na plný úvazek, další 4 na částečný. Podnik A si externě najímá účetní společnost a úklidovou firmu. Pokud je potřeba obstarat nábor nového zaměstnance, řeší danou situaci ředitel

za pomoci svého asistenta či někoho z administrativy. K tomuto nedochází často, poslední zaměstnanec nastoupil v roce 2015. Od tohoto roku je tým stabilní.

Každý měsíc podnik A vyřídí mezi 7 500 a 9 000 objednávkami. Průměrná cena jedné objednávky je 290 Kč. Webové stránky podniku A neumožňují nakoupit bez vytvoření účtu na této stránce. To firmě umožňuje sledovat nákupní chování zákazníků a evidovat historii všech objednávek, které byly provedeny. S tímto podnik začal v roce 2012, v databázi má tedy téměř 9 let záznamů.

Podnik A uchovává následující informace o svých zákaznících:

- jméno a příjmení,
- doručovací adresa,
- telefonní číslo (není povinný údaj, přesto ho většina zákazníků uvádí, aby mohli obdržet SMS s detaily o doručení),
- e-mailová adresa,
- heslo pro přístup k účtu na webových stránkách.

Firma neuchovává informace o platebních kartách klientů. Informace nutné pro doručení zásilek sdílí podnik A s dopravcem, kterého si zákazník pro doručení své zásilky vybere. Podnik spolupracuje s Českou poštou a dvěma dalšími soukromými dopravci.

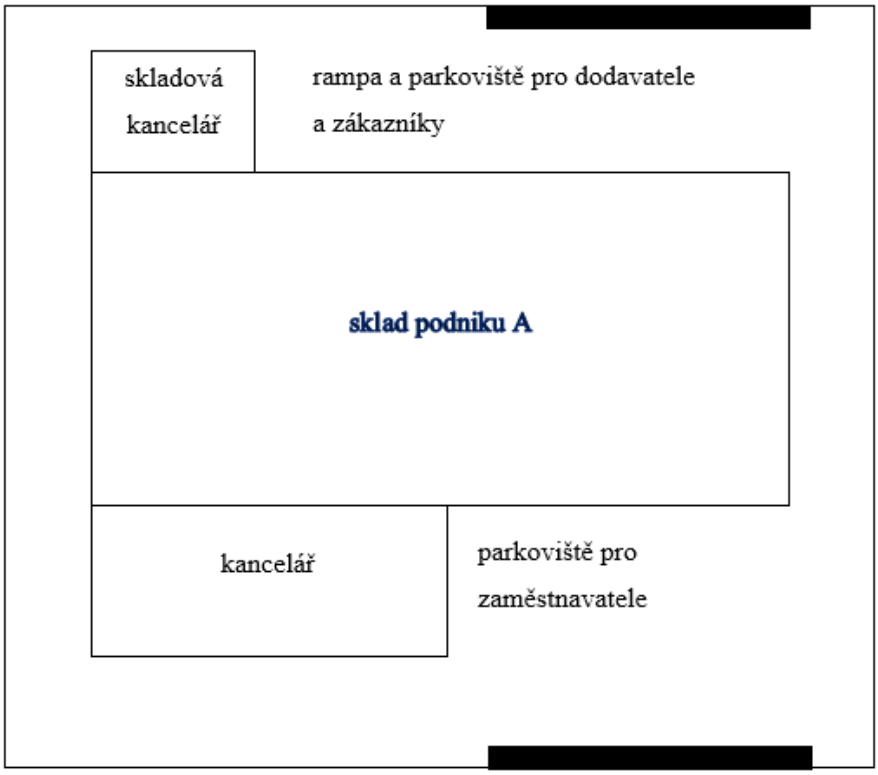
5.1.2 Počítačová síť a hrozby

Počítačová síť je pro podnik A klíčová. Bez fungujícího e-shopu a dat, které získává pro vyřízení objednávek, by nebyl schopen fungovat. Podnik A má celkem 11 počítačů, každý zaměstnanec pracující v kanceláři má k dispozici jeden počítač a další 4 jsou k dispozici ve skladu. Ty slouží k vyřizování objednávek zákazníků a tvorbě objednávek u dodavatelů. Každý zaměstnanec pracující v kanceláři má přístup pouze ke svému počítači, který má chráněn heslem. Všichni zaměstnanci byli proškoleni v souladu s GDPR nařízením o tom, že nemají svůj počítač nechávat spuštěný bez dozoru. Jelikož se jedná o stolní počítače, není možnost, aby si je zaměstnanci odnesli domů.

Situace je poněkud komplikovanější u počítačů umístěných ve skladu. Ty jsou sdílené, přiřazeny uživatelům sklad 1 – sklad 4. Každý z těchto uživatelů používá stejné heslo, které je napsáno na lístku a pověšeno na nástěnce ve skladové kanceláři a pravidelně se neaktualizuje. Neexistuje žádné pravidlo, podle kterého by zaměstnanci přistupovali pouze z 1 určitého počítače. Jedinou zásadou je to, že tři počítače bývají využívány pro vyřizování objednávek zákazníků a pouze jeden pro objednávky od dodavatelů,

pokud se nevyskytne nějaká nečekaná situace. To, který z těchto počítačů pracuje na jaké operaci, se liší každý den.

Firemní kultura v podniku A je velice uvolněná. Zaměstnanci mohou na svých počítačích kontrolovat svůj soukromý e-mail a není kontrolováno, jaké webové stránky pracovníci navštěvují. Do kanceláří se nelze dostat bez dozoru. Dveře jsou zamčené a návštěvník musí zazvonit, aby se dostal dovnitř. Skladová kancelář je více přístupná, neboť e-shop umožňuje vyzvednout zásilku přímo ve skladu. Návštěvník se tedy dostane do objektu, ve kterém podnik A sídlí. Dveře skladové kanceláře by měly být zamčeny a jsou opatřeny zvonkem, který mají zákazníci využít. Velice často se stává, že dveře zůstávají otevřené, především v letních měsících. Za rohem od těchto dveří je rampa, jejíž vrata bývají také často nezajištěná. Půdorys objektu zachycuje Obrázek 8.



Obrázek 8: Plán sídla podniku A

Zdroj: vlastní

Jak je patrné z Obrázek 8, objekt má dva vjezdy. Jeden z nich slouží pro zaměstnance a vede na parkoviště určené pro jejich vozy. Tato brána je téměř vždy zavřená. Rozdílná situace platí pro vjezd, který slouží zákazníkům či dodavatelům. Tato brána je otevřená po celou pracovní dobu. Neexistuje totiž další vchod, kterým by se mohli zákazníci pěšky dostat do skladové kanceláře a vyzvednout si svou zásilku.

Podnik A využívá datové synchronizace se svými dodavateli. To zvyšuje rizika, jelikož při napadení sítě podniku A existuje hrozba rozšíření útoku také do dodavatelských sítí. Obecně lze tedy říct, že riziko jde dvěma směry – k dodavatelům a k zákazníkům. Podniku A hrozí nebezpečí úniku obchodních tajemství, strategií či krádež osobních údajů jeho zákazníků. Mezi tyto údaje patří jméno a příjmení zákazníka, doručovací adresy, telefonní čísla a e-mailové adresy. Hacker by také mohl získat informace o nákupním chování těchto zákazníků. Podnik eviduje veškerou historii objednávek, které zákazníci učinili.

Při rozboru hrozeb, se kterými se podnik A může setkat, lze vhodně aplikovat Tabulka 4 představenou Jirovským (2007), která byla součástí předcházející kapitoly a tabulku v příloze A. Podnik čelí útokům ve všech oblastech, jak po telefonu, tak přes serverové místnosti a offline prostředí. Objekt, ve kterém podnik A sídlí není dostatečně chráněn před vstupem neoprávněných osob a jejich přístupem k sítí. Tento nedostatek vyplývá z absence určitých pravidel – zamčení druhé příjezdové brány, zamčení dveří skladové kanceláře, odhlašování z počítačů v ní umístěných. Je tedy patrné, že právě skladová kancelář představuje pro podnik A vyšší bezpečnostní hrozbu. Ta je celkově podmíněna uvolněnou firemní kulturou, kdy zaměstnanci při kontrole svých osobních e-mailů či návštěvě nebezpečných webových stránek mohou zanést škodlivý virus do celé sítě. To však není jedinou možnou hrozbou. V minulosti se podnik A setkal s pharmingem při napadení jejich webových stránek a s útokem Man in the Middle.

5.1.3 Etický hacking a ochrana

Ochrana pro podnik A leží ve stejné oblasti, kde byly identifikovány hrozby. Jedná se tedy jak o ochranu sítě, tak o ochranu offline prostředí a hardwaru firmy.

Klíčovým bude tedy průzkum, jakožto první fáze etického hackingu. Etický hacker by měl využít kromě hromadného pingu a portu skenů také databázi ARIN, RIPE a APNIC pro vyhledávání informací, např. rozsah IP adres, jmenné servery či jména konkrétních osob (Harris a kol., 2008). Jak připomínají McCarthy a Weldon-Siviy (2013), nevzdělaní programátoři a chyby v programování vedou k bezpečnostním dírám. Podnik A by proto měl prověřit, zda jím zvolený zaměstnanec odpovědný za IT záležitosti disponuje dostatečnými znalostmi, které garantují ochranu dat firmy. Podnik by měl rovněž vytvořit směrnice dbající na využívání počítačů ve skladové kanceláři. Důležité je měnit častěji heslo, které by nemělo být pro všechny počítače stejné a viditelně vystavené na pracovišti.

Vedle zkoumání sítě a jejích potenciálních děr a slabin by měla být zkoumána také offline rovina ochrany dat podniku A. Umožnění přístupu nepovolaných osob na pracoviště

či ponechávání spuštěných zařízení bez dozoru vystavuje podnik A citelnému nebezpečí. Příloha E definuje úkony pro posouzení bezpečnosti a průniků do systému a v příloze F jsou doporučená nastavené systémů.

5.2 Případová studie II

Druhá případová studie se zaměřuje na podnik B, který nabízí široké veřejnosti jazykové kurzy. Více podrobností obsahují následující podkapitoly.

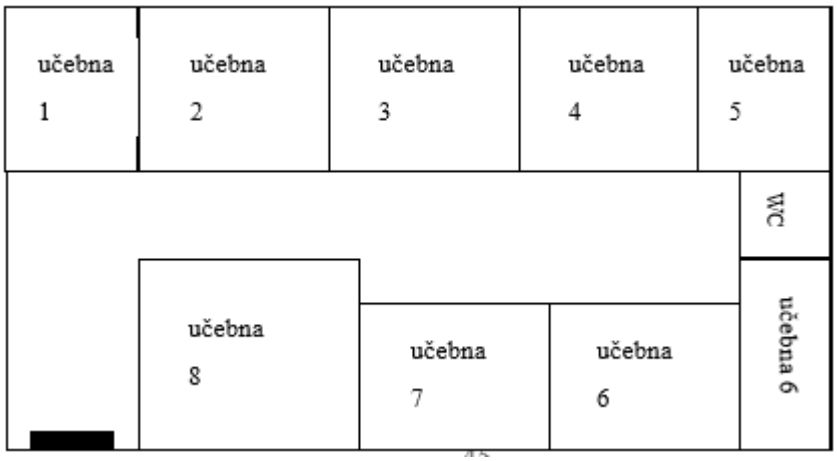
5.2.1 Základní specifika podniku

Jak bylo zmíněno výše, podnik B nabízí jazykové kurzy pro širokou veřejnost. V nabídce jazykové školy je výuka anglického, francouzského, španělského, italského, ruského, německého, švédského a japonského jazyka. Všechny kurzy jsou rozděleny do čtyř úrovní – úplní začátečníci, mírně pokročilí, pokročilí, konverzace. Do konverzačních kurzů se mohou přihlásit pouze takoví zájemci, jejichž znalost daného jazyka odpovídá úrovni C1/C2.

Podnik B započal své lektorské aktivity v roce 2015. Od svého vzniku sídlí stále na stejném místě, v prvním a čtvrtém patře obytné budovy. V prvním patře se nachází pouze kanceláře a zasedací místnost, ve čtvrtém patře potom učebny. Obě patra zachycují Obrázek 9 a Obrázek 10.

Obrázek 9: Plán prvního patra podniku B

Zdroj: vlastní



Obrázek 10: Plán čtvrtého patra podniku B

Zdroj: vlastní

V kanceláři č. 2 sedí ředitel podniku B, v kanceláři č. 1 se nachází finanční oddělení a první část administrativního oddělení, které se stará o chod jazykové školy. Kancelář č. 3 patří druhé části administrativy, která má na starosti komunikaci s lektory a klienty školy. Zvykem v rámci chodu podniku B je to, že lektoři sedí během přípravy na jednotlivé hodiny v zasedací místnosti č. 1. Druhá zasedací místnost slouží pro porady, pohovory a jiné schůzky.

Škola není vybavena recepcí. Budova, ve které sídlí, má vstupní dveře na číselný kód, který je sdělen jejím klientům při uhrazení kurzovného a také jednotlivým lektorům. Dveře v prvním patře jsou vždy uzamčené a jsou opatřeny zvonkem. Vchodové dveře ve čtvrtém patře zůstávají během pracovní doby otevřené. Ta je od 9 do 17 hodin. Některé jazykové kurzy se konají v pozdějších termínech, proto jsou lektorům, kteří je vyučují, rozdány klíče od vchodových dveří do prvního a čtvrtého patra, a také klíče od učebny, ve které hodina probíhá. Každý lektor má potom k dispozici klíče od učeben, ve kterých vyučuje, a to po dobu trvání kurzu.

Informace o lektorech i klientech jsou uchovávány v elektronické i papírové podobě. V kanceláři č. 1 se v listinné podobě nachází faktury od lektorů, dodavatelů (např. kancelářského materiálu, knih apod.) a informace o úhradách kurzovného. Tyto podklady jsou ve skříňce, která není opatřena zámkem. V kanceláři ředitele se nachází informace o zaměstnancích a jejich pracovní smlouvy, vše v uzamčeném šuplíku.

V kanceláři č. 3 jsou k dispozici kontaktní informace všech klientů i lektorů. Mezi tyto informace patří:

- jméno a příjmení,
- kontaktní adresa,
- telefonní číslo,
- e-mailová adresa,
- bankovní spojení,
- kurzy (navštěvované u klientů/vyučované u lektorů),
- historie (navštěvované kurzy u klientů/vyučované kurzy u lektorů, počátek spolupráce).

Právě kombinace informací o bankovním spojení, e-mailové adrese a telefonním čísle je důvodem, proč je podnik B zařazen v tabulce do vysoce rizikové skupiny. Tyto informace jsou uchovávány v uzamčené skříňce.

Všichni zaměstnanci podniku B mají klíče jak od prvního a čtvrtého patra, tak od všech kanceláří v prvním patře. Zasedací místnosti a sklad se nezamykají, jelikož neobsahují žádné cennosti ani data o klientech či lektorech. Lektoři mají k dispozici informace o klientech, kteří se účastní jejich kurzů. Sděleny jsou jim pouze jména a příjmení, jelikož jakýkoliv kontakt by měl probíhat přes administrativu podniku B. Přesto však není výjimkou, že lektor požádá studenty, aby mu na sebe dali e-mail či telefonní číslo, pokud chtějí. Tok těchto informací nikdo nesleduje a nekontroluje.

Podnik B má nastavenou externí spolupráci s úklidovou firmou, účetní firmou a IT firmou v případě, že se vyskytnou technické potíže např. s webovými stránkami. Obsahově si je spravuje sama škola. Zveřejňuje na nich nové kurzy, informace o kurzovném, lektorech, zpětnou vazbu klientů apod.

5.2.2 Počítačová síť a hrozby

Celkem v podniku B pracuje šest zaměstnanců včetně ředitele. Jeden je zodpovědný za finanční chod školy, druhý za administrativu spojenou s jejím chodem a třetí je na pozici asistenta. Všichni tito zaměstnanci pracují v kanceláři č. 1 a každý z nich je disponuje svým notebookem. Zbývající dva zaměstnanci sedí v kanceláři č. 3, jeden komunikuje s klienty školy, druhý s lektory. I oni mají svůj vlastní pracovní notebook.

Zaměstnanci byli poučeni, že nemají svůj notebook opouštět, jsou-li na něm přihlášeni a pracují-li s osobními údaji klientů, spolupracovníků či lektorů. V praxi se to však nedodržuje.

Pokud opouští všichni svou kancelář, měli by rovněž uzamknout dveře. I toto se ne vždy v praxi provádí. Zaměstnanci si mohou domů odnášet svůj pracovní notebook, kontrolovat na něm soukromé e-mailové adresy a nikdo nesleduje, jaké stránky navštěvují.

Lektoři nemají k dispozici žádný pracovní notebook, avšak každá učebna na čtvrtém patře je vybavena stolním počítačem. Z tohoto důvodu má každý lektor vlastní účet, pomocí kterého se mohou do sítě školy přihlásit. Lektoři by měli tyto počítače využívat pouze v průběhu hodiny pro výuku, avšak často se stává, že je lektoři v mezičasech během výuky využívají také pro soukromé účely. Historii těchto počítačů nikdo nesleduje a přístup není nikterak omezen.

Podnik B nemá svou síť propojenou s žádným dodavatelem, hrozba tedy směřuje na fungování podniku a jeho sítě a na jeho klienty. V posledním případě se jedná zejména o hrozbu krádeže a zneužití jejich osobních údajů a bankovních informací.

5.2.3 Etický hacking a ochrana

Podnik B sdílí na svých webových stránkách všechna jména lektorů, kteří u nich jazykové kurzy vyučují. Poskytují také detailní informace o svém sídle – co návštěvníci naleznou na prvním patře, co na čtvrtém, pracovní dobu, jak se do budovy dostat apod. Tyto informace např. kterémukoliv návštěvníkovi webu sdělí, že čtvrté patro je v průběhu celé pracovní doby odemčené. Toto je prvním problémem, který je etický hacker schopen zjistit bez jakýchkoliv informací pramenících přímo od podniku.

Dalším problémem je nízké zabezpečení na offline úrovni. Přestože jsou lektoři poučeni, že mají uzamknout učebnu po konci hodiny, není výjimkou, že se toto neděje. Zejména v průběhu pracovního dne, kdy lektoři předpokládají, že v učebně bude po patnácti minutách přestávky probíhat další hodina. Protože jsou hlavní vchodové dveře na patře odemčené, má kdokoliv přístup k počítači, který se v neuzamčené učebně nachází.

Jako poslední stojí za zmínku hrozby a ochrana pro samotnou počítačovou síť. Externí IT firma je zodpovědná pouze za náhlé technické potíže, nikoliv za automatickou kontrolu zabezpečí jako je firewall nebo antivirus. Pokud tedy uživatelé sami neaktualizují software, nikdo nekontroluje, zda je ochrana aktuální. Zároveň neexistují žádná školení a pravidla, jak se vyhnout riziku, např. otevření podezřelé přílohy v soukromém e-mailu apod. Za zmínku rovněž stojí to, že všichni zaměstnanci mají přístup do sdílených složek na disku. Kdokoliv z nich tedy může nalézt kontaktní informace lektorů či klientů, přestože s nimi není oprávněn pracovat. Určení a nastavení práv přístupu je tedy dalším krokem k zajištění

ochrany dat, se kterými podnik B pracuje. Podnik B byl zasažen scamwarem a pharming útoky. Právě v návaznosti na tyto útoky si podnik najal etického hackera, aby prověřil zabezpečení podnikové sítě a proškolil zaměstnance odpovědného za IT. Instalace a pravidelné aktualizace firewallu a antiviru pomohly odstranit některá rizika. Právě z tohoto důvodu představuje největší hrozbu selhání lidského faktoru.

5.3 Případová studie III

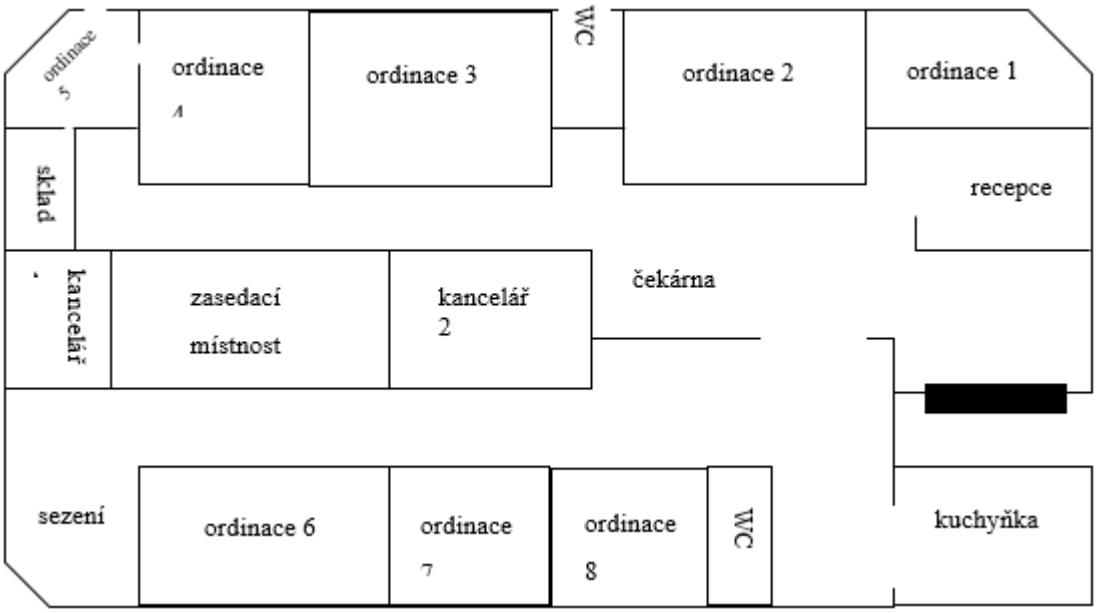
Třetí případová studie byla vytvořena pro psychologickou poradnu, jejíž situace představuje dle Tabulka 5 nejvyšší riziko právě proto, že tento podnik C zpracovává velké množství citlivých údajů o svých klientech.

5.3.1 Základní specifika podniku

Podnik C započal svou aktivitu v roce 2013 a jeho služby se zaměřují na konzultace v oblasti duševního zdraví. Podnik zaměstnává pouze pět osob, ostatní spolupracovníci pracují na živnostenský list. Z těchto pěti zaměstnanců je jedna ředitelka, dvě recepční a dva administrativní pracovníci. Jejich náplní práce je komunikovat s jednotlivými terapeuty ohledně prostorů, zařizovat skupinové akce či workshopy apod. Na živnostenský list spolupracují s podnikem C jednotliví terapeuti. Jich je celkem 25, jedná se jak o psychology, tak psychiatry. Někteří z nich pracují také v jiných organizacích či firmách nebo mají vlastní praxe. Jejich docházka do prostoru podniku C se tedy značně liší.

Podnik C sídlí ve třetím patře obytné budovy. V prvních dvou patrech jsou kanceláře, na zbývajících třech bytové jednotky. Hlavní vchod do budovy je neustále zamčený, je tedy nutné při příchodu zazvonit. Psychologická poradna je přístupná pouze jedněmi dveřmi, na které musí návštěvník zazvonit při vstupu do budovy. Hned za dveřmi se nachází malá recepce, kde pacient nahlásí, za kterým terapeutem přišel. Není tedy možné, aby se mezi ordinacemi pohyboval někdo neohlášený. Terapeuti musí rovněž zvonit, pouze dva z nich mají klíče od vstupních dveří. Ti jimi disponují, jelikož pracují každý den s pacienty podniku C. Plán prostor zachycuje Obrázek 11.

Jak je z plánku patrné, podnik C má k dispozici osm ordinací, zasedací místnost, kuchyňku, dvě WC a dvě kanceláře. Kancelář č. 1 je určena ředitelce, kancelář č. 2 administrativním pracovníkům. Ve skladu se uchovává jak např. káva, papír do tiskárny, propisky apod., tak informační materiály o poradně. Žádné citlivé informace o klientech či zaměstnancích v místnosti nejsou. Proto zůstává neustále odemčená.



Obrázek 11: Prostory podniku C

Zdroj: vlastní

Podnik C externě spolupracuje s IT, účetní a úklidovou firmou. Navazování a udržování této spolupráce spadá mezi úkoly ředitelky a v minulosti se nevyskytly žádné výrazné problémy či nedostatky.

V kanceláři ředitelky se nachází uzamčená skříňka, ve které jsou informace o zaměstnancích poradny a spolupracujících terapeutech. Tyto informace má ředitelka jak v papírové podobě ve zmíněné skříňce, tak ve složkách na svém počítači a na cloudovém úložišti. V kanceláři č. 2 jsou informace o klientech poradny, rovněž v uzamčené skříňce. Tyto informace jsou:

- jméno a příjmení,
- adresa trvalého bydliště,
- kontaktní adresa (pokud se liší od adresy trvalého bydliště),
- e-mailová adresa,
- telefonní číslo,
- zdravotní pojišťovna,
- zaměstnání,
- diagnóza (pokud relevantní),
- prvotní důvod návštěvy poradny,
- terapeuty/terapeuti, které navštěvuje,
- medikace (pokud relevantní).

Již na první pohled je patrné, že se jedná o citlivé osobní údaje. Psychologická poradna má celkem 214 klientů včetně dětských pacientů. Pokud má klient o návštěvu poradny zájem, vyplní online formulář, kde uvede své jméno, kontaktní informace a základní důvod návštěvy. Tyto důvody jsou přednastaveny ve formuláři tak, aby odpovídaly profilaci terapeutů, ale nevyžadovaly detailní informace potenciálních klientů. Tyto formuláře zpracovávají administrativní pracovníci a hledají danému zájemci vhodného terapeuta. Následně zjišťují, zda má poradna ještě volnou kapacitu a kdy je nejbližší možný volný termín pro klienta. S těmito informacemi zavolají zájemci zpět a domluví první návštěvu. Na ní je vyplněný vstupní formulář, kde klient uvádí detailnější informace (viz výčet výše) a podepisuje, že souhlasí se zpracováním osobních údajů.

Následující schůzky si již klient domlouvá přímo s terapeutem. Ten má k dispozici termíny podle svého rozvrhu, který sestavil pro podnik C v souladu s kapacitami jednotlivých ordinací (čili místností). Tento rozvrh je k dispozici na recepci (pouze po dotázání, není viditelný a veřejně přístupný). Recepční dostává k dispozici pouze termíny a jména terapeuta a klienta. Jméno klienta je jí sděleno proto, aby mohla posoudit, zda příchozí člověk má skutečně sjednanou schůzku a může ho vpustit dovnitř.

5.3.2 Počítačová síť a hrozby

Jak vyplývá z předchozí podkapitoly, počítačová síť má pro fungování podniku C klíčovou roli. Bez funkčního webového formuláře mohou klienti zavolat na recepci, avšak toto fungování poradny komplikuje. V minulosti se několikrát vyskytly problémy s formulářem, vždy však byly rychle odstraněny.

V podniku C se nachází celkem dvanáct počítačů – v ordinacích, na recepci, v kanceláři ředitelky a dva v kanceláři administrativních pracovníků. Počítače v ordinacích slouží terapeutům. Ti si během sezení s klienty dělají poznámky, které mají dovoleno psát pouze na papír. Po skončení sezení je přepisují do souboru na počítači. Každá ordinace je vybavena jedním stolním počítačem a každý terapeut má k dispozici vlastní účet, ke kterému se přihlašuje. V každé ordinaci je také skartovačka, kterou musí terapeuti použít pro likvidaci papírových poznámek. Přístup k poznámkám mají terapeuti pouze v prostoru podniku C, nikoliv např. z domova (ani pomocí VPN). K poznámkám terapeutů nemají přístup administrativní pracovníci ani recepční, pouze ředitelka. To je z důvodu, kdyby terapeut náhle ukončil spolupráci a klient přecházel k někomu jinému.

Ředitelka i administrativní pracovníci mají k dispozici pracovní notebook, který si mohou odnést domů. Platí však přísná pravidla, že na něm nesmějí pracovat na veřejných místech.

Výjimkou jsou školení či semináře, během kterých však nesmí otevírat např. informace z webových formulářů potenciálních klientů. Administrativní pracovníci i recepční jsou proškoleni, že nesmí počítač opouštět, pokud jsou na něj přihlášení.

Jak je patrné z popisu, podnik C eliminoval hrozby offline útoku (přístup nepovolané osoby k počítačům) na minimum. Stále však čelí nebezpečí napadení sítě, což by mohlo mít fatální dopad na fungování poradny a životy jejích klientů. Zaměstnanci jsou poučeni, že nemají otevírat neznámé přílohy v e-mailech či navštěvovat podezřelé webové stránky.

5.3.3 Etický hacking a ochrana

Podnik C spolupracuje na správě svých informačních sítí s externí společností. K tomuto kroku se rozhodla právě proto, že zpracovává citlivé osobní údaje ve velkém rozsahu a vyhodnotila, že spolupráce s odborníky bude jednou z cest, jak eliminovat hrozby krádeže či napadení jejích dat. Právě ta podnik C upozornila na nutnost odstranění citlivých osobních údajů z cloudového uložiště, které bylo spravováno externím subjektem.

Přesto je klíčové sledovat, zda se toto tvrzení odráží v realitě. Podnik C by neměl nabýt dojmu, že není důležité monitorovat, zda jsou bezpečnostní prvky správně aktualizovány a zda odpovídají jejím potřebám.

6 VYHODNOCENÍ

Při pohledu na hrozby, které podnikům A, B a C hrozí, je patrné, že se v mnohých případech překrývají. Všechny podniky čelí rizikům spojeným se spoofingem, phishingem, pharmingem, adwarem, spywarem, trojským koněm, virem, červem i spamem. Přesto zde existují určité rozdíly. V případě spoofing a phishing útoků je podnik B více v ohrožení proto, že zpracovává údaje o bankovním spojení a kreditních kartách svých klientů. Pharming útoky, které se soustředí na manipulaci s provozem webových stránek, představují hrozbu pro všechny podniky, avšak od každého z nich mohou hackeři ukrást jinak citlivá data.

Právě rozdíl v potenciální škodě je to, co odlišuje podniky A, B a C a něco, co vyžaduje speciální pozornost etických hackerů. Podnik B a podnik C čelí větším rizikům v případě úniku a zneužití dat, jelikož zpracovávají citlivé údaje svých zákazníků. Podnik C by se mohl stát cílem ransomwaru, jelikož „zajmutí“ údajů o zdravotním stavu klientů představuje situaci, ve které by podnik určitě zvažoval zaplacení výkupného za znovunabytí přístupu k těmto datům. Naopak Man in the middle představuje hrozbu pouze pro podniky A a B, u kterých dochází k častější výměně informací mezi podnikem a jeho klienty či dodavateli.

Etický hacking představuje pro všechny podniky účinnou metodu, jak otestovat vlastní zabezpečení a zjistit, kde má v současnosti slabiny. Všechny podniky využívají základní zabezpečení, jako firewall a antivirus. Etický hacker má však nástroje na to, aby systém prozkoumal detailněji, případně také zaměstnance všech zmíněných podniků vzdělal v otázce kybernetické bezpečnosti.

Případové studie se také detailně soustředily na sociální inženýrství a hrozby, které pro data podniků A, B a C leží v offline prostředí. Sociální inženýrství operuje se selháním lidského faktoru. Případové studie ukazují, že síť zkoumaných podniků může být v ohrožení navzdory tomu, jak jsou jejich systémy zabezpečeny, pokud selže některý z pracovníků. Právě toto je důležitou oblastí, kterou je nezbytné analyzovat v průběhu hodnocení zabezpečení podniků a při tvorbě návrhů, jak identifikované nedostatky odstranit.

6.1 Prevence

Hlavním úkolem, který můžeme maximálně eliminovat následky případného útoku je bezpečnostní politika a prevence. Je tedy na místě přijetí opatření minimalizujících nebezpečí průniku do systému.

Cíle hackingu můžeme rozdělit na (Thomas, 2005):

- *příležitostný* – systém, v němž útočník v podstatě náhodou odhalil zranitelné místo a pokusí se o jeho zneužití,
- *záměrně zvolený cíl* - systém, který si útočník vybral za svou oběť úmyslně. Motiv volby není podstatný. Důležité je jeho cílené odhodlání k útoku.

Hacker, který je zdatný v metodách sociálního inženýrství, vezme drobnou informaci a s pomocí dalšího snadno získaného údaje se prolomí o úroveň výš. Příkladem může být následující případ: pokud zná hacker kromě osobního čísla také úplné jméno zaměstnance, telefonní linku, oddělení, přesné místo pracoviště, e-mail a dokonce i jméno nadřízeného. Každá z těchto informací vypadá sama o sobě zdánlivě nevinně, ale dohromady tvoří nebezpečně přesnou mozaiku (Thomas, 2005).

Tyto "nevinné" informace je třeba chránit. Zaměstnanci musí také vědět, že nesprávné zacházení s takovýmito interními údaji může skutečně vážně ohrozit společnost a nakonec i samotného zaměstnance. Veškeré firemní údaje je potřeba považovat za citlivé a nesmí se nikomu prozrazovat, s výjimkou výslovného povolení (např. Zásady klasifikace dat či podobný dokument) (Thomas, 2005).

Přirozeně se můžeme domnívat, že samy bezpečnostní technologie nás před zlomyslnými cíli hackerů dokáží ochránit. V takovém případě chápeme význam bezpečnosti jen částečně, protože jsme zapomněli na ten nejslabší článek řetězu: *lidský faktor*. Skutečná bezpečnost nelze koupit v nějakém jednom produktu. Je to celá řada procesů, do nichž jsou kromě produktů zapojeni také zaměstnanci organizace (Thomas, 2005).

Žádný počítačový systém není a nikdy nebude zcela bezpečný. Lze je ovšem zabezpečit dostatečně se zřetelem k účelu, k němuž se používá (Thomas, 2005). Toto zabezpečení vyžaduje prostředky:

- technické,
- programové,
- finanční,
- lidské,
- i organizační.

Typy dat, které se se dají zneužít

- osobní údaje – např. poštovní adresa, telefonní číslo, datum narození,
- finanční údaje – např. software pro správu osobních financí,
- data o zákaznících,
- zdravotní údaje.

Pokud se hacker dostane do sítě má v rukou tyto možnosti (Thomas, 2005):

- *Servery* – zařízení, které může hacker ovládat a ze kterého může na dálku spouštět útoky proti jiným, důležitějším cílům.
- *Pevné disky* – může sloužit jako odkladiště pochybného nebo nezákonného obsahu
- *Připojení k Internetu* – může sloužit jako alternativní prostředek pro napojení do jiných firem a vedení útoků proti nim.
- *Osobní informace o zaměstnancích* – informace, které zaměstnavatel potřebuje shromažďovat o svých zaměstnancích (např. výplaty) může hacker snadno odcizit.

6.2 Návrh řešení

Níže jsou uvedeny hlavní body řešení.

Návrh na zajištění bezpečnosti

- Zaměstnanci jsou pravidelně proškolováni a souhlasí s ochranou informací.
- Zaměstnanci jsou odpovědní za řádné používání počítačových prostředků a mají přístupné pouze informace, které potřebují k výkonu práce.
- Stejně tak klient má přístup jen k informacím, které potřebuje.
- Zaměstnanec je povinen ochránit zařízení firmy, pokud je ponecháno bez dozoru a to tak, že opouští-li počítač (či zařízení podobného charakteru) musí se z něho odhlásit nebo ho uzamknout. Toto provádí i po konci pracovní doby.
- Citlivé informace týkající se firmy, zaměstnanců nebo klientů včetně počítačových prostředků, které se nepoužívají, musí být bezpečně uschovány či zabezpečeny proti přístupu a manipulaci (a to i při ochodu z pracoviště).
- Počítače ponechané v prostorech firmy mají zašifrovaná data, která jsou dostupná pouze danému uživatelskému účtu, ten je zabezpečen silným heslem.
- Pro připojení pracovního zařízení z domu do firemní sítě je využíváno připojení skrze VPN (pokud je dovoleno připojení do sítě).
- Cizí zařízení se do firemní sítě nepřipojuje, je možné používat jen zařízení, které je kontrolováno firmou.
- HW i SW je využíván pouze pro firemní, nikoli soukromé účely.
- Je dovoleno používat licencovaný, originální a schválený SW, žádný WAREZ, zároveň se používá k účelu, ke kterému byl pořízen.
- Návštěvy pohybující se v oblasti citlivých informací podléhají schválení pověřenou osobou, evidují se v knize návštěv a pohybují se ve firmě s doprovodem.
- Každý zaměstnanec má vlastní uživatelský účet zabezpečený heslem. Přístupové údaje nikomu nesděluje, ani nejsou vyvěšeny na viditelném místě. Výjimkou je evidence v zapečetěné obálce v trezoru, která se otevírá při krizových situacích.
- Zaměstnanec heslo mění v pravidelných časových intervalech. Jeho délka musí být alespoň 8 znaků a volí se tak, aby nebylo snadno odvoditelné. Nevhodné je vlastní jméno a příjmení, jméno partnera, dětí, data narození, rodné číslo.
- Přístupový kód (heslo) se mění, jakmile dojde k jeho prozrazení nebo náznaku prozrazení.

- Hesla nesmí být uložena v prohlížeči či jiném automatickém nástroji pro přihlašování.
- Uživatel je odpovědný za činy realizované jeho účtem.
- Firemní email nesmí být používán k vyřizování soukromé korespondence.
- Zaměstnanec je povinen dodržovat nařízení týkající se zasílání a přijímaní povolených typů příloh, stahování jakýchkoliv neznámých aplikací nebo samospustitelných souborů, navštěvování nepovolených či rizikových WWW stránek a podobně. Zvláštní nebezpečí představují spustitelné programy (zejména, ale ne výlučně se jedná o koncovky *.exe, *.com a *.bat). Důležité je dávat si pozor nad používáním tzv. dvou přípon souboru. Skutečná přípona je ta, která je zcela na konci souboru (tj. soubor „obrazek.jpg.exe“ není obrázek, ale program, a to s největší pravděpodobností virus).
- Neotevírání souborů přiložených k e-mailům či v jiné online komunikaci od neznámých osob.
- Výběr a implementace vhodných technických opatření – např. zavedení přístupových karet, omezení přístupu uživatelů k datům podle jejich skutečných potřeb a stupně důležitosti dat, nastavení práv uživatelů komunikujících prostřednictvím Internetu, antivirové kontroly, filtrování veškeré komunikace směřující dovnitř i ven z vnitřní sítě a podobně pomocí firewallu či proxyserveru. Zabezpečení fyzické ochrany výpočetní techniky a dat (v odůvodněných případech to muže znamenat i náležité stavební úpravy, kvalitní dveře s bezpečnostním zámkem, bezpečnostní fólie a mříže na oknech, poplachové zařízení atd.).
- Ustanovení bezpečnostních předpisů a bezpečnostní politiky.
- Použití ochrany napájení a záložních zdrojů.
- Pravidelné zálohování dat a systémů.
- Kontrola aktualizací a instalace záplat v celém programovém vybavení.
- Nastavení šifrování dat na disku a používání šifrované/zabezpečené (pomocí SSL) komunikace v síti.
- Používání monitoringu činností a ukládání jejich výstupů do logů.
- Vyhnutí se bezdůvodnému sdělování jakýchkoliv zneužitelných informací v online i offline (adresa, telefon, kreditní karta, email, heslo a podobně).
- Nezapojování se do jakýchkoliv nelegálních dění na Internetu (stahování nelegálního software, videa, hudby a podobně).

- Externí zdroje jako (e-mail, CD-ROM, DVD, USB média) jsou kontrolované antivirovým programem. Kontrolován je též i celý disk počítačových systémů a prostředků.
- Nepouštění osob k počítači, které nechtějí dodržovat bezpečnostní pravidla (to platí i o vlastních příbuzných).

Navrhované řešení bezpečného provozu systému:

- přijmutí takových opatření, která co nejvíce omezí možnost útoku na počítačový systém,
- testování přijatých opatření a použitých technologií,
- detekce průniku nebo počátečních přípravných aktivit směřujících k průniku do systému a maximální využití nástrojů, které jsou k tomu určeny /přijmout okamžitá opatření vedoucí ke zvýšení bezpečnosti ohrožené části systému nebo eliminaci útočníka,
- vyšetřování průniku, shromažďování důkazů a odstraňování vzniklých škod.

Opatření minimalizující nebezpeční průniku do systému:

- *identifikace a autentizace* uživatele – funkce k sestavení relace s uživatelem (ověření identity i v případě, kdy se neověřuje identita uživatele, ale oprávněnost a identita procesu vyžadujícího relaci),
- *řízení přístupu* – řízení toků dat mezi procesy, objekty nebo uživateli (používání kategorií přístupových práv, jejich ověřování a administraci),
- *revize přístupů* – sledování a zaznamenávání pokusů, které mají vyzkoušet přístupová práva a ověřit relevantní bezpečnostní akce,
- *opakovaný přístup k objektům* – speciální funkce systému sledující prostřednictvím řízení přístupu k datovým objektům, jak, kým nebo kdy jsou tyto objekty používány, zejména pokud se jedná o opakované použití téhož datového objektu,
- *preciznost a přesnost* – postup zaměřený na korektnost a konzistenci relevantních bezpečnostních informací
- *spolehlivost služby* – bezpečný přenos dat komunikačním prostředím.

Příloha E definuje úkony pro posouzení bezpečnosti a průniků do systému.

Příloha F obsahuje doporučená nastavení pro jednotlivé komponenty systému a systém jako takový.

ZÁVĚR

Aby bylo možné jakékoliv chyby správně a efektivně odstranit, je nejprve nezbytné je znát. Právě toto poznání umožňuje etický hacking. Výhodou jeho nástrojů je to, že podnik reálně čelí útokům, avšak místo toho, aby byl poškozen, se učí, jak zlepšovat své procesy a operace.

Tato bakalářská práce se zaměřila na etický hacking a přínos, který podnikům nabízí. Cílem práce bylo demonstrovat, jaké hrozby podnikům hrozí, jak se jim lze ubránit a jakou roli v tomto procesu hraje etický hacking a sociální inženýrství. Zjištění role sociálního inženýrství lze označit za přidružený cíl práce, jelikož žádný systém, se kterým pracují lidé, není možné plně zabezpečit, pokud nejsou právě lidé zahrnuti jako významný faktor.

V rámci práce byly představeny tři případové studie, které byly vytvořeny pro e-shop, jazykovou školu a psychologickou poradnu. Všechny tyto podniky operují na odlišných trzích, zpracovávají jiná data a v jiném rozsahu. Jejich společným faktorem je to, že mohou čelit kybernetickým útokům, které mohou být vedeny jak v online, tak v offline prostředí. Autor na nich demonstroval, že ačkoliv jsou podniky rozdílné, všechny mohou profitovat z etického hackingu a sociálního inženýrství. Toto je důležité zjištění z několika důvodů. Vytvořené podniky nebyly mezinárodní korporace, jejich primárním zaměřením nebylo IT. Proto by se na první pohled mohlo zdát, že etický hacking není správným nástrojem pro zajištění jejich bezpečnosti. A zároveň byla vyzdvihnuta role lidského faktoru a vliv, jaký mají uživatelé na bezpečnost dat, se kterými pracují. Na jejich roli by podniky nikdy neměly zapomínat a měly by dbát o řádné proškolení svých zaměstnanců včetně toho, jak správně zacházet a zabezpečit hardware.

POUŽITÁ LITERATURA

ALZAHRANI, Abdulrahman, et al. An overview of ransomware in the windows platform. In: *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2017. p. 612-617.

BRABLEC, Martin, 2021 [online]. Jak psát případové studie: postupy, osvědčené otázky. Obsahová agentura. [cit. 2021-03-01]. Dostupné z https://www.obsahova-agentura.cz/blog/jak-psat-pripadove-studie

CZECH INVEST, n.d.. [online]. Definice malého a středního podnikatele. Czech Invest. [cit. 2021-03-01]. Dostupné z https://www.czechinvest.org/cz/Sluzby-pro-male-a-stredni-podnikatele/Chcete-dotace/OPPI/Radce/Definice-maleho-a-stredniho-podnikatele

DENIS, Matthew; ZENA, Carlos; HAYAJNEH, Thaier. Penetration testing: Concepts, attack methods, and defense strategies. In: *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2016. p. 1-6.

ENDORF, Carl F. *Detekce a prevence počítačového útoku*. Grada publishing as, 2005.

ESET, n.d. [online]. Antivirus. ESET. [cit. 2021-03-01]. Dostupné z https://www.eset.com/cz/antivirus-software/

FAILY, Shamal. Ethical hacking assessment as a vehicle for undergraduate cyber-security education. 2014.

GENÇ, Ziya Alper; LENZINI, Gabriele; SGANDURRA, Daniele. Cut-and-Mouse and Ghost Control: Exploiting Antivirus Software with Synthesized Inputs. *Digital Threats: Research and Practice*, 2021, 2.1: 1-23.

GREGR, Filip. Penetrační testy a odhalování zranitelností síťových prvků. 2015. Ústav telekomunikací.

HARRIS, Shon. *Hacking: manuál hackera*. Praha: Grada, 2008. ISBN 978-80-247-1346-5.

HORALEK, Josef, et al. Analysis of the use of Rainbow Tables to break hash. *Journal of Intelligent & Fuzzy Systems*, 2017, 32.2: 1523-1534.

ILINČEV, Ondřej, n.d. [online]. Jak napsat případovou studii (včetně příkladů). Ilinčev. [cit. 2021-03-01]. Dostupné z https://www.ilincev.com/pripadova-studie

IWANT, n.d.. [online]. Operační systém. iWant. [cit. 2021-03-01]. Dostupné z https://www.iwant.cz/Slovnik/operacni-system-a18

JANÁK, David, 2002. [online]. Historie operačních systémů Windows a Unix. MUNI. [cit. 2021-03-01]. Dostupné z https://www.fi.muni.cz/usr/jkucera/pv109/2002/xjanak_tisk.html

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

JELIČ, Pavel, 2021. [online]. Jak chránit Mac před napadením hackery: 5 tipů, které musíte znát. Jablíčkář. [cit. 2021-03-01]. Dostupné z https://jablickar.cz/jak-chranit-mac-pred-napadenim-hackery-5-tipu-ktere-musite-znat/

KASPERSKY, n.d. [online]. What is a Brute Force Attack? Kaspersky. [cit. 2021-03-01]. Dostupné z https://www.kaspersky.com/resource-center/definitions/brute-force-attack

KASPERSKY, n.d. [online]. What is Pharming & How to Prevent it? Kaspersky. [cit. 2021-03-01]. Dostupné z https://www.kaspersky.com/resource-center/definitions/pharming

KASPERSKY, n.d. [online]. What is a Replay Attack? Kaspersky. [cit. 2021-03-01]. Dostupné z https://www.kaspersky.com/resource-center/definitions/replay-attack

KASPERSKY, n.d. [online]. What is Spear Phishing? Kaspersky. [cit. 2021-03-01]. Dostupné z https://www.kaspersky.com/resource-center/definitions/spear-phishing

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

KOVALČÍK, Marek. 2020 [online]. Etický hacking – laicky a jednoduše. BDO Česká republika. [cit. 2021-03-01]. Dostupné z https://www.bdo.cz/cs-cz/blog/it-security/12-2020/eticky-hacking-–-laicky-a-jednoduse

LINUX EXPRES, n.d.. [online]. Co je Linux?. Linux Expres. [cit. 2021-03-01]. Dostupné z https://www.linuxexpres.cz/co-je-linux

LINUX, n.d.. [online]. Výhody operačního systému Linux. Linux. [cit. 2021-03-01]. Dostupné z https://proc.linux.cz/proc/

MALLIK, Avijit. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2019, 2.2: 109-134.

MANAGEMENT MANIA. 2015 [online]. Spoofing. Management Mania. [cit. 2021-03-01]. Dostupné z https://managementmania.com/cs/spoofing

MAREŠ, Jiří. Tvorba případových studií pro výzkumné účely. *Pedagogika*, 2015, 65.2: 113-142.

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

MICROSOFT, n.d. [online]. Na Windows 10 se můžete spolehnout. Microsoft. [cit. 2021-03-01]. Dostupné z https://www.microsoft.com/cs-cz/windows

NAYAK, Gopi Nath; SAMADDAR, Shefalika Ghosh. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In: *2010 3rd International Conference on Computer Science and Information Technology*. IEEE, 2010. p. 491-495.

PLAŠIL, PRÁCE Bc MATOUŠ. Soubor laboratorních úloh k demonstraci počítačových útoků. 2015.

ROUBAL, Jan; ČEVELÍČEK, Michal; ŘIHÁČEK, Tomáš. Jak jednoduše provést a napsat případovou studii: Vodítka pro psychoterapeuty v praxi. *Psychoterapie*, 2019, 13.1.

SAHARE, Bhawana; NAIK, Ankit; KHANDEY, Shashikala. Study of ethical hacking. *Int. J. Comput. Sci. Trends Technol*, 2014, 2.4: 6-10.

SCAMBRAY, Joel; SHEMA, Mike. *Hacking bez tajemství: webové aplikace*. Computer Press, 2003.

TECHSLANG, n.d. [online]. What is a Rainbow Table Attack? Techslang. [cit. 2021-03-01]. Dostupné z https://www.techslang.com/definition/what-is-a-rainbow-table-attack/

THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.

Trend Micro: Exploit Kit [online]. [cit. 2021-4-5]. Dostupné z: https://www.trendmicro.com/vinfo/za-en/security/definition/exploit-kit

VOHANKOVÁ, Alena, 2020 [online]. Co je to virus, jak se šíří a k čemu je antivirus? AVAST. [cit. 2021-03-01]. Dostupné z https://www.avast.com/cz/besafeonline/blog/co-je-to-virus-jak-se-siri-a-k-cemu-je-antivirus

PŘÍLOHY

PŘÍLOHA A – TYPICKÉ HROZBY

Hrozba	**Popis**
Porušení autorizace	Osoba, která je autorizována k použití zdroje pro jistý účel jej použije k jinému, neautorizovanému účelu.
Obejití řízení	Útočník využije bezpečnostních mezer v systému nebo jeho slabin.
Potlačení služby	Omezení legitimního přístupu k informacím nebo jiným zdrojům v síti.
Nezákonný odposlech	Informace je získávána monitorováním přenosového kanálu.
Emisní nebo VF (vysokofrekvenční) odposlech	Informace je extrahována z vysokofrekvenčního vyzařování nebo emisí či jiných elektromagnetických jevů, ke kterým dochází při provozu elektronického zařízení.
Nelegitimní použití	Zdroj je používán neautorizovanou osobou nebo neautorizovaným způsobem.
Indiskrece	Autorizovaná osoba prozradí důvěrnou informaci neautorizované osobě z neopatrnosti nebo za úplatu.
Únik informace	Získání důvěrné informace neautorizovanou osobou.
Narušení integrity	Konzistence dat je narušena jejich neautorizovaným vytvořením, úpravou nebo vymazáním.
Změna dat při přenosu	Přenášená data jsou během přenosu informačním kanálem změněna, odstraněna nebo zcela vyměněna.
Maškaráda	Jedna entita (osoba nebo systém) se představuje jako jiná entita.
Vytěžení odpadových médií	Informace je získávána z magnetických nebo papírových médií, vyhozených do odpadu.
Fyzický průnik	Útočník získá kontrolu nad systémem proniknutím k jeho ovládacím prvkům.
Replay	Zachycená kopie legitimní transakce je využita pro opětovný přenos s nelegitimním úmyslem.
Popření skutečnosti	Strana zúčastněná ve vzájemné komunikaci později popře, že k takové komunikaci došlo.
Vyčerpání zdrojů	Jistý zdroj, např. port je úmyslně natolik zatížen, že je znemožněno používání služby, která je na něj vázána, řádnými uživateli.
Podvržení služby	Podvržený systém nebo systémová komponenta, které se vůči uživateli chovají jako běžná součást systému, slouží k získání citlivých informací od důvěřivého uživatele.
Krádež	Kritický prvek bezpečnostního systému (např. přístupová karta) nebo veškeré citlivé informace jsou zcizeny.
Analýza provozu	Informace je neautorizovanou entitou získána pomocí sledování provozu a výběrem jeho podstatných částí.
Zadní vrátka	Do systému je zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismy.
Trojský kůň	Software obsahuje zdánlivě nevinnou nebo neviditelnou část kódu, která – pakliže je spuštěn – ohrozí bezpečnost uživatele.

Zdroj: Jirovský, 2007

PŘÍLOHA B – TERMINOLOGIE PŘÍPADOVÝCH STUDIÍ

Anglický termín	**Český termín**	**Poznámky**
case	případ	obsah i rozsah tohoto termínu je velmi široký
single case	jeden případ	
individual case	individuální případ	
unique case	unikátní případ	
extreme case	extrémní případ	
critical case	kritický případ, zásadní případ, krizový případ	
typical case	typický případ	
collective case	kolektivní případ	zahrnuje více než jeden případ, přičemž jeho jednotky mohou, ale nemusí být situovány na jednom místě
case study	případová studie	v lékařských oborech a v klinické psychologii se používá termín *kazuistika*
single-case study, single case study	jednopřípadová studie	
multiple cases	mnohočetné případy	
multiple-case study	mnohonásobná případová studie, mnohopřípadová studie, vícečetná případová studie, vícepřípadová studie	česká terminologie není ještě ustálena
exploratory case study	exploratorní (průzkumná) případová studie	
explanatory case study	explanační (vysvětlující) případová studie	někdy se používá též termín *causal case study*
pilot case study	pilotní případová studie	
evidence-based case report	*kazuistika* založená na důkazu	termín se používá v medicíně
intrinsic case study	intrinsitní případová studie	představuje snahu o holistické porozumění unikátnímu případu
instrumental case study	instrumentální případová studie	nejprve se volí jev, potom se vyhledají případy, které tento jev reprezentují, a ty se nakonec podrobněji prozkoumají
collective case study	kolektivní případová studie	hloubkové zkoumání více případů
multiple site case study (zkráceně MultiSite case study)	studie rozdílně lokalizovaných případů	
teaching case study	výuková případová studie	

Zdroj: Mareš, 2015

PŘÍLOHA C – KYBERNETICKÁ TRESTNÁ ČINNOST V MEZINÁRODNÍCH DOKUMENTECH

Mezinárodní dokumenty zabývající se kybernetickou trestnou činností a hackingem (Kolouch, 2016):

- Manuál OSN o prevenci a kontrole trestných činů spojených s počítači
- Úmluva Rady Evropy č. 185 o kyberkriminalitě
- Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě
- Dokumenty EU/ES sloužící k harmonizaci právních úprav při potírání kybernetické trestné činnosti:
    - Směrnice Rady 91/250/EHS o právní ochraně počítačových programů
    - Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů
    - Směrnice Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES
    - Směrnice č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)
    - Rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu
    - Rámcové rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků
    - Směrnice Evropského parlamentu a Rady č. 2002/21/EC o společném regulačním rámci pro sítě a služby elektronických komunikací (rámcová směrnice)
    - Směrnice Evropského parlamentu a Rady č. 2002/19/EC o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice)
    - Směrnice Evropského parlamentu a Rady č. 2002/20/EC o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice)
    - Směrnice Evropského parlamentu a Rady č. 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě)

- Směrnice Evropského parlamentu a Rady 2002/58/EC týkající se zpracovávání osobních údajů a ochrany soukromí v oblasti elektronických komunikací (směrnice o ochraně údajů v elektronických komunikacích)
- Směrnice Komise č. 2002/77/ES o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami (soutěžní směrnice)
- Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy
- Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) ze dne 15. 11. 2006
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007
- Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti ze dne 27. listopadu 2008
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“ ze dne 30. 3. 2009
- Sdělení komise Radě a Evropskému parlamentu, Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě. 2012
- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013, o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004, ze dne 21. května 2013
- Směrnice Evropského parlamentu a Rady 2013/40/EU, o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, ze dne 12. srpna 2013

- Nařízení Evropského parlamentu a Rady (EU) č. 513/2014, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nástroj pro finanční podporu policejní spolupráce, předcházení trestné činnosti, boje proti trestné činnosti a řešení krizí a zrušuje rozhodnutí Rady 2007/125/SVV, ze dne 16. dubna 2014
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ze dne 23. července 2014
- Nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. května 2016
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, ze dne 6. července 2016 (NIS Directive)

PŘÍLOHA D – PRÁVNÍ NORMY ČR VZTAHUJÍCÍ SE KE KYBERNALITĚ A HACKINGU

Právní normy České republiky tykající se kybernality a hackingu (Kolouch, 2016):

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

PŘÍLOHA E – POSUZOVÁNÍ BEZPEČNOSTI A TESTOVÁNÍ PRŮNIKU

Posuzování zranitelných míst a možnosti průniku do sítí a systémů, upraveno podle Thomas (2005):

- **Posouzení zranitelných míst a možností průniku zevnitř (penetrační testy)**
    - Zjištění základních informací o síti.
    - Zjištění a zaznamenání všech veřejně dostupných informací o firemní síti – ujasnění toho, co všechno se může útočník zcela legálně dozvědět.
    - Pomocí technik mapování sítě zjistit topologii a fyzické rozložení sítě.
    - Provést zkoumání a prohledávání síťových aplikací.
    - Provést detekci otisku operačních systémů a zranitelných míst a odhalit tak zranitelné systémy.
    - Charakterizovat vzorky síťového provozu a datových toků, které dále porovnáme s očekáváným profilem normálního provozu.
    - Detekovat veškeré potencionálně slabé systémy zabezpečení uživatelů (například uživatelé, kteří si nikdy nemění heslo; nezabezpečené bezdrátové sítě).
    - Analýza zranitelných míst pomocí veřejných, privátních i vlastních nástrojů.
    - Ruční kontrola všech zjištěných (automaticky detekovaných) zranitelných míst a vyloučení falešných poplachů.
    - Pozorování praxe v oblasti vnitřních bezpečnostních postupů.
    - Analýza jištěných skutečností a podrobná zpráva s dalšími doporučeními.

- **Posouzení zranitelných míst a možností průniku zvenčí (penetrační testy)**
    - Zjištění základních informací o síti.
    - Zjištění a zaznamenání všech veřejně dostupných informací o firemní síti – ujasnění toho, co se může útočník zcela legálně dozvědět.
    - Pomocí technik neviditelného mapování sítě zjistit topologii a fyzické rozložení sítě – ověřit, zda je možné v síti detekovat tyto simulované útoky.
    - Provést zkoumání a prohledávání sítových aplikací.
    - Podle potřeby vyzkoušet metody průchodu firewallem, násilného vytáčení (war dialing) a „nájezdu“ (war driving).
    - Provést detekci otisku operačních systémů a zranitelných míst a odhalit tak zranitelné systémy.
    - Charakterizovat vzorky síťového provozu a datových toků, které dále porovnáme s očekávaným profilem normálního provozu.
    - Detekovat veškeré potenciálně slabé systémy zabezpečení uživatelů (například uživatelé, kteří si nikdy nemění heslo; nezabezpečené bezdrátové sítě).
    - Analýza zranitelných míst pomocí veřejných privátních i vlastních nástrojů.
    - Ruční kontrola všech zjištěných (automaticky detekovaných) zranitelných míst a vyloučení falešných poplachů.
    - Analýza zjištěných skutečností a podrobná zpráva s dalšími doporučeními.

- **Posouzení fyzické bezpečnosti**
    - Pozorování a kontrola míst možného vstupu do budovy zvenčí a kontrola činností „strážců“.
    - Kontrola technických systémů fyzického střežení, (např. prokazování pracovníků při vstupu, zapisování návštěvníků).
    - Kontrola mechanismů fyzické ochrany informačních prostředků, ale i papírových dokumentů.
    - Zjištění rozsahu fyzických prostředků pro ochranu počítačového vybavení, (například omezení přístupu k počítačovému prostředí, záložní napájecí zdroje a chráněné kanály pro datovou komunikaci).
    - Pozorování zažitých zvyklostí pracovníků s ohledem na fyzickou bezpečnost.
    - Pozorování metod fyzické likvidace kriticky důležitých dat, např. s tím související prohledávání odpadků.
    - Doporučení pro další zabezpečení informačních prostředků před fyzickými útoky.
    - Kontrola postupů pro zálohování a ukládání kriticky důležitých dat.
    - Přezkoumání zásad pro vstup firemních dodavatelů a cizích návštěvníků do budovy a kontrola zacházení s neznámými jednotlivci.

PŘÍLOHA F – DOPORUČENÁ NASTAVENÍ

Síť
Firewall, screening router nebo jiné filtrující zařízení je zřízeno mezi webovou aplikací a nedůvěryhodnými sítěmi
Firewall/směrovač je nakonfigurován tak, aby směrem dovnitř k webové aplikaci dovoloval jen nezbytnou komunikaci (typicky pouze HTTP a/nebo SSL).
Firewall/směrovač je nakonfigurován tak, aby směrem ven od webové aplikace dovoloval jen nezbytnou komunikaci (typicky jsou blokovány pakety TCP SYN, aby se serverům zabránilo v navazování spojení směrem ven).
Na firewallu/bráně jsou aktivována příslušná opatření proti odepření služby DoS, například příkaz Cisco "rate limit“.
Zařízení pro rozložení zátěže jsou nakonfigurována tak, aby neprozrazovala informace o interních sítích.
Pro detekci běžných útoků přes TCP/IP může být případně implementován systém detekce sítových útoků (Network Intrusion Detection Systém - NIDS). V tom případě by měly být k dispozici zásady a zdroje pro kontrolu záznamů.
Pravidelně je prováděno skenování slabých míst sítě, aby se zajistilo, že neexistují žádná slabá místa na úrovni sítě nebo počítačů.
Webový server
Jsou instalovány nejaktuálnější opravy od výrobce.
Servery jsou nakonfigurovány tak, aby neprozrazovaly informace o softwaru (například je změna informace v titulku).
Servery jsou nakonfigurovány tak, aby nepovolily reverzní proxy.
Jsou zakázány síťové služby, které nejsou nezbytné.
Bezpečnostní nastavení závislá na výrobci jsou implementována tam, kde to připadá v úvahu.
Účty uživatelů a skupin, které nejsou nezbytné (např. účet Host), jsou zakázány nebo zrušeny.
Audit v operačním systém je povolen, stejně jako záznamy webového serveru ve formátu W3C.
Nepotřebné moduly a rozšíření HTTP jsou zakázány na všech serverech (např. nepoužité knihovny, mody u Apache odinstalovány)
Ukázkový webový obsah a ukázkové webové aplikace odinstalovány.
Pro složky, které to vyžadují, je nakonfigurován vhodný ověřovací mechanismus.
Protokol Secure Socket Layer (SSL) je nainstalován pro ochranu komunikace ohrožené odposlouchávám.
Virtuální kořenové složky s webovým obsahem jsou umístěny na oddělených vyhrazených discích/svazcích (bez nástrojů pro administraci).
Pokud je to možné, účet, pod kterým běží služba HTTP, byl měl mít co nejméně práv.
Vhodně nastavená oprávnění (Access Control List) pro webové složky a soubory.
Funkce WebDAV zakázány nebo odstraněny, pokud nejsou používány. Jinak by měly být silně omezeny.
Servery jsou testovány skenery (vulnerability scanner) pro nalezení slabých míst využitelných na dálku. Nalezené problémy jsou řešeny.

Databázový server
Databázový software je nainstalován tak, aby běžel s co nejmenšími oprávněními.
Databázový software je aktualizován na poslední verzi s využitím oprav od výrobce.
Ukázkové účty a databáze jsou odstraněny ze serveru.
Je povolena vhodná filtrace paketů na úrovni protokolu IP pro omezení komunikace mezi webovým a databázovým serverem.
Mezi webovým serverem a databází je použito vhodné ověřování.
Změněna počáteční hesla databázových uživatelů (neponecháno prázdné heslo nebo přednastavené).
Oprávnění databázových uživatelů jsou vhodně omezena.
Pokud nejsou nezbytné, měly by být rozšířené uložené procedury (extended sotred procedures) smazány z databázového serveru a příslušné knihovny odstraněny z disku.
Hesla databázových uživatelů by neměla být uložena ve skriptech aplikace.
Aplikace
Vývojové a ladicí servery fyzicky jsou oddělené od provozního prostředí.
Přiměřená oprávnění (ACL) jsou nastavena pro složky a soubory aplikace.
Na straně serveru je prováděna vhodná validace vstupů.
Zdrojový kód aplikace očištěn od tajných údajů, soukromých dat a důvěrných informací.
Dočasné a neaktuální soubory (např. soubory .bak) jsou odstraněny ze serveru.
Přiměřeným způsobem je řešená správa stavů (nepoužívané hodnoty v otevřeném textovém tvaru v souborech cookie, náhodně generované identifikátory relace, citlivé hodnoty jsou šifrovány a podobně).
Role uživatelů v aplikaci vytvářeny s co nejmenšími oprávněními.
Pro šifrování jsou použity ověřené algoritmy vhodné pro danou úlohu (ne XOR!).
Vkládané soubory jsou umístěné mimo virtuální kořenové složky se správně nastavenými oprávněními (ACL).
Volání nebezpečných funkcí by měla být nalezena a měli bychom se jim pokud možno vyhnout.
Měl by být proveden detailní bezpečnostní audit zdrojového kódu.
Mělo by být stylem "black-box" provedeno vzdálené testování zaměřené na možný útok.
Strana klienta
Je použita poslední verze prohlížeče a souvisejícího softwaru včetně oprav.
Spouštění ovládacích prvků ActiveX, Java appletů, Flash animací je zakázáno.
Aktivní skriptování v prohlížeči je zakázáno.
V prohlížeči jsou zakázány tagy "Meta refresh" a "IFRAME".
Správa souborů cookie je povolena buď v prohlížeči, nebo pomocí nástroje třetí strany.
Klient pošty je nakonfigurován tak, aby používal nejkonzervativnější možné nastavení bezpečnosti.

Zdroj: upraveno podle Scambray a kol., 2003