POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Kyberterorismus, kybernetická válka – prostředky, metody a protiopatření

Diplomová práce

Cyber terrorism, cyber war – means, methods and countermeasures

Diploma thesis

VEDOUCÍ PRÁCE

doc. PhDr. Brzybohatý Marian Ph.D.

AUTOR PRÁCE

Bc. Denisa POKORNÁ

PRAHA

2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

V Praze, dne 15. března 2023

.....

Bc. Denisa Pokorná

Anotace

Diplomová práce se zabývá tématem kyberterorismu a kyberválky a prostředky, metodami a protiopatřeními, která se moderními teroristy používají a nastiňuje, co je předmětem války současnosti. Práce plynule přechází od obecného tématu k detailnímu popisu jednotlivých metod a zaměřuje se na nejčastěji používané techniky a metody. Důkladněji se věnuje metodám sociálního inženýrství, DDoS útokům a metodám prolamování hesel. Zároveň sestavuje základní požadavky na zabezpečenou organizaci a nabízí doporučující postupy. Seznamuje čtenáře s novinkami v úpravě, které jsou připravovány. Běžní uživatelé internetu možná ani netuší, jaká nebezpečí jim hrozí neuvědomělým brouzdáním po internetu a na sociálních sítích pro ně má tedy tato práce vzdělávací charakter.

Abstract

The diploma thesis deals with the topic of cyberterrorism and cyberwar and the means, methods and countermeasures used by modern terrorists and outlines what is the subject of war today. The work smoothly passes from a general topic to a detailed description of individual methods and focuses on the most used techniques and methods. It covers social engineering, DDoS attacks and password cracking in more detail. At the same time, it compiles the basic requirements for a secure organization and offers recommended procedures. It acquaints the reader with news which are being prepared. Ordinary Internet users may not even have an idea of what they are at risk of when they surf the Internet and social networks unconsciously, for them the work is educational in nature.

Klíčová slova

kyberterorismus * kyberválka * hacker* IDS* IPS* prolamování hesel* odposlech sítě* DDoS útoky*

Key words

cyberterrorism* cyberwar* hacker* IDS* IPS* password cracking* sniffing* DDoS Attacks*

Úvod

Cílem práce je pomocí deskripční metody a přehledové analýzy poukázat na aktuální nejpoužívanější metody zločinců. V současné době je společnost z většiny závislá na informačních technologiích. Již si ani neumíme představit, že bychom se vrátili do let minulých a byli kupříkladu nuceni využívat ke komunikaci s ostatními listinnou poštu. Nejedná se však pouze o otázku dorozumívání se, ale obecně počet úkonů, realizovaných digitálně. Množství těchto úkonů neustále roste a zároveň s nimi stoupá i jejich závažnost. Počítačové sítě jsou využívány v dopravě, průmyslu, medicíně, finančnictví, knihovnictví, vládním sektoru atd. Společnost se tedy kromě hrozeb terorismu, organizovaného zločinu, korupce, přírodních katastrof a mnoha jiného musí vypořádávat také s hrozbami na poli digitálním. V důsledku narušení počítačové bezpečnosti útoky může dojít k velkým škodám, např. ničení konkurence nebo získání know-how firmy, zablokování rozvodů vody, elektřiny, plynu, kolapsu v dopravě, bankovních společnostech. V případě kyberterorismu nebo kybernetické války jsou tyto škody výrazně ničivější a v zájmu každého státu nebo firmy by měla být určitá míra prevence před ohrožením digitálního prostoru, event. nastavení funkčních protiopatření.

1. Kyberterorismus a kyberválka

1.1 Bezpečnost

Bezpečnost je široce využívaným pojmem, jenž má mnoho definic a není jednotně vymezen. Terminologický slovník MV ČR z roku 2004 uvádí definici bezpečnosti jako „*stav, kdy jsou na efektivní míru omezeny hrozby pro objekt a jeho zájmy a tento objekt je k omezení stávajících i potenciálních hrozeb efektivně vybaven a ochoten při něm spolupracovat*“[1].

Pod pojmem bezpečnost se také rozumí „*společností (státem) stanovená (garantovaná) schopnost zamezení toho, aby konkrétní riziko překročilo únosnou mez. Pro zajištění bezpečnosti (omezení stávajících i potenciálních hrozeb) se odpovědný subjekt, např. stát, popř. mezinárodní organizace, efektivně připravuje řešit možná ohrožení. Hrozby mohou směřovat např. vůči obyvatelstvu, svrchovanosti státu, vnitřnímu pořádku, majetku, životnímu prostředí, plnění mezinárodních bezpečnostních závazků a dalším společenským zájmům.*“[2]

S bezpečností úzce souvisí pojmy hrozba, riziko, zranitelnost a aktivum.

Hrozbou chápeme „*objektivní skutečnost, která může znamenat negativní dopad*

1 Terminologický slovník - krizové řízení a plánování obrany státu. In: MV ČR [online]. Praha: MV ČR, 2016 [cit. 2023-03-12]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

2 Ministerstvo vnitra Odbor bezpečnostní politiky [online]. In: Vnitřní bezpečnost a veřejný pořádek. Krizové řízení. Praha 2005. [cit. 2023-03-12]. Dostupné z: https://docplayer.cz/20919444-Ministerstvo-vnitra-odbor-bezpecnostni-politiky.html

pro chráněný zájem v daném prostředí (ohrožení) – na určitém území, ve vymezeném období apod.“[3] Čelit hrozbám lze protiopatřeními, jejichž intenzita je odstupňována podle důležitosti, polohy apod. konkrétního objektu či chráněného zájmu. Některá protiopatření mohou být dosti nákladná i přesto, že ani nedosahují plné účinnosti.

Zjednodušeně se jedná o jakýkoliv fenomén, který má potenciální schopnost poškodit zájmy daného státu.

Riziko je „*možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí.*“[4] Riziko lze vždy odvodit z konkrétní hrozby. Pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, tj. míru rizika, je možné určit na základě tzv. analýzy rizik, která zahrnuje i zhodnocení naší připravenosti hrozbám čelit.

Aktivum je *„vše, co má pro společnost nějakou hodnotu a mělo by být odpovídajícím způsobem chráněno“*.[5]

Zranitelnost je *„vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou“*.

[3] Ministerstvo vnitra Odbor bezpečnostní politiky [online]. In: Vnitřní bezpečnost a veřejný pořádek. Krizové řízení. Praha 2005. [cit. 2023-03-12]. Dostupné z: https://docplayer.cz/20919444-Ministerstvo-vnitra-odbor-bezpecnostni-politiky.html

4 Bezpečnostní strategie 2003

5 Analýza rizik. ACRESIA [online]. [cit. 2023-03-12]. Dostupné z: https://acresia.com/index.php/sluzby/69-analyza-rizik

1.2 Terorismus

Terorismus je „*formou organizovaného násilí obvykle zaměřeného proti nezúčastněným osobám za účelem dosažení politických, kriminálních nebo jiných cílů*“.[6] Teroristické metody, jimiž se teroristické snaží takových cílů dosáhnout, se vyznačují nesmírnou brutalitou a bezohledností využívajíce přitom psychologických manipulací, vydírání, vyhrožování, zadržování rukojmích apod. Jedná se o plánovanou činnost motivovanou obvykle politicky, nábožensky, finančně (páchání organizované kriminality) nebo z psychických důvodů (spáchání teroristického útoku duševně nemocnou osobou).

Formy terorismu literatura rozděluje na letální a neletální.[7] Každou z těchto forem dále na konvenční a nekonvenční dle použitých prostředků.

Při **letálních**, smrtících, formách terorismu jsou využívány základní donucovací prostředky typu střelných zbraní, výbušnin, hořlavin, bodných a sečných zbraní (**konvenční** způsob letální formy) nebo zbraně hromadného ničení – zbraně chemické, biologické, jaderné a termické (**nekonvenční** způsob letální formy).

Neletální formy terorismu jsou takové, které využívají moderní prostředky nebo staré nástroje, avšak použité novým způsobem v kombinaci s letálními prostředky. **Konvenční** způsob neletální formy, který je kombinován s prostředky letálními a

[6] Analýza rizik. ACRESIA [online]. [cit. 2023-03-12]. Dostupné z: https://acresia.com/index.php/sluzby/69-analyza-rizik

[7] FOLTIN, Pavel a David Řehák. Důvody realizace a formy terorismu [online]. MOČR 2005 [cit. 12.03.2023]. Dostupné Vojenské rozhledy: http://www.mocr.army.cz/mo/obrana_a_strategie/1-2005cz/foltin.PDF

je označován jako tzv. unarmed terrorism (neozbrojený terorismus), je páchán zneužitím prostředků každodenního života k útoku – např. dopravních prostředků. Ke konvenčnímu způsobu neletální formy také patří zneužití výpočetní techniky a internetu k útoku nebo tzv. mediální terorismus, označovaný jako psychologický terorismus.

Psychologický terorismus definujeme jako *„plánované zneužívání hromadných sdělovacích prostředků a dalších psychologických prostředků v době míru, za účelem ovlivnění názorů, emocí, postojů a chování jednotlivců či cílových skupin populace tak, aby přímo nebo svými důsledky ohrožovaly bezpečnost a ústavní principy státu. Pro moderní vedení propagandy je typické zejména využití masových médií, např. plakátů, filmů, televizních programů, inzerátů, fotografických snímků, novinářských tiskových forem, ale také počítačové techniky.“*[8]

Nekonvenční způsob neletální formy zahrnuje zbraně využívající principů akustiky, optiky a elektromagnetického impulsu.

1.3 Válka

Francouzsko-česko-anglický sborník vojenských pojmů a definic (Strategicko-politická část) definuje válku jako „*otevřený ozbrojený konflikt vyhlášený mezi dvěma státy nebo společenskými komunitami, který se projevuje přerušením normálních politických a diplomatických aktivit mezi oběma stranami, případně mobilizací všech jejich dostupných zdrojů. V oblasti, kde ke střetu dochází, může vyústit ve vyhlášení válečného stavu nebo válečné situace.*“[9]

---

[8] BRZYBOHATÝ, M. Současný terorismus. In: FOLTIN, Pavel a David Řehák. Důvody realizace a formy terorismu [online]. MOČR 2005 [cit. 12.03.2023]. Dostupné Vojenské rozhledy: http://www.mocr.army.cz/mo/obrana_a_strategie/1-2005cz/foltin.PDF

[9] Válka. In: *MV ČR* [online]. Praha: MV ČR, 2016 [cit. 2023-03-12]. Dostupné z:

1.4 Špionáž

Špionáž (strategické zpravodajství) je oborem lidské činnosti, který se zabývá sběrem neveřejných a především utajených informací. Motivací bývá snaha o získání konkurenční výhody, sběr podkladů pro budoucí útok, nebo zkvalitňování vlastní obrany. Strategické informace jsou získávány z těchto zdrojů: HUMINT (lidské zdroje), SIGINT (radiový odposlech, tzv. signální zpravodajství), IMINT (obrazové systémy družic a letadel), MASINT (měření a podpisové zpravodajství, např. měření seismických vln), OSINT (otevřené zdroje – média, technická dokumentace), ACINT (akustické zpravodajství), GEOINT (geologický průzkum), PHOTINT (analýza fotografií), RADINT (radarový provoz), ELINT (elektronické zpravodajství), COMINT (komunikační zpravodajství), FISINT (zpravodajství zahraničních přístrojových signálů – např. elektromagnetické emise), FININT (finanční zpravodajství).

1.5 Válečná špionáž

Špionáž v době míru a v období války je posuzována odlišným způsobem.
L'ubomír Majerčík k válečné špionáži uvádí: *„Válečné právo špionážní aktivity uznává, i když špioni mohou být tvrdě potrestáni, pokud jsou chyceni. Špioni zajatí na nepřátelském území v průběhu ozbrojeného konfliktu nejsou oprávněni k podobnému zacházení s válečnými zajatci – mohou být popraveni, ale až po řádném soudu. Špion, který úspěšně splnil svůj úkol a vrátil se na své území, nesmí být v případě zajetí souzen jako špion. Kromě špionáže ve válečném právu*

https://www.mvcr.cz/mvcren/docDetail.aspx?docid=21281162&docType=ART

je shromažďování zpravodajských informací v době míru z vesmíru a moří jasně v mezinárodním právu povoleno.“[10]

1.6 Sabotáž

Sabotáž spočívá v páchání utajené činnosti, která má za cíl úmyslně narušovat nebo poškozovat funkce technického systému nebo zařízení protivníka. Motivací bývá konkurenční boj, boj o moc, snaha o eliminaci protivníka, prosazení politického nebo ideologického cíle aj.

1.7 Kyberprostor

Kyberprostorem (též kybernetickým prostorem) je myšleno „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“[11]
Kyberprostor je uznán jako jedna z operačních domén (vedle operační domény pozemní, námořní, vzdušné a vesmírné).

1.8 Kybernetická bezpečnost

Kybernetická bezpečnost je „*souhrnem právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.*“[12]

---

[10] Špionáž. *Global Politics: Internet Archive* [online]. [cit. 2023-03-12]. Dostupné z: https://web.archive.org/web/20080203202457/http://www.globalpolitics.cz/clanek/spionaz.html

[11] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.
[12] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Česká pobočka AFCEA, 2013, s. 57. ISBN 9788072513970.

1.9 Kyberkriminalita

Kyberkriminalita je způsob trestné činnosti páchané v prostředí informačních a komunikačních technologií a na síti. Spadají sem trestně postižitelná škodlivá chování na internetu – např. internetové pirátství (pořizování nelegálních kopií, nelegální Peer-to-Peer sdílení souborů, porušování autorského zákona nebo průmyslových práv), šíření závadového obsahu, závažná forma kyberšikany, kybergroomingu a kyberstalkingu, ale také sofistikovaná organizovaná kriminalita, krádeže identity nebo kyberterorismus.

ad) **Šíření závadového obsahu**

Šířením závadového obsahu rozumíme především šíření extremistických a nenávistných sdělení, hanobení národa, popírání holokaustu (v mnoha zemích světa), sdělení vyzývající k násilí či rasismu, šíření zakázaného druhu pornografie vyobrazující znásilnění nebo sexuální kontakt se zvířetem, zemřelou osobou či dítětem. K páchání nelegální činnosti touto formou není třeba zvláštních znalostí.

ad) **Kyberšikana, kybergrooming a kyberstalking**

Kyberšikana (šikana prostřednictvím elektronických médií), kybergrooming (lákání obětí na schůzku skrze internet) a kyberstalking (pronásledování oběti pomocí ICT technologií) jsou škodlivé způsoby chování uživatele prostřednictvím internetové sítě, které mohou dosahovat závažnosti postižitelné trestním zákoníkem. Bývají doplňovány o techniky sociálního inženýrství (viz níže).

1.10 Kyberterorismus, kyberválka

Kyberterorismus, kybernetický terorismus, řadíme ke konvenčnímu způsobu neletální formy terorismu. Z důvodů rychlého šíření informačních a komunikačních

technologií a digitalizace je tento druh terorismu ve 21. století na vzestupu a doplňuje klasické formy terorismu. Veškeré státní složky a celá kritická infrastruktura moderní společnosti je závislá na informačních a provozních systémech, což samo o sobě dává kyberteroristům do rukou mocnou zbraň, jak jsme se již mohli přesvědčit v případě Stuxnet, počítačového červa objeveného roku 2010, který byl speciálně vyvinut k útokům na systémy SCADA, systémy dohledového řízení a sběru dat, používané také k průmyslové kontrole tlaku a dalších fyzikálních vlastností jaderných centrifug.

Kyberválka, kybernetická válka, je způsob války zneužívající k ničení infrastruktur, získání informací nebo oslabení protivníka doménu kyberprostoru. Získané informace mohou být dále zneužity pro sabotáž, demoralizaci nebo likvidaci protivníka prostřednictvím ovlivňování veřejného mínění a šíření propagandy. Odcizení citlivých nebo utajených informací je velkou konkurenční výhodou moderního válčení – bývá spojováno s pojmem informační válka. Válka v kyberprostoru může probíhat v souvislosti s válkou vedenou běžnými konvenčními metodami.

1.11 Kybernetická bezpečnostní událost, kybernetický bezpečnostní incident

§ 7, odst. 1 zákona o kybernetické bezpečnosti definuje kybernetickou bezpečnostní událost: *„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.“*[13]

§ 7, odst. 2 zákona o kybernetické bezpečnosti definuje kybernetický

[13] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

bezpečnostní incident: *„Kybernetickým bezpečnostním incidentem je kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.“*[14]

Narušení bezpečnosti informací znamená narušení jejich integrity (neporušenosti), dostupnosti (záruky dostupnosti informace v době, kdy je informace potřeba) a důvěrnosti (k informaci má přístup pouze oprávněná osoba). Tyto tři atributy, tzv. triáda CIA (Confidentiality-Integrity-Availability) jsou chráněny společnostmi nejvíce, avšak v posledních letech hovoří autoři i o dalších atributech, např. Parkerian Hexad Model (1998 Donn B. Parker)[15] Autenticita-Vlastnictví-Užitečnost ve spojení s CIA triádou. Za zmínění stojí také odpovědnost, autorizace, nepopiratelnost a přípustnost.[16]

1.12 Hacker

Pojem hacker je široký, zpravidla označuje osobu s perfektní znalostí fungování

[14] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

[15] 1.3 Models of Security – CIA Parkerian Hexad. *ENG LIBRE TEXTS*[online]. [cit. 2023-03-12]. Dostupné z: https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.3_Models_of_Security_-_CIA___Parkerian_Hexad

Analýza rizik. *ACRESIA* [online]. [cit. 2023-03-12]. Dostupné z: https://acresia.com/index.php/sluzby/69-analyza-rizik

16 FRYČ, Bc. Martin. *Audit informační bezpečnosti: Význam auditu informační bezpečnosti v procesu zavádění bezpečnostního standardu PCI v organizaci* [online]. Praha, 2009 [cit. 2023-03-12]. Dostupné z: is.ambis.cz. Diplomová práce. Bankovní institut vysoká škola Praha - informační technologie a management.

informačních systémů, na jejichž problémy je schopna adekvátně reagovat.
V oblasti kybernetické bezpečnosti se však setkáváme s několika druhy hackerů, kteří ani tuto definici v plném rozsahu nemusí splňovat – white hat hackers, black hat hackers, grey hat hackers, green hat hackers, blue hat hackers, red had hackers, purple hat hackers, script kiddies, státem (národem) sponzorovaní hackeři, hactivististé a škodící insideři nebo informátoři.

White hat hacker (Ethical Hacker), česky bílý nebo etický hacker, je odborníkem na konstrukce počítačových systémů a sítí, zpravidla bývá programátorem v podniku. Své znalosti používá k vyhledávání zranitelností a následného zdokonalování systému. **Black hat hacker**, česky černý hacker, je druhem hackera, který se snaží proniknout do počítačů a sítí za účelem svého finančního zisku nebo páchání škod. **Grey hat hacker**, česky šedý hacker, rád prozkoumává počítače a síť, ale na rozdíl od black hat hackera nemá potřebu finančního obohacení ani páchání škod, avšak občas se může dopouštět překračování zákona. **Green hat hacker**, česky zelený hacker, je bílým hackerem nováčkem, který se teprve učí a může se z tohoto důvodu dopouštět chyb. **Blue hat hacker**, česky modrý hacker, má zájem na vylepšování kybernetické bezpečnosti a je podobný bílému hackerovi, většinou se ale jedná o externího pracovníka společnosti. **Red hat hacker**, česky červený hacker, je digitálním aktivistou, který se svými hackerskými způsoby snaží o předání poselství, politického názoru apod. **Purple hat hacker**, česky fialový hacker, je druhem hackera, který testuje bezpečnost software a hardware pouze na svých počítačích a ve své síti. **Script kiddies**, česky skriptovací děcka, je označení, které používají kvalifikovaní hackeři pro nezkušené osoby, jež pro škodlivé účely používají skripty/kódy vytvořené jinými osobami, aniž by věděly, na jakém principu tyto skripty/kódy pracují. **Státem (vládou) sponzorovaní hackeři** jsou útočníci s různými motivacemi, kteří jsou finančně sponzorováni státy nebo vládami. Vzhledem k zastřešení státem nebo

vládou, které je jim poskytováno, je obtížné tyto skupiny zastavit a provést atribuci čili přisouzení viny za útok. **Hacktivisté**, česky hackerští aktivisté, jsou skupinou, která se prostřednictvím počítačových technik, pokouší na základě vlastního přesvědčení a prosazovat společenské změny. **Zlovolní insideři a informátoři**, jsou osoby, které vypouštějí citlivé informace z organizací ven, a tím ji ohrožují.

Obrázek 1 - Hacker

1.3 Crime as a Service

Crime as a Service, česky zločin jako služba, je označení pro prodej nástrojů a služeb zkušenými kyberzločinci a jejich nabízení méně zkušeným útočníkům za účelem usnadnění provedení útoků, které by pouze se svými omezenými znalostmi nebyli méně zkušení útočníci schopni provést. Prodej nástrojů běžně probíhá na tzv. Dark Webu, což je skrytá šifrovaná síť internetu, kterou je možno

prohlížet pouze pomocí speciálního software – např. anonymní prohlížeč Tor. Anonymní prohlížeč Tor vzniknul s čistým záměrem vyhnout se cenzuře totalitních režimů, avšak umožnil současně odsun zločinců z veřejné části internetu na Dark Web.

2. Prostředky, metody, techniky

K základním prostředkům využívaným kyberzločinci patří počítač, internetová síť, získané informace a lidský faktor. V rámci těchto prostředků jsou zločinci vytvářeny promyšlené nástroje a metody k naplňování jimi stanovených cílů. Východiskem zdokonalování obranných opatření proti kybernetickým hrozbám je zejména pochopení, jakým způsobem funguje Internet, kritické myšlení a odolnost proti lidským manipulacím.

2.1 Jak funguje internet?

Internet si lze představit jako globální systém propojující dílčí počítačové sítě, které mezi sebou vzájemně komunikují na základě společných pravidel přenosu, tzv. síťových protokolů, a to prostřednictvím různých přenosových cest – mobilních stanic, satelitů nebo kabelů (optické, metalické) atd.

Mezi síťové protokoly řadíme transportní protokoly rodiny TCP/IP, protokoly pro komunikaci s webovými stránkami, pro komunikaci prostřednictvím emailu, pro přenos souborů po síti a pro nastavení přesného času v počítači.

Sada protokolů TCP/IP (Transmission Control Protocol) slouží pro komunikaci zařízení v rámci celosvětové internetové sítě. K TCP/IP řadíme protokoly IP, TCP, DHCP. Základem připojení zařízení do sítě je IP (Internet Protocol) a DHCP (Dynamic Host Configuration Protocol). IP označuje unikátní identifikační adresu, kterou zařízení používá v danou chvíli pro připojení do sítě. Přidělování IP adresy každému zařízení je automaticky zajištěno pomocí protokolu a serveru DHCP. Dle IP adresy je síťový přenosový protokol TCP (Transmission Control Protocol) poté schopen dopravit požadovaná data do správného zařízení.

Zjednodušeně řečeno, datový soubor, např. video nebo fotografie, přenášený po síti pomocí TCP je automaticky převeden do formy binární soustavy nul a jedniček, resp. impulzů vypnuto a zapnuto. Tato forma je dále rozdělena na šestimístné kombinace nul (vypnuto) a jedniček (zapnuto), tzv. **paketů**. Každý paket souboru získává své pořadové číslo. Pakety mohou cestovat ke koncovému adresátovi různými cestami vedení internetu (kabely, rádiové vlny aj.). Po dosažení konečného cíle, tj. zařízení se správnou IP adresou, se seskládají do původní formy dle svých pořadových čísel. K přiřazení dat do správné aplikace v rámci cílového přístroje slouží tzv. **síťové porty**, na kterých procesy aplikací v zařízení běží. Na každém portu s daným číslem může běžet pouze jedna služba.

Již před započetím přenosu TPC zjišťuje, k jakému cílovému portu zařízení a s jakou IP adresou data přiřadí. Následně provede tzv. **třístupňové ověření (1. zaslání paketu SYN, 2. obdržení paketu SYN-ACK, 3. zaslání paketu ACK)**, zda bude vůbec přenos mezi zařízeními možný. Je-li vše v pořádku, pakety se odešlou. Ztratí-li se paket s některým pořadovým číslem po cestě, resp. není-li dodán do určité stanovené doby, chybějící paket se prostřednictvím TPC znovu dopošle a soubor se následně sestaví.

Je-li místo TPC používán protokol UDP (User Datagram Protocol), taktéž určený pro přenos dat, při ztrátě paketu se chybějící paket znovu nezašle, a stejně tak se ani nezachová pořadí paketů, dorazí-li některý z nich déle. UDP je rychlejší než TPC, avšak neprovádí u koncového zařízení ověření, zda mu lze soubor odeslat. Je tedy poměrně nespolehlivý a v důsledku toho může koncový uživatel obdržet nekompletní data zapříčiňující chybnou funkčnost nebo zobrazení přijatého datového souboru.

Slovník s pojmy vztahujícími se k této oblasti podrobněji viz dále **Příloha č. 1**.

Útoky kyberzločinců je možno pro účely přehlednosti rozčlenit.

Dle druhu použitého prostředku existují útoky:

- s využitím psychologického působení
- s využitím volně či veřejně dostupných dat
- přímé fyzické útoky
- s využitím software nástrojů
- s využitím hardware nástrojů
- útoky kombinující výše uvedené

Dle předmětu útoku se vyskytují útoky na:

PC software, PC hardware, Internet, instant messaging, Internet věcí, mobilní platformy, informace a podobná aktiva (např. osobní údaje, data, utajené informace), satelitní systém a jiné stanice, umělou inteligenci, provozní a řídící systémy, digitální měny, systémy kritické informační infrastruktury, významné informační systémy, systémy základní služby, cloudové služby, elektronické služby, biometrické systémy, platební systémy, NFT (nezaměnitelný token), …

Dle složitosti útoky lze dělit na:

- jednoduché
- sofistikované – pokročilá trvalá hrozba, organizovaná kriminalita, vícevektorový DDoS útok, kyberšpionáž, sabotáž, rozsáhlé kyberteroristické a kyberválečné útoky

Rozdělení dle použité prostředku, resp. metody a techniky je klíčovým obsahem této kapitoly a rozeberu jej podrobněji.

2.2 S využitím psychologického působení – metody sociálního inženýrství

Pretexting

V rámci pretextingu zločinci využívají smyšlené scénáře, které mají přesvědčit oběť, aby dobrovolně poskytla soukromé informace. Podkladem pro tvorbu scénářů jsou pravdivé informace, např. datum narození, rodné číslo zaměstnance, jméno nadřízeného nebo jiné informace vzbuzující důvěryhodnost útočníka.

Phishing, Spear Phishing, Smishing a Vishing

Phishing, česky rhybaření, je podvodná technika využívaná na internetu k získávání citlivých údajů v elektronické komunikaci. V rámci phishingového útoku se útočník vydává za důvěryhodnou organizaci či autoritu. Na základě omylu se může nechat běžný uživatel internetu oklamat. Daný člověk např. otevře email, ve kterém je požádán, aby se přihlásil do svého internetového bankovnictví a aktualizoval své osobní údaje. Email obsahuje odkaz na falešnou přihlašovací stránku internetového bankovnictví. Uživatel na tento odkaz bezmyšlenkovitě klikne, zadá své přihlašovací údaje a odešle. Do svého bankovnictví přihlášen není, skrytí útočníci vydávající se za bankovní instituci však tímto způsobem získali jeho klientské číslo a heslo. Emaily mohou být rozesílány prostřednictvím botnetu. Speciálním druhem phishingového útoku je tzv. whaling, kdy se útočník vydává za zaměstnavatele výše postaveného zaměstnance, a snaží se pomocí oficiálně znějícího emailu získat od zaměstnance citlivé osobní údaje, poslat mu malware v příloze emailu nebo se pokusit provést podvodnou transakci peněz.

Obrázek 2 - Phishing

Spear Phishing je na rozdíl od phishingu cíleným útokem. Cílí na organizace nebo jednotlivce. Nejčastěji se jedná o podvodný email obsahující naléhavý požadavek. Obsah zprávy zní věrohodně, a stejně tak zdánlivý odesílatel emailu je považován za důvěryhodného člověka (např. zaměstnanec firmy).

Smishing je formou phishingu. Citlivé údaje se snaží vylákat prostřednictvím SMS zpráv.

Telefonní Phishing nebo také **vishing** či **voice phishing**, česky **hlasový phishing**, je technika podvodných telefonátů a hlasových zpráv, kterými se pachatelé pokoušejí získat citlivé informace od svých obětí, a to především pod smyšlenou záminkou – ohrožení bankovního účtu oběti, nabídka výhodného úvěru apod. Útočníci požadují sdělení přihlašovacích nebo citlivých osobních údajů, nabízí instalaci výhodných PC nebo mobilních aplikací, požadují zaslání fotografie občanky, provedení bankovní transakce, výběr a následné vložení peněz na jiný účet atd. Aby byl telefonát ještě důvěryhodnější, útočník využívá někdy tuto techniku ve spojení s podvržením ID (telefonního čísla) volajícího (tzv. Caller ID

Spoofing), takže přijímající oběti se na displeji telefonu zobrazí skutečně číslo, které používá banka, policie, zákaznická služba, byť se jedná o útočníka. Číslo na oběť bývá získáno v důsledku nadměrného sdílení osobních údajů obětí na internetu, ale také souhlasu s podmínkami užívání internetové služby nebo např. akceptace služeb třetích stran. Útočníci v některých případech využívají v rámci telefonního phishingu tzv. Interaktive Voice Response System, česky systém interaktivní hlasové odezvy, předem nahraný automatizovaný hlasový hovor.

Zlomyslná volání

Princip zlomyslného volání ve smyslu útoku spočívá ve volání na tísňovou linku z neoprávněných důvodů, za účelem jejího úmyslného zablokování nebo zneužití složek integrovaného záchranného systému.

Baiting

Baiting je způsobem sociálního inženýrství, při němž útočník ponechá infikované paměťové médium (CD, USB flash disk) na místě, kde se oběť vyskytuje, a využije její zvědavosti nebo chamtivosti paměťové médium prozkoumat nebo si jej ponechat. V případě, že si bude chtít poté oběť prohlédnout, co se na paměťovém médiu nachází, nebo si médium ponechat k užívání, může si jeho vložením do PC nainstalovat virus, za pomocí něhož útočník získá přístup k PC nebo PC síti, což může být velmi ničivé zejména v případech, kdy se jedná o síť korporátní.

Quid pro Quo (Něco za něco)

Při Quid Pro Quo útočník požaduje citlivé údaje výměnou za poskytnutí protislužby, o kterou má s největší pravděpodobností oběť zájem.

Tailgating (též Piggybacking)

Tailgating (Piggybacking) označuje fyzické přidružení se k uživateli, který má přístup do zabezpečeného prostoru.

Pharming

Pharming se od phishingu odlišuje pouze tím, že oběť nemusí klikat na žádný odkaz, jde tedy o phishing bez návnady. Při pharmingu útočníci odcizí doménu webové stránky (viz dále DNS Hijacking) nebo infikují mezipaměť DNS serveru (viz dále DNS Cache Poisoning) a přepíší IP adresu, čímž zapříčiní, že oběť je po napsání správné adresy webu (např. internetového bankovnictví) do URL řádku automaticky přesměrovaná na falešnou stránku.

Typosquatting

Typosquatting by se dal podřadit nejen pod metody sociálního inženýrství, ale také pod cybersquatting (viz dále), jelikož může mj. sloužit k poškozování obchodní značky. Jedná se o způsob útoku, který předpokládá pochybení uživatele, především překlep nebo pravopisná chyba při zadávání URL adresy webové stránky do adresního řádku webového prohlížeče. Řekněme, že uživatel potřebuje navštívit stránku www.Seznam.cz a namísto ní zadá do adresního řádku www.Snezam.cz, což útočníci předvídají, a proto si doménu s překlepem úmyslně zaregistrují. Při zadání této chybné adresy je uživatel přesměrován na stránky s malware nebo podvodné stránky určené k vylákání citlivých údajů z uživatele.

Cybersquatting (též Domain Squatting)

Cybersquatting je metoda, při níž pachatel zaregistruje a používá (event. pomocí reklamy dále přeprodává) doménové jméno, které je stejné nebo nápadně podobné známé obchodní značce nebo obchodnímu jménu, v důsledku čehož může návštěvníky domény uvádět v omyl, že se jedná o tuto známou obchodní značku nebo jméno. Následky mohou být katastrofální v případě, že útočník okopíruje také obsah stránky obchodní značky a vydává se za ni. Může posloužit

také k vydírání zástupce obchodní značky pomocí umístění reklamy na stránkách domény s varováním, že neodkoupí-li si doménu podvodníka, bude na ní zveřejněna pornografie nebo jiný závadný materiál, čím může vytvářet úmyslně pravé obchodní značce špatné jméno.

HTTP/S Spoofing

Metoda HTTP a HTTPS Spoofing, česky podvržení HTTP a HTTPS, též známá jako IDN homografický útok (homografický phishing), jejíž podstatou je oklamat uživatele a napodobit stránku, kterou chce navštívit. Útočník si zaregistruje doménu, která má vizuálně stejný název domény jako pravý web. Často nelze tyto weby od sebe na první pohled rozeznat. Falešný web může mít dokonce SSL šifrování. Rozdíl v názvech domény spočívá v použité jazykové sadě znaků nebo falšování písmen, např. ve využití skutečnosti, že omikron v řecké abecedě se podobá písmenu o v latince, nebo že zfalšovat písmeno lze použitím dvou písmen za sebou – použít písmena rn místo písmene m.

Ostatní metody založené na psychologickém působení

Řadíme sem např. *hacking sdíleného virtuálního serveru*, *zkracování škodlivých URL odkazů*, *padělání stránek a oklamání uživatele*, *skrývání před anti-phishing filtry*, *přesměrování uživatele na stránku s vyskakovacím oknem a využití jeho zmatečného chování* (např. při pokusu o zavření omylem klikne vyskakovací okno), *tapnabbing* (vylákání přihlašovacích údajů podstrčením stránky falšující oblíbenou a uživatelem často navštěvovanou stránku), tzv. *deep fake útoky* (provádění podvodných a dezinformačních videoreklamních a obrazových kampaní s falešnými osobami prostřednictvím využívající prvků umělé inteligence se záměrem oklamat lidi) atd.

2.3 S využitím volně či veřejně dostupných dat

Pachatel zde využívá faktu, že uživatelé na sebe na internetu uvádějí velké množství informací sami. Útočník nepozorovaně sesbírá informace z veřejně přístupných databází (z webových stránek, OSINT,..) a může se je pokusit dále zneužít.

2.4 Přímý nebo fyzický útok

Nejznámějšími metodami přímého útoku je tzv. dumpster diving, útok tváří v tvář, návštěva falešného pracovníka a dodání zařízení se škodlivým software, tzv. malware.

Dumpster diving

Dumster diving, česky prohledávání odpadků, je metoda zneužití vyhozených neskartovaných nebo nedostatečně skartovaných dokumentů, z nich může útočník získat osobní údaje nebo jiné citlivé informace a případně je dále zneužít buďto v surové podobě k přístupu do systému (např. nalezené na papíře zapsané přihlašovací údaje) nebo v sociálním inženýrství.

Útok tváří v tvář

Útok tváří v tvář znamená získání potřebných informací přímo. Útočník neváhá a fyzicky napadne nebo okrade oběť o čipovou kartu, doklady, techniku apod.

Falešný pracovník (servisní technik, dodavatel)

Falešného pracovníka nemusí řadoví zaměstnanci poznat a mohou se jím nechat oklamat a okrást.

Dodání zařízení s malware

Při dodání zařízení s malware se může jednat o jakékoliv technické zařízení, na které je možno nainstalovat malware – paměťové medium typu USB s malware nebo např. celý počítač s operačním systémem infikovaným malware.

2.5 S využitím software

Metody a techniky s využitím software hackerských nástrojů jsou vedle metod a technik sociálního inženýrství nejrozšířenější skupinou.

2.5.1 DISTRIBUCE MALWARE

Malware (z angl. malicious software) je typ škodlivého nebo obtěžujícího programu, který provádí v počítači činnost bez souhlasu oprávněného uživatele. Může být distribuován prostřednictvím přenosných paměťových médií, neúmyslným nainstalováním či stažením nakaženého software do počítače (tzv. drive-by-download, drive-by-installation), šířen v těle souborů .doc apod., uvnitř emailu, HTML kódem, v důsledku využívání falešného antiviru aj. způsoby.

Škodlivá či obtěžující činnost je různého druhu a rozsahu v závislosti na použitém typu malware.

Typů malware je mnoho, nejznámější jsou boty a botnety, adware a scamy, viry, červy, spyware, trojští koně, backdoory, rootkity, keyloggery, keysniffery, ransomware, spamy a scareware.

Bot a botnet

Bot, nebo také zombie, je malwarem infikovaný počítač, který může být dálkově ovládán příkazy hackerů.

Botnet je pak celá sítě těchto počítačů umožňující hackerům DDoS útoky (viz níže) na servery (přetížení až paralyzování stránek), zaznamenávání stisku kláves při

zadávání textu do formulářů – např. hesla k bankovnímu účtu (keylogging), pořizování snímků obrazovky, přístup k webové kameře, šíření jiných typů malware a odesílání spamu a phishingových zpráv.

Adware a Scam

Adware je druh malware spočívající v zobrazování vyskakovacích oken a reklam. Některé adware jsou neškodné, jiné mohou obsahovat odkazy na stránky s dalšími druhy malware, nebo mohou sloužit k podvodům (tzv. scams). S nevyžádanou reklamou si poradí software typu AdBlock.

Virus

Virus je škodlivý program nebo část programového kódu spouštějící se bez vědomí uživatele. Ke svému šíření využívá jako hostitele spustitelné soubory. Snaží se o získání kontroly nad počítačovým systémem nebo jeho částí a následně poškození uživatele samotného (např. smazáním souborů bez jeho vědomí).

Červ

Červ je druh počítačového viru, který se dokáže replikovat sám a šíří se zpravidla prostřednictvím počítačových služeb. Lze jej vyrobit například pomocí software *Internet Worm Maker Thing*.

Spyware

Spyware (špionážní software) tajně zaznamenává naši online aktivitu, získává data a shromažďuje osobní údaje, jako jsou uživatelská jména, hesla, čísla kreditních karet, historie prohlížených stránek a údaje o chování na internetu. Nebezpečí spyware tkví v jeho utajení a obtížnému odhalení. Do počítače může být nainstalován spolu s jiným programem, otevřením infikované přílohy e-mailu nebo při volném stahování hudby nebo filmů. Jakmile je spyware v počítači,

předává naše data inzerentům nebo počítačovým zločincům. Používá se zejména ke krádeži identity a podvodům s kreditními kartami. Některé spyware instalují další malware, který dokáže měnit nastavení počítače nebo prohlížeče.

Trojský kůň

Trojský kůň je škodlivý kód, který je ukryt v počítačovém programu a na první pohled se tváří užitečně. Sám se však nešíří. Cílem je ovládat počítač uživatele útočníkem, manipulace a mazání dat, získání hesel, vzdálené ovládání systému apod.

Backdoor (Backdoor attack)

Backdoor, česky zadní vrátka, je způsob napadení počítače, při kterém útočník obejde autentizační mechanismus počítače nebo systému a pro budoucí využití tohoto počítače nebo systému, např. krádeže dat, kyberšpionáž nebo sofistikovanější útoky APT, si do něj ponechá vzdálený přístup, aniž by to oprávněný uživatel zařízení zjistil.

Rootkit

Rootkit je program navržený hackery tak, aby mohl bez našeho vědomí získat přístupová práva administrátora na našem počítači.

Keylogger (též Keystroke Logger)

Softwarový keylogger je speciální formou spyware, špionážního software (např. Perfect Keylogger Lite). Útočník jím sbírá zaznamenané stisky jednotlivých kláves provedené uživatelem. Keylogger je využitelný zejména k získávání přístupových údajů (hesel atd.).

Ransomware

Ransomware je škodlivý program, který blokuje počítačový systém nebo šifruje v něm obsažená data. Následně se výhružnou zprávou dožaduje zaplacení výkupného za obnovení přístupu.

Spam

Spam je je nevyžádané sdělení masově šířené internetem – nevyžádané reklamní emaily, příspěvky na diskuzních fórech, komentáře, zprávy v instant messaging apod.

Scareware

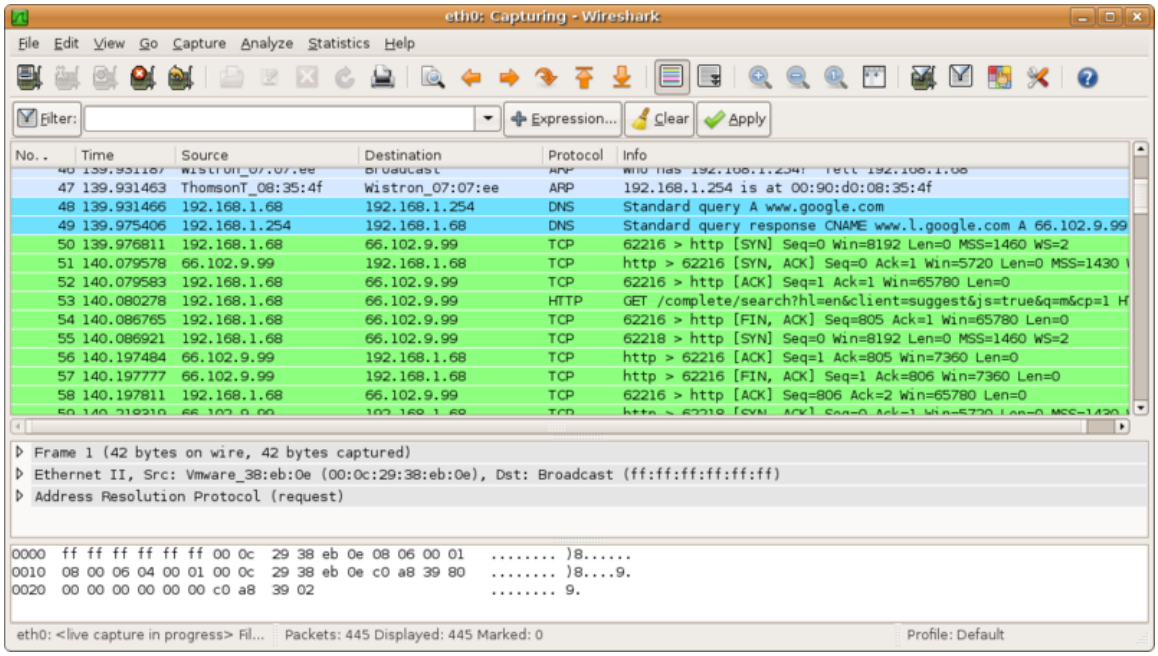
Scareware je druhem malware, který uplatňuje metody sociálního inženýrství a snaží se s pomocí oken s klamným varováním nebo doporučením přesvědčit uživatele PC v důsledku vyvolání úleku nebo zděšení ke stažení falešného programu. Příkladem scareware je Rogue Security Software, jehož cílem je oklamat uživatele oznámením, že v jeho počítači se nachází malware a je potřeba jej odstranit. Následně se jej snaží program přesvědčit k zaplacení a stažení falešného antiviru, se kterým je do počítače nainstalován skutečný malware, nejčastěji trojský kůň.

Logický bombový malware

Logický bombový malware, je druh malware, který funguje jako časovaná bomba. Nemusí být spuštěn okamžitě, útočník může vyčkávat na jeho spuštění. V základních rysech se neliší od předchozích druhů škodlivého software, byť má některá specifika – může mazat soubory, krást informace, bránit přístupu do jiných aplikací, zneužít přihlašovací účty k rozesílání spamu, spotřebovávat systémové prostředky nebo těžit kryptoměny.

2.5.2 ODPOSLECHY SÍŤOVÉHO PROVOZU

Odposlechem síťového provozu, v literatuře zmiňovaným pod názvy Sniffing, Eavesdropping nebo Wiretapping lze zachytávat pakety dat přenášené po síti. Je-li komunikace po síti zasílána nešifrovaně zejm. přes protokoly HTTP, FTP, Telnet, SMTP, POP, IMAP, může ji útočník pomocí software snadno přečíst. Obtížnější cestou je odposlech komunikace šifrované (HTTPS, SFTP aj.), neboť ta může být přečtena jen po zjištění privátního klíče určeného k dešifrování. K odposlechům jsou využívány např. programy *WireShark a Ethereal.*



Obrázek 3 - WireShark

Odposlech hesla provádí útočník ***metodou Man In The Middle***, česky člověk uprostřed, buďto vytvořením veřejné WiFi s důvěryhodným názvem a jejím odposlechem pomocí software (tzv. WiFi Passive Eavesdropping), nebo narušením spojení, při kterém útočník skrytě vstoupí mezi komunikaci dvou účastníků (např. webový server a uživatele) a komunikaci odposlechne.

SSL (Secure Socket Layer) Stripping (SSL/HTTPS Downgrade), česky by bylo možno přeložit jako odstranění SSL vrstvy (degradace SSL/HTTPS), je označení pro změnu spojení mezi uživatelem a webovým serverem zabezpečeného pomocí protokolu SSL, tj. HTTPS, na spojení nezabezpečené, tj. HTTP. SSL Stripping útočník provede buďto výše uvedenými způsoby – vytvořením veřejné WiFi či narušením spojení s nastavením proxy serveru, nebo falšováním identity prostřednictvím ARP (viz níže).

Vytvoření veřejného WiFi hotspotu je poměrně zřejmé, jak je však možné spojení narušit? Uživatel zadá do webového prohlížeče požadavek, tj. adresu stránky, který je odeslán webovému serveru. Pokud nevypíše do URL řádku rovnou zabezpečenou adresu HTTPS, je požadavek odeslán nezabezpečeně přes HTTP protokol. Webový server uživatele poté přesměruje z nešifrovaného HTTP na šifrované HTTPS. Útočník využije okamžiku třícestného potřesení rukou, kdy pomocí software zachytí a pošle dál HTTP požadavek (SYN) uživatele a HTTP odpověď (SYN-ACK) serveru o přesměrování, a následně se připojí k serveru prostřednictvím HTTPS, přičemž s uživatelem samotným naváže HTTP spojení a nastaví vlastní proxy server, díky kterému obdrží útočník všechny požadavky uživatele.

ARP Spoofing, česky falšování identity prostřednictvím ARP (Address Resolution Protocol), je typ útoku s využitím komunikačního protokolu ARP určeného pro zjišťování MAC adresy na základě IP adresy v místní síti LAN. Při ARP spoofing útočník pomocí software (např. Ettercap) manipuluje s protokolem ARP tím, že opakovaně vkládá do místní sítě falešné ARP pakety s odpovědí na neexistující dotaz na MAC adresu routeru se známou IP adresou. Jakmile se počítač oběti pokusí připojit k internetu, zkontroluje, zda se v mezipaměti ARP LAN nachází MAC adresa routeru. Pokud se v mezipaměti ARP LAN MAC adresa routeru nenachází, začne se ARP dotazovat všech zařízení v celé lokální síti. Útočník

využije toho, že vkládá velké množství falešných odpovědí a skutečnosti, že ARP zachytí falešnou odpověď dříve než pravou vyslanou routerem. Falešná odpověď sděluje ARP protokolu, že router s IP adresou má MAC adresu ve skutečnosti patřící útočníkovi. Následně se tedy počítač oběti připojí k zařízení útočníka namísto routeru, zatímco zařízení útočníka se připojí k routeru, a tím se stane prostředníkem mezi routerem a uživatelem, který může odposlouchávat komunikaci nebo s ní dále manipulovat. Závěrem může útočník změnit podnikovou tabulku ARP, tzv. ARP table, tak, že obsahuje zfalšované MAC mapy dle svých potřeb, a útok se tak může postupně dále rozšiřovat – **ARP Cache Poisoning**, česky otrávení ARP mezipaměti.

K odposlechu se využívá: *Cain and Abel, Wireshark (dříve Ethereal).*

2.5.3 MANIPULACE DATOVÉHO TOKU

Velmi používanou metodou manipulace datového toku je tzv. ***Man In The Middle Attack***, kdy útočník nejenže datový tok zachycuje, ale stává se také aktivním prostředníkem, který do komunikace zasahuje – pozměňuje ji nebo maže (tzv. Active Eavesdropping, česky aktivní odposlech).

Útoky typu Man In The Middle mohou být konstruovány různým způsobem – pomocí výše uvedené otravy mezipaměti ARP, odposlechu vlastní veřejné WiFi nebo SSL Strippingu, dále prostřednictvím IP/HTTP/DNS Spoofingu, únosu emailu nebo únosu relace (krádež cookies).

IP Spoofing, česky podvržení IP adresy, je vytvoření a následné odeslání datového paketu s falešnou zdrojovou IP adresou, která patří oběti namísto útočníka. Využívá se při DDoS útocích, kdy útočník zamění svou IP adresu za adresu oběti, vyšle požadavek na server a server následně odpovídá oběti, nikoliv útočníkovi.

DNS (Cache) Poisoning, česky otrávení (mezipaměti) DNS, též DNS Spoofing, česky podvržení DNS, je metoda vložení falešného záznamu do mezipaměti DNS překladače domén. Útočník pozmění IP adresu, na kterou je odkazováno z konkrétní domény. Zadá-li poté uživatel do adresního řádku název domény, falešný záznam přesměruje uživatele na jiný web, než který zamýšlel navštívit. Je zneužíváno zejména pro pharming (viz výše).

E-mail Hijacking, česky únos emailu, je technikou Man In The Middle útoku, při kterém útočník získá přístup do emailu, a poté monitoruje nebo manipuluje s komunikací. Útočníci jsou dokonce schopni zfalšovat emailovou adresu a zasílat z ní zprávy.

Únos spojení, taktéž relace (Session / Cookie Hijacking)

Neoprávněný přístup k informacím nebo službám webového serveru může útočník získat pomocí metody únosu spojení. Při tomto způsobu útoku dochází k odcizení cookies, která si webový server ukládá do webového prohlížeče uživatele. Útočník se díky nim může za uživatele před webovým serverem vydávat.

K obraně proti útokům Man In The Middle je využíván např. *antivirus Ettercap*.

2.5.4 ÚTOKY NA PROLAMOVÁNÍ HESEL

Vyjma technik softwarového inženýrství slouží ke zjišťování hesel software k prolomení hesla. Jakmile útočník získá heslo (ve většině případů tzv. zahašované), např. odcizením databáze, pokusí se jej prolomit s pomocí software (většinou probíhá automatizovaně). K prolomení se využívají útoky hrubou silou, slovníkové útoky, hybridní útoky, útoky maskou, rainbow tables attacks a credential stuffing attack.

Brute Force Attack (česky útok hrubou silou) je základním druhem útoku, při kterém se útočník snaží rovnou uhádnout heslo zkoušením různých kombinací znaků.

Dictionary Attack (česky slovníkový útok) je variantou útoku hrubou silou a pracuje s databází potenciálních hesel – zkoušením hesel ze slovníku nebo nejčastěji používaných hesel.

Hybrid Attack (česky hybridní útok) je kombinací útoku hrubou silou a slovníkového útoku. Využívá slovníkový generátor a zároveň znalosti o uživateli.

Mask Attack (česky útok maskou) útočník použije, jakmile zná alespoň část hesla a jeho rozsah. Zná-li kupř. posledních šest znaků, postačí mu pomocí software zjistit prvních šest znaků.

Při **Rainbow Table Attack** (česky útok duhovou tabulkou) útočník použije tabulku se seznamem předem vytvořených zahašovaných hesel a prolomení probíhá tak, že software zjišťuje, které zahašované heslo se shoduje se zahašovaným heslem, jež bylo odcizeno.

Credential Stuffing Attack je způsob útoku, při kterém útočník má přístup k přihlašovacím údajům uživatele do účtu jedné služby a snaží se je využít pro přihlášení do účtu jiné služby. Profituje ze skutečnosti, že uživatelé velmi často používají stejné heslo nebo přihlašovací údaje k přihlašování na několik účtů.

Částečnou obranou proti prolamování hesel je kryptografické hašování hesel.

Kryprografické hašování je proces, při němž je pomocí hašovacího algoritmu („šifrovacího“ matematického mechanismu) převáděn vložený vstup (např. heslo) na výstup („zašifrované“ heslo ve formě unikátního řetězce znaků) zvaný hash

(česky haš). Délka znaků tohoto řetězce a jeho velikost v bitech závisí na typu použitého hašovacího algoritmu.

Hašování se od šifrování odlišuje tím, že neumožňuje zpětný chod – nelze tedy ani při znalosti použitého hašovacího algoritmu přeložit haš zpět na heslo (jak by bylo možno při dešifrování), avšak pokaždé, když ve stejné kódovací znakové sadě na stejný vstup (stejné heslo) použijeme stejný hašovací algoritmus, obdržíme stejný výstup (stejný haš). Tohoto principu je zneužíváno při prolamování hesel – viz níže zejm. technika duhových tabulek.

V současnosti nejčastěji používané hašovací algoritmy jsou Secure Hash Algorithm 2 a 3 (SHA-2, SHA-3), BLAKE, BLAKE2, BLAKE3, RIPEMD, Whirlpool, existují však i další (Gost, Blowfish, Snefru, Tiger, CRC-32, Keccak, Shake aj.).

Některé hašovací algoritmy jsou již zastaralé a zranitelné a není tak obtížné je prolomit, např. Message-Digest 4 a 5 (MD4, MD5) a Secure Hash Algorithm 0 a 1 (SHA-0, SHA-1).

Uveďme si pro názornost příklady haše. Jednoduché heslo „hackingprincess“ zašifrujeme přes online generátor hašů (např. zde: https://codebeautify.org/md5-hash-generator nebo zde: https://dencode.com/hash) pomocí hašovacího algoritmu SHA-2 s výslednou velikostí řetězce 256 bitů (tj. SHA256), SHA-2 s výslednou velikostí řetězce 384 bitů (tj. SHA384) a algoritmu Whirlpool, u něhož je jediná možná volba bitová velikost řetězce 512 bitů. Zde jsou tři výsledné haše (použita byla znaková sada UTF-8):

- hackingprincess -> SHA256 -> ec118e16b367a8e6fadd818224a1c169d1eeb65d4e8bd95545a7cf09afbeefe6

- hackingprincess -> SHA384 -> 82b41496019262a2648362d5b6c85095ee993a8140c9365da05bccf944ba1b5bf48b4236c280e6a0524393a190f9efc5
- hackingprincess -> Whirlpool -> 4766718A6DBB646126EEE4027D3C9266393876A0AD8BD3E7E14257EC8BB6F5ACACAF2D0312932F2234F88BD0D60AAB609C67986916111BF1D4E4C77965D27BD4

K prolamování hesel je využíván software:

Aircrack-ng, Distributed Password Recovery, Offline NT PW & Registry Editor, Ophcrack Live CD, Password Kit Enterprise, Protected Storage Passview, Pst Password, John the Ripper, Hashcat, L0phtCrack, Rainbow Crack, IKECrack,…

2.5.5 SKENOVÁNÍ PORTŮ

Skenování portů je průzkumná metoda zjišťování stavu TCP nebo UDP portů na vzdáleném zařízení. Pomocí nalezených vhodných portů může útočník proniknout do systému. Pro průzkum portů na vlastním zařízení si uživatel vystačí s příkazovou řádkou, potřebuje-li však útočník zjistit status portů na jiném počítači, využije k tomu příslušný software. Samotný sken je proveden vysláním skenovacího paketu. Ve výsledcích technik skenování mohou být nalezeny porty otevřené, zavřené nebo filtrované. Otevřené jsou takové porty, na kterých právě probíhá nějaká služba a mohou být zneužity k napadení počítače, na zavřených portech prozatím žádná služba neběží, což neznamená, že se nemůže v budoucnu změnit, a filtrované jsou porty hlídané firewallem uživatele. Na základě

čísla portu je možné ze seznamu portů TCP a UDP organizací IANA a ICANN vyhledat, na kterém portu se nachází konkrétní služba. V seznamu lze zjistit pouze některé ze služeb, jež se nacházejí na portech od č. 0-49151. Není-li možné dopátrat se ke službě běžící na daném portu, může útočník port dále skenovat a zjistit jak probíhající službu, tak konkrétní program služby. Při této fázi je již nutné komunikovat s počítačem uživatele prostřednictvím aplikačních protokolů, v důsledku čehož jsou do počítače napadeného ukládány záznamy o provedených akcích/změnách, tzv. logy – útok je tedy následně v systému zjistitelný.

Technik skenování existuje více – Pingování, UDP skenování, SYN skenování (tzv. napůl otevřené skenování), XMAS skenování, Connect skenování, FIN, Null, ACK skenování, Window skenování, Idle skenování.

Ke skenování portů se využívá *Nmap (Network Mapper), Zenmap, Angry IP Scanner, Advanced Port Scanner*.

2.5.6 NARUŠENÍ TELEFONNÍ SÍTĚ

Phreaking je metoda napojení se na cizí telefonní linku v rozvodnicích, veřejných telefonních budkách nebo přímo na telefonní vedení s úmyslem čerpání určitých výhod – hovory zdarma kamkoliv, surfování po internetu zdarma nebo např. odposlouchávání cizích telefonních hovorů.[17]

2.5.7 DOS, DDOS A DRDOS ÚTOKY

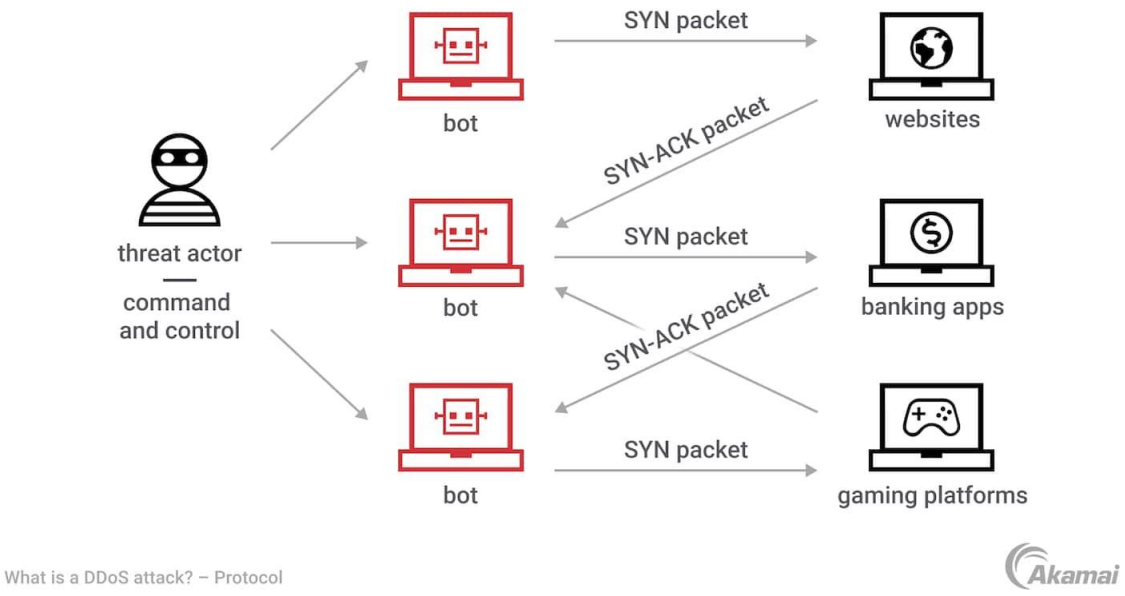
DoS (Denial of Service), česky odepření služby, je způsob napadení webové stránky nebo služby, kterým se ji útočník snaží vyřadit z funkce nebo znepřístupnit

[17] https://cs.wikipedia.org/wiki/Phreaking

uživatelům, a to tím, že stránku nebo službu zahltí velkým množstvím požadavků, příp. zneužije nějaké chyby.

DDoS (Distributed Denial of Service), česky distribuované odepření služby, je podtypem DoS, při kterém útočník využije ohromné množství počítačů z různých geografických lokalit. Pro účely DDoS útoků hackeři běžně využívají nakažené počítače nicnetušících lidí, tzv. boty.

DRDoS (Distributed Reflected Denial of Service), česky distribuované odražené odepření služby, je sofistikovaná forma DoS útoku. Útočník odešle na velké množství počítačů požadavky, které mají jako svou zdrojovou adresu uvedenou adresu nicnetušícího uživatele. Počítač uživatele je poté zahlcen odpověďmi na takto podvržené požadavky, proto je někdy tento útok označován jako Spoofed DDoS Attack, česky podvržený distribuovaný DoS útok.[18]



Obrázek 4 - DDoS útok

[18] https://cs.wikipedia.org/wiki/Denial_of_service

DoS a DDoS útoky můžeme rozdělit do tří základních skupin s uvedením nejznámějších druhů útoků:

1) **Volumetrické**

Volumetrické útoky jsou nejstarším druhem útoků. Zahlcují kapacitu šířky pásma mezi sítí napadeného a internetem nebo uvnitř sítě napadeného. Největší volumetrické útoky v současné době jsou měřeny v terabitech za sekundu (Tbit/s), tj. cca 9 tis. průměrných internetových připojení.

ICMP (Ping) Flood, česky záplava tzv. ping pakety, je útok, při kterém je cílem zahltit náhodné porty vzdáleného zařízení pomocí tzv. ping paketů (Echo Request Packets), které měří rychlost internetu mezi dvěma zařízeními připojenými k síti. Pakety jsou útočníkem odesílány tak rychle, jak je jen možné, bez vyčkání na odpověď, přičemž spotřebovávají jak odchozí, tak příchozí šířku přenosového frekvenčního pásma, neboť server napadeného obvykle též reaguje na ping pakety, a to odesláním zpětných ping paketů (Echo Reply Packets). Uvedený proces výrazně zpomaluje systém serveru napadeného.

Cílem **UDP DDoS Flood Attack**, česky UDP DDoS záplavového útoku, je zahltit náhodné porty vzdáleného zařízení pomocí UDP paketů, což způsobí, že zařízení neustálým odposlechem portů a následným zasíláním zpětných chybových odpovědí o nedostupnosti cíle paketu čerpá ze svých zdrojů a může způsobit nepřístupnost služeb na těchto zdrojích závislých.

SSDP (Simple Service Discovery Protocol) DDoS Attack, distribuovaný útok odepření služby s využitím jednoduchého protokolu vyhledávání služeb. Při tomto útoku dochází ke zneužití hardwarových zařízení (nalezených skenováním)

fungujících na bázi protokolu UPnP (universal plug and play) zapojených do sítě, na která útočník pomocí botnetu vyšle zjišťovací UDP paket s podvrženou zdrojovou adresou oběti. Zjišťovací paket obsahuje požadavek na zaslání co nejvíce dat. Každé zařízení tedy odešle oběti co nejvíce dat a server napadeného je jimi zahlcen do takové míry, že může vést k odepření služby běžnému provozu.

Při **DNS (Domain Name System) DDoS Flood Attack**, česky záplavovém útoku na systém doménových jmen, útočník využije botnetu k zaplavení serveru DNS konkrétní domény, čímž naruší překlad DNS pro danou doménu a ohrozí web nebo schopnost webové aplikace reagovat na běžný provoz.

2) Protokolové

Protokolové útoky zneužívají konstrukci protokolu TCP/IP k vyčerpání zdrojů cílového systému. K dosažení cíle využívají speciálně vytvořených paketů, a jsou tedy měřeny v paketech za sekundu (PPS). Největší útoky v minulosti prozatím dosáhly až stovek milionů paketů.

Nuke DoS Attack je typ zastaralého útoku, při němž útočník odesílá frangmentované nebo poškozené pakety (obvykle ICMP) na počítač oběti, jehož operační systém se zpomalí a zastaví. Následně dojde k pádu zranitelného systému, často se zobrazením modré obrazovky smrti (BSoD, Blue Screen of Death).

SYN Flood, česky záplava pomocí SYN (synchronizačních) požadavků, je útok, při němž útočník využívá slabiny v rámci třícestného potřesení rukou, tzv. three ways handshake, a odešle velké množství SYN požadavků, aniž by poté

odpověděl na odezvu SYN-ACK (synchronize-acknowledge, česky synchronizovat-potvrdit), případně zašle mnoho SYN požadavků z podvržené IP adresy. V každém případě systém napadeného vyčkává na poslední signál ACK pro každý z požadavků od útočníka, dokud nejsou vytvořena spojení nová, a tedy zůstává stále třícestné potřesení rukou nedokončené. Proces vyčkávání čerpá zdroje systému napadeného a může v důsledku vyústit v odepření služby.

ACK DDoS Flood Attack, česky záplavový DDoS útok pomocí ACK, při kterém se útočník z několika zařízení pokusí přetížit server nevyžádanými pakety TCP ACK, což způsobí zpomalení až zhroucení serveru a odepření služby legitimním požadavkům.

SYN-ACK DoS/DDoS Flood Attack, česky záplavový SYN-ACK DoS/DDoS útok, probíhá odesláním falešných paketů SYN-ACK na cílový server vysokou rychlostí. Server může být v důsledku zjišťování, proč mu byl paket zaslán, natolik zaneprázdněn, že odmítne službu ostatním legitimním požadavkům.

Teardrop DDoS Attack, česky slzný útok, je útokem, při kterém útočník odešle záměrně rozfragmentovaný informační paket na server a zneužije chybu zabezpečení protokolu TCP/IP vzniklou při opětovném sestavování paketu. V důsledku této zranitelnosti, kterou obsahují starší verze operačních systémů Windows a Linux, server nemůže paket znovu sestavit, dojde k jeho přetížení a selže systém nebo aplikace, jež paket zpracovává.

Smurf DDoS Attack, česky šmoulí DDoS útok, je útok, při němž útočník zašle pomocí programu smurf.c (Smurf, česky šmoula) velké množství ICMP paketů s podvrženou zdrojovou adresou, tj. adresou oběti, na mnoho zařízení, jež následně odpovídají na ICMP pakety na podvrženou adresu a zahltí oběť nevyžádaným síťovým provozem. Již se nepoužívá.

Při útoku zvaném **Ping of Death**, česky ping smrti, útočník odešle do systému oběti abnormálně velký na části rozfragmentovaný ping paket, který je chybový nebo zavirovaný. Po svém opětovném složení paket způsobí v napadeném systému přetečení zásobníku a vede k pádu systému. Tento útok se již nepoužívá.

3) Útoky na aplikační vrstvě

Útoky na aplikační vrstvě se zaměřují na veřejně přístupné aplikace prostřednictvím velkého objemu podvrženého nebo falešného provozu. Jsou měřeny v desítkách milionů požadavků za sekundu (RPS).

HTTP Flood Attack, česky HTTP záplavový útok, využívá zahlcení serveru pomocí internetových požadavků v prohlížeči. Útok probíhá pomocí botnetu. Možné jsou dva způsoby – buďto útok typu HTTP GET, při kterém boty zasílají mnoho požadavků na zobrazení obrázků, souborů či jiných prostředků z cílového serveru, nebo HTTP POST, při němž je odesíláno velké množství požadavků POST na cílový server prostřednictvím formuláře na webu. V prvním případě dojde k odmítnutí služby pro ostatní legitimní požadavky, ve druhém dojde k zahlcení kapacity serveru a odmítnutí služby.

Nízký a pomalý DoS/DDoS útok bývá proveden pomocí nástrojů Slowloris, R.U.D.Y. (R-U-DEAD-YET?) nebo Sockstress. Slowloris odesílá pouze části hlaviček HTTP, v důsledku čehož server ponechává otevřené spojení. R.U.D.Y. generuje požadavky HTTP POST, sděluje serveru, kolik dat má očekávat, díky čemuž server udržuje otevřené spojení, a posléze zasílá data velmi pomalu. Sockstress využívá slabiny v třícestném ověřování TCP/IP a vytváří spojení neomezené. Je velmi těžké odlišit provoz způsobený útokem od běžného provozu, jelikož přenos dat je sice velmi pomalý, ale zároveň dostatečně rychlý na to, aby nevypršelo časové spojení se serverem. Útok se zaměřuje na prostředky aplikací nebo serverů, a tím jejich procesy výrazně zpomaluje, čímž může docházet ke zpomalení nebo odepření služeb legitimním uživatelům. Útok lze spustit z jednoho počítače, nevyžaduje se botnet.

Při **DNS Amplification Attack**, česky zesilujícím útoku na DNS, útočník zašle prostřednictvím několika málo počítačů na vybrané DNS servery, jež vedou mnoho záznamů o doménách (např. o doménách 3. řádu), žádost o sdělení všech záznamů o doménách, s tím, že podvrhne svou IP adresu dotazujícího a nahradí ji adresou oběti. Efekt zesílení spočívá v principu, že na DNS server směřuje velikostně malý požadavek od útočníka, kdežto oběť je v důsledku neustále příchozích výrazně větších paketů odpovědí naprosto zaplavena, což její server vyřadí z provozu.

Memcached Amplification DDoS Attack, česky zesilující DDoS útok s využitím UDP memcached serverů, které se používají pro zrychlení webových stránek a sítí, je typ útoku, při kterém útočník sám nebo pomocí botnetů zahltí oběť internetovým provozem. Útočník podvrhne zdrojovou adresu (změní na adresu

oběti) HTTP GET požadavků na UDP memcached servery, které následně odpoví oběti a zahltí provozem jeho zdroje, což vyústí v odepření služby požadavkům běžného provozu.

Při **NTP Amplification DDoS Attack**, česky NTP zesilovacím DDoS útoku, útočník využije botnetu k zaslání UDP paketů s podvrženou IP adresou oběti na NTP (Network Time Protocol) server, který má povolený příkaz monlist. Pomocí příkazu monlist pak každý UDP paket odešle požadavek na veřejně přístupné NTP servery, jež odpoví výslednými daty na podvrženou adresu a zahltí okolní síťovou infrastrukturu napadeného záplavou provozu a vede k odmítnutí služby.

QUIC DDoS Flood Attack, česky záplavový QUIC DDoS útok, je zahlcení cílového serveru daty odeslanými UDP zašifrovanými (pomocí TLS) pakety přes QUIC transportní protokol, což výrazně zpomaluje službu legitimním uživatelům nebo vyřadí server z provozu.

QUIC DDoS Reflection Attack, česky reflexní QUIC DDoS útok, je podvržení IP zdrojové adresy útočníka za adresu oběti a vyžádání si informací z několika serverů pomocí zprávy „hello“, na který servery odpovídají TLS zašifrovanou zprávou ACK, tedy větším množstvím dat než obsahuje zpráva útočníka. Odpovědi z jednotlivých serverů následně obdrží oběť.

Ke speciálním útokům, jež nelze podřadit pod jednotlivé kategorie, patří dále například DDoS útoky na kryptoměny, Ransom DDoS útoky, Peer-to-Peer útok nebo vícevektorové DDoS útoky.

DDoS útoky na kryptoměny se zaměřují na kryptoměnové burzy mincí a snaží se přetížit cíl falešným provozem. Nejčastěji využívají útoků SSDP, NTP zesilovacích útoků a útoků na aplikační vrstvě.

Ransom DDoS Attack, česky DDoS útok za výkupné, je metoda, při níž útočníci slibují zastavení probíhajícího DDoS útoku, event. neprovedení plánovaného DDoS útoku výměnou za peníze.[19]

Peer-to-Peer (P2P) DDoS Attack, česky DDoS útok Klient-Klient, je způsob útoku využívající šířky pásma a Peer-to-Peer sítě. Útok je zesílen prostřednictvím jednotlivých uživatelů sítě a je zaměřen vůči cíli mimo P2P síť.

Při použití **Multi-Vector DDos Attack**, česky vícevektorového DDoS útoku útočníci využívají několik (někdy i osm nebo více) forem (tzv. vektorů) DDoS útoků zároveň, přičemž vrství vektory najednou, nebo v průběhu útoku vektor změní. Často jsou využívány kombinace volumetrických útoků s útoky na aplikační vrstvě. Sofistikované vícevektorové útoky již lze zařadit pod APT – pokročilým trvalým hrozbám. Vícevektorové útoky je velmi obtížné blokovat, zejména pokud jsou útočníkem prováděny automatizovaně a na případnou obranu reagují v reálném čase. Obvykle se jedná o napadání e-mailů, databází, webových stránek za

[19] Learning. *CLOUDFLARE* [online]. [cit. 2023-03-12]. Dostupné z: https://www.cloudflare.com/learning/

účelem ničení sítě a dlouhodobého odepření služby oprávněným požadavkům nebo získávání citlivých dat.[20]

2.5.8 ÚNOSY DNS SERVERU

Únos / přesměrování DNS (Domain Name Server Hijacking / Redirecting) je typ útoku, při kterém útočník přesměruje požadavek uživatele z jedné IP adresy, kterou měl uživatel zamýšlen navštívit, na jinou prostřednictvím infikování DNS malwarem. Využívá se ve spojení s pharmingem.

Při **únosu místního DNS** útočník počítač uživatele napadne malware – trojským koněm a následně změní místní nastavení DNS, aby uživatele přesměroval na škodlivou stránku.

Únos DNS routeru lze provést přenastavením DNS adresy routeru na jinou. Útočník se k nastavení routeru dostane, pokud má router slabé heslo nebo stále původní heslo, se kterým je dodáván, event. nalezne jinou chybu v software routeru.

Při **únos DNS technikou Man-in-the-Middle, tzv. DNS Spoofing** (viz výše) napadne útočník mezipaměť DNS.

Nečestný DNS server je typ DNS útoku, při kterém útočník napadne DNS a změní záznamy DNS, tak aby požadavky uživatele přesměrovaly zcela jinam (na falešnou stránku útočníka)[21]

---

[20] Understanding and Stopping MultiVector DDoS Attacks. *CORERO* [online]. [cit. 2023-03-12]. Dostupné z: https://www.corero.com/understanding-and-stopping-multi-vector-ddos-attacks/

[21] DNS Hijack. *IPSHU* [online]. [cit. 2023-03-12]. Dostupné z: https://cs.ipshu.com/dns_hijack

2.5.9 VYHLEDÁVÁNÍ ZRANITELNOSTÍ

Web Debugging

Web Debugging, česky ladění chyb na webu, je metoda vyhledávání a oprava chyb ve zdrojovém kódu webové stránky. Nejedná se primárně o útočnou metodu, ale je možné ji pro útok zneužít, tím, že útočník vyhledá zranitelnost a využije ji např. pro XSS útok (viz níže).

Directory Traversal Attacks

Directory Traversal (File Path Traversal) Attacks, česky útoky na procházení adresáře (procházení cesty k souborům), jsou útoky zneužití protokolu HTTP, konkrétně chyb zabezpečení v adresářích webového serveru nebo chyb zabezpečení v kódu webové stránky, které mají za cíl získání neoprávněného přístupu k soukromým informacím uloženým na webovém serveru a jejich případné další využití. Návštěvník stránky by měl mít v běžném případě přístup pouze k takovým souborům, který server, na kterém webová aplikace běží, umožní. Webové servery používají k omezení přístupu kořenový adresář a seznamy řízení přístupu (tzv. Acces Control Lists), kde kořenový adresář je část přístupná návštěvníkům a seznamy řízení přístupu jsou nastavení přístupových práv, oprávnění k prohlížení, úpravě nebo spuštění jednotlivých souborů nakonfigurované správcem webového serveru. Je-li filtrování nebo ověřování vstupu od návštěvníka stránky nedostatečné, může návštěvník v případě, že je útočníkem, zadat do řádku s URL adresou URL adresu upravenou pomocí příkazu, a získat tak přístup k souborům na serveru mimo kořenový adresář.

Web Cache Poisoning

Web Cache Poisoning, česky otrava webové mezipaměti, je metoda, při které útočník vloží infikovaná data do serveru mezipaměti webového serveru (např. server poskytovatele internetových služeb). Server mezipaměti je dočasným úložištěm pro data vzdáleného webového serveru. Jakmile chce uživatel navštívit webovou stránku, data ze vzdáleného serveru se mu zašlou a zároveň se jejich kopie uloží na server mezipaměti, který se nachází v bližší vzdálenosti uživatele. Tento server mezipaměti mohou následně využívat další návštěvníci nacházející se v oblasti, pro kterou je server mezipaměti určen. Místo toho, aby byl požadavek na zobrazení webové stránky zaslán vzdálenému serveru, je nejprve zasílán serveru mezipaměti, který zjistí, zda se stránka v jeho úložišti nenachází, pokud nikoliv, je požadavek předán na vzdálený server. V důsledku toho, že k serveru mezipaměti webového serveru mají přístup i jiní uživatelé v dané lokalitě, mohou být napadeni, pokud se snaží všichni přistoupit ke stejné stránce a jestliže útočník vloží škodlivá data do serveru mezipaměti.

HTTP Response Splitting Attacks (CRLF Injection)

HTTP Response Splitting Attacks (CRLF Injection), česky útoky na rozdělení odpovědí (vkládání CRLF), jsou útoky manipulující s protokolem HTTP u zranitelných webových aplikací. CRLF odděluje HTTP hlavičku a HTML tělo stránky. Útočník dá serveru falešné sdělení o ukončení HTTP hlavičky tím, že vloží pomocí adresního řádku údaj CRLF spolu s dalším záznamem, např. příkaz s malware. Navštívená adresa spolu se záznamem bude zaznamenána v systému webové aplikace a může být využita k otrávení webové mezipaměti.

Web Server Misconfiguration

Web Server Misconfiguration, česky nesprávná nebo neoptimální konfigurace systému nebo jeho části může vést ke zranitelnosti. Servery jsou často dodávány

s ukázkovými aplikacemi, konfiguračními soubory, skripty, webovými stránkami, účty, hesly, povolenými službami a funkcemi – např. správa obsahu, funkce ladění, vzdálené správy. Mohou mít neošetřený přístup pro správu souborů nebo nesprávně nastavené certifikáty, šifrování apod. Všechny tyto problémy mohou vést k tomu, že je útočník nějakým způsobem využije, např. metodou procházení cest souborů, vkládání SQL a jiných příkazů.

Website Defacement

Website Defacement, česky znehodnocení webové stránky, je útokem, který změní vizuální vzhled webové stránky nebo poškodí její funkčnost. Bývá proveden na základě zjištěné zranitelnosti (např. neošetřené vstupy od anonymních uživatelů), která je dále využita různými technikami, zejm. vkládáním SQL, XSS nebo procházením cest souborů.

Obrázek 5 - WebSite Defacement

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS), česky skriptování mezi weby je metoda narušení webových stránek umožňující spouštět cizí skripty nebo kódy v prohlížeči oběti. Využívá se pro napadení stránek, které jsou na takový útok náchylné, a to především k poškození vzhledu stránky, získání důvěrných dat návštěvníků, sledování uživatelů nebo přesměrování webu na jiný. Cílí tedy na ostatní uživatele stránky. Princip spočívá v tom, že útočník místo dat do okna formuláře nebo

vyhledávání na webové stránce zadá Javascript nebo HTML kód, který se v důsledku chybného zabezpečení ověřování vstupů na stránce provede. Existuje několik typů XSS – typu 0, I, II nebo kombinovaný XSS.

Pro zranitelnosti typu 0 XSS se využívá software *Sboxr*.

Watering Hole Attack

Watering Hole Attack, česky útok na napajedlo, je metoda útoku na jednotlivce, skupiny nebo celou organizaci. Využívá technik sociálního inženýrství nebo distribuce malware. Útočník hádá, které webové stránky jsou nejvíce navštěvované, a ty se pokusí infikovat na základě zjištěné zranitelnosti, případně přesměrovat z nich uživatele na podvodnou stránku. Útočník spoléhá na to, že některý z návštěvníků se nakazí.

Doxing a kompromitace webových stránek

Doxing je označení pro metodu veřejného odhalení osobních informací, které útočník neoprávněně zjistil o uživateli nebo společnosti např. kompromitací webových stránek, a to za účelem jejich zdiskreditování, vydírání, pomsty apod.

Kompromitace webových stránek označuje neoprávněný přístup k těmto stránkám a jejich datům na základě různých technik (napadení webového serveru, vkládání SQL, XSS, využití nalezené chyby v zabezpečení aj. zranitelností).

Buffer Overflowing

Buffer Overflowing, česky přetečení vyrovnávací paměti, je metoda, při níž hacker daty přeplní vyrovnávací pamět RAM určenou v počítači pro dočasné ukládání dat. V důsledku toho se začnou data zapisovat do vedlejšího úložiště a mohou přepsat jiná data, o která tímto způsobem uživatel přijde, event. dojde k selhání celého

znestabilizovaného systému. Pokud není přetečení zabraňováno samotným operačním systémem počítače, může jej útočník způsobit např. využitím chyby v kódování aplikace, jejíž kód přetečení nezabraňuje, a to tak, že aplikaci zašle určitý typ kódu, který je schopen toto přetečení zajistit.

Command Injection (Shell Injection)

Zranitelnosti mohou být vyhledávány nejen ve zdrojových kódech, které jsou přístupné, ale také v programech, ke kterým není kód zveřejněn, a to s pomocí disassembleru a debuggeru (viz cracking). Zranitelnost v aplikaci může být využita tak, že útočník vpraví příkaz, tzv. shellcode, do neošetřeného vstupu webové aplikace, a tím způsobí útok nebo kompletní převzetí operačního systému zařízení nebo serveru, na kterém aplikace běží. Shellcode je drobný příkaz upravený do speciální podoby strojového kódu (viz cracking).

Zero Day Attack

Zero Day Attack, česky útok nultého dne, nebo též využívání zranitelností nultého dne, je metoda zneužití odhalené programátorské chyby v nově vydaném software nebo aktualizaci. Na základě chyby jsou útočníkem vytvářeny tzv. exploity (programy s malware nebo popisy, které znázorňují, jak chyb v programu využít). Do vydání opravy software nebo aktualizace se uživatel stále nachází v původní ohrožené pozici, tzv. nultém dni.

Pivoting

Pivoting je metodou, kdy se útočník pokouší prostřednictvím stroje, který napadl a získal k němu přístup, využít další přístroje v síti.

Reverzní inženýrství

Při reverzním inženýrství útočník využije kopii software (příp. hardware), který chce napadnout, k tomu, aby zjistil, jak daný produkt funguje, jak je zkomponován, aniž by znal jeho zdrojový kód. Zároveň vyhledává zranitelnosti a bezpečnostní prvky, které by mohl následně zneužít nebo obejít. Využívá při nich kompilátorů, disassemblerů a debuggerů.

Software na vyhledávání zranitelností ve webových aplikacích: *Invicti (dříve Netsparker), Fortify WebInspect, Acunetix, Tenable.io,…*

2.5.10 ÚTOKY NA DATABÁZE

SQL Injection

SQL Injection, česky vkládání SQL, je technika využívající k útoku strukturovaný dotazovací jazyk SQL (Structured Query Language) určený pro ukládání, manipulaci a načítání dat z relačních databází. Na základě neošetřeného vstupu, např. prostřednictvím formuláře na webu nebo přihlašovacího formuláře, může útočník nejčastěji s pomocí chybových hlášek zjistit, jaká databáze je využita, a jakým způsobem funguje. Na základě odpovědí serveru na své dotazy dále vkládá jiné dotazy, které neošetřený vstup na stránce provede, a útočník se postupně dostane k citlivým údajům skrytě uloženým v databázi nebo položky z databáze dokonce odstraní. Na internetu jsou navíc přístupné seznamy s informacemi, příkazy a klíčovými slovy týkajícími se procesů probíhajících v jednotlivých druzích relačních databází včetně jejich zranitelností, což tyto útoky usnadňuje.

Používaný software: *SQL Map, McAfee Vulnerability Manager,…*

2.5.11 OSTATNÍ METODY

Cryptojacking

Cryptojacking je relativně nová metoda páchání kybernetické kriminality, při které zločinci využívají výkon počítače uživatele bez jeho vědomí k těžbě kryptoměn, a to prostřednictvím speciálního programu s malware (tzv. cryptomining malware), který pracuje tajně na pozadí infikovaného počítače.

Formjacking

Při tomto velice nebezpečném útoku vkládají pachatelé do formuláře (zpravidla platebního) na webové stránce Javascript nebo jiný kód s malware, který jim následně odesílá platební údaje, jež uživatelé do formuláře zadají. Odcizené údaje mohou přeprodávat.

Peer-to-Peer Attack

Peer-to-Peer Attack, česky útok Klient-Klient, je způsob útoku, při kterém jsou útočník a jeho oběť ve stejné síti (např. veřejný hotspot), a útočník se snaží uskutečnit útok v rámci této sítě využitím zranitelnosti (např. přetečení zásobníku) některé síťové aplikace, např. program BitTorrent. Peer-to-Peer Attack bývá nejčastěji využit k předání malware, útoku nultého dne nebo speciálního volumetrického DDoS útoku.

Cracking

Metoda crackingu slouží k odstraňování ochranných nebo omezujících prvků ze software s neveřejným chráněným zdrojovým kódem. Prováděním crackingu jsou porušována autorská práva. Odstranění ochrany programu může být dosaženo pomocí několika technik, nejčastěji provedením tzv. disassemblingu a debuggingu.

Při provádění disassemblingu je zapotřebí speciálního software – disassembleru. Nejprve je vyžadováno převedení programu do formy strojového kódu prostřednictvím software editoru (např. HxD Hex Editor) a poté je ze strojového kódu dále pomocí disassembleru (např. Capstone Engine) získán kód se syntaxí podporovanou procesorem zařízení, tzv. assembly code, česky jazyk symbolických adres. Jazyk symbolických adres (instrukcí) již je pro člověka čitelný a pokouší se znázornit tentýž program s totožnými funkcemi jiným způsobem než jej znázorňuje zdrojový kód, který byl použit pro tvorbu programu (např. Python, Java nebo C – „matka jazyků“) a který cracker nezná – mnoho programů má z pochopitelných důvodů chráněný neveřejný kód (zejm. snaha jiných o kopírování programu). Poté může cracker ve výstupu z disassembleru, tj. v jazyce symbolických adres, za pomoci debuggeru sledovat, jak se program chová a zda by se v něm na nějakém místě nedala nalézt zranitelnost nebo jakým způsobem by bylo možno odstranit ochranu proti kopírování.

Využívá se také tento software: *Anydvd (HD), DVD Shrink, Vista Loader*.

Lockpicking

Lockpicking, česky „vyháčkování“ je v běžném případě metodou přímého útoku. Pachatel se pokouší pomůckami, nejčastěji planžetami, opatrně proniknout do zámku a otevřít dveře. V současné době existují aplikace, např. KeyDecoder, které umožňují, aby si útočník mechanický klíč vyfotografoval přes telefon a následně si nechal totožný klíč vyrobit. Aplikace mu sama detailně vyměří a zobrazí parametry klíče. Je sice potřeba, aby se pachatel nějakým způsobem ke klíči dostal a „zapůjčil si jej“ pro ofocení, není však nutné, aby jej odcizil.

Odcizení domény

Odcizení domény je možné získáním přihlašovacích údajů k účtu u poskytovatele domény. K přihlašovacím údajům se útočníci dostanou buďto technikami

sociálního inženýrství, nebo hrubou silou (např. hádání hesla). Poté provedou změny v konkrétní informaci k DNS, tj. v IP adrese.

Útoky na volání přes internet (VoIP)

Útoky na VoIP (Voice Internet Protocol) jsou útoky na servery provozující službu volání přes internet. Útočníci používají techniky vyhledávání zranitelností ve webové aplikaci, vzdálený odposlech nebo útoky na síť nebo poskytovatele internetového připojení.

Útoky na Průmysl 4.0

K útokům na průmysl řadíme útoky na biometrické systémy, na různé typy průmyslových řídicích systémů (ICS), na analyticko-kognitivní výpočetní techniku nebo techniku využívající strojové učení (robotika a umělá inteligence), systémy pro dohledové řízení a sběr dat (SCADA), cloud computing, internet věcí (IoT), průmyslový internet věcí (IIoT) a útoky na digitální měny a nezaměnitelné tokeny, virtuální realitu a kvantové počítače.

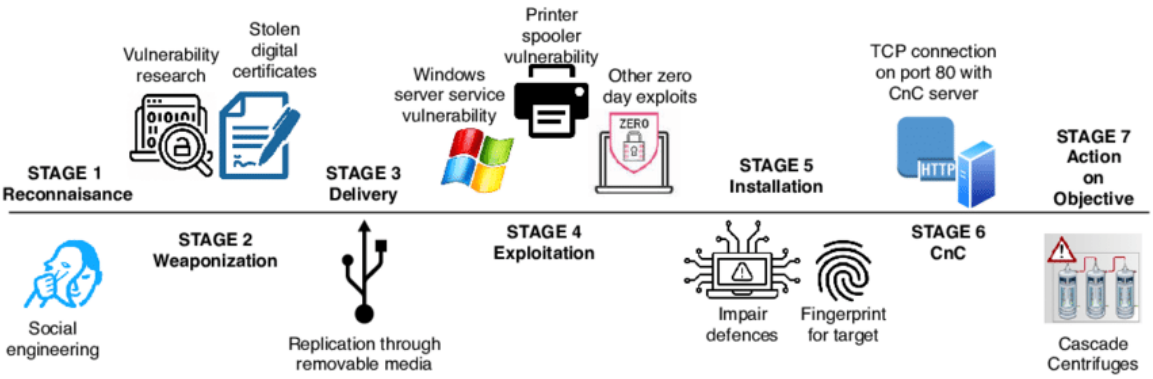
- Útoky na biometrické systémy – APT, poskytnutí falešného biometrického vzorku senzoru, falšování sady funkcí, přepsání funkce aplikace, útok trojským koněm a jiným malware,…
- Útoky na ICS systémy – využití chyb v konfiguraci a zastaralého software nebo hardware, útoky malware (zejm. ransomware), narušení a změna přístupových oprávnění, APT, DDoS útoky…
- Útoky na umělou inteligenci a robotiku – APT, deepfake útoky, malware, phishing, DDoS útoky,..
- Útoky na SCADA systémy – APT, malware, zneužití zranitelnosti,..
- Útoky na cloud computing – chybná konfigurace, prolamování hesel, SQL injection a krádeže dat, škodlivé aktivity insiderů,…

- Útoky na internet věcí – krádeže dat, phishing, podvržení, zneužití ponechaného výchozího nastavení zařzení, DDoS útoky, malware,…
- Útoky na průmyslový internet věcí – desynchronizace koncových bodů pomocí falešných paketů, DDoS záplava SYN, útok na transportní protokol MQTT (využití zranitelnosti),...
  - ***Internet věcí*** je síť chytrých fyzických zařízení, které mají zabudovanou elektroniku, vlastní software, pohyblivé části a senzory, jimiž jsou schopné automatizovaně, bezdrátově a v reálném čase komunikovat s ostatními zařízeními, aplikacemi a systémy. Některá z těchto zařízení jsou schopná reagovat na vstupy člověka, svými charakteristikami sem tedy spadají i biometrické systémy. Zařízení internetu věcí využívají speciálně konstruovaných komunikačních protokolů, případně HTTP nebo HTTPS protokolu.[22]
  - Zařízení ***průmyslového internetu věcí*** tvoří základ Průmyslu 4.0
- Útoky na digitální měny a nezaměnitelné tokeny – podvody s bankomaty na kryptoměny, provedení podvodných transakcí, cryptojacking, ransomware, útoky na kryptografii,…
- Útoky na virtuální realitu – krádeže dat, neověřený nákup doplňkových zařízení (např. bootleg gadgets) a následné stáhnutí malware nebo poškození dat, podvody při online nakupování, sociální inženýrství, …
- Útoky na kvantové počítače – druhy typických útoků jsou prozatím otázkou budoucnosti

Pokročilé kybernetické útoky typu APT

[22] Internet věcí – Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_v%C4%9Bc%C3%AD

APT (Advanced Persistent Threat), česky pokročilá trvalá hrozba, je označení pro útoky, které odolávají v čase a jsou sofistikovaného charakteru. Jejich účelem jsou většinou rozsáhlé škody v systémech a mohou zůstávat delší dobu nepozorované, neodhalené nebo recidivovat. Pachatelé těchto útoků získají přístup k systému klasickými metodami, především prostřednictvím distribuce malware nebo zneužití zranitelnosti aplikace, přičemž se snaží o následné udržení možnosti tohoto přístupu (ponechaná otevřená vrátka) a odstraňování stop po svých návštěvách. V rámci systému se poté útočník pokouší s pomocí technik prolamování hesel a dešifrování získávat další přístupová oprávnění k propojeným systémům, serverům, databázím atd., provádí změny v těchto systémech a získávají, mažou nebo pozměňují citlivá data.



Obrázek 6 - Stuxnet (APT)

Další vybraný software

OpenVAS - skenování zranitelností; **Qualys Guard** - vyhledávání zranitelností v síti; **Maltego** - program pro dolování dat z otevřených zdrojů OSINT; **Shark** - ovládání PC přes internet, aniž by o tom uživatel cizího PC věděl; **Nikto** - skener bezpečnostních problémů webového serveru; **SolarWinds**, **SoftPerfect** - monitoring sítě a správa IT infrastruktury; **Fing** - síťový skener; **Security Event**

Manager - automatizuje správu řízení bezpečnosti; **LiveAction** - analýza sítě a její management; **Medusa** - platforma pro vývojáře javascriptu; **Nmap NSE** - skriptovací engine **Nmap**; **Intruder** - skener online zranitelností založený na cloudu

2.6 S využitím hardware

2.6.1 VYBRANÉ METODY

Keysniffing a mousejacking

Keysniffer (Keyboard Sniffer) je hardwarové zařízení, které slouží ke snímání úhozů bezdrátové klávesnice s dodávaným USB hardwarovým klíčem. Každý úhoz klávesnice je před svým odesláním do hardwarového klíče převáděn na nezašifrovaný radiofrekvenční paket. Tento paket může být následně útočníkem odposlechnut keysnifferem ze vzdálenosti několika metrů. Stejná technika využívaná pro odposlech bezdrátové myši je nazývána mousejacking.

Skimming

Pachatel v rámci skimmingu instaluje do bankomatu speciální zařízení na snímání magnetického proužku platební karty a zadaných kláves – může se jednat o minikameru nebo sofistikovaný keylogger. Následně údaje nahraje na padělanou platební kartu a využije ji pro výběr hotovosti.

GPS Spoofing

Útočník může pomocí rádiového zařízení nacházejícího se v blízkosti GPS (např. Software Defined Radio SDR) a vysílajícího falešné signály rušit GPS signál.

2.6.2 HARDWAROVÉ NÁSTROJE

Hardwarové nástroje (mnohé z nich běžného použití, zneužívané hackery):

Ubertooth 1, Ubertooth 2 Alfa, Raspberry Pi, Arduino MKR-1000, Digispark, Attify Badge, Bluetooth 4.0 Low Energy Micro Adapter Bluetooth Dongle, Multiblue Dongle USB Bluetooth, Wifi Deauther, Alfa Wifi Adapter, RTL-SDR, Nokia 900, WiFi Yagi Antenna, Kali Nethunter, USB Rubber Ducky, Proxmark 3, Hack RF One, Keylogger Hardware, LAN Turtle, WiFi Pineapple (sada nástrojů), Keysweeper, Magspoof (Alfa AWUS036NH).

3. Opatření

V této kapitole bych se chtěla zaměřit na účinná opatření proti výše uvedeným hrozbám.

3.1 Právní předpisy

Protiopatření by byla sama o sobě zbytečná, pokud by nebylo známo, proti jaké hrozbě se uplatňují, kdo a v jakých případech by je měl uplatňovat a jakým způsobem a s kým by měl spolupracovat. Z těchto důvodů je vhodné ujasnit si, kdo a podle jakých právních předpisů spravuje kritické systémy, komu je zadáván dohled nad těmito systémy a kdo má povinnost podílet se na obraně při jejich ohrožení.

Mezinárodní dokumenty a spolupráce

Směrnice Evropského parlamentu a Rady 2013/40/EU z 12. 8. 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.

Nařízení eIDAS, resp. Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Usnesení Evropského parlamentu ze dne 3. 10. 2017 o boji proti kyberkriminalitě (2017/2068(INI)).

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. 4. 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, tzv. GDPR).

Úmluva Rady Evropy o počítačové kriminalitě z 1. 7. 2004, sdělení č. 104/2013 Sb., a její dodatkový protokol z 1. 3. 2006.

Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. 3. 2017, o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.

GovCERT (viz níže) je členem FIRST, TF-CSIRT a CSIRT NETWORK.

NÚKIB (viz níže) mezinárodně spolupracuje s NATO, EU (např. agentura ENISA), dále s americkými FBI, DHS, Ministerstvem obrany, NSA, BotNet Feed a Shadowserver Foundation, jihokorejskou NIS, s izraelskými MalMab a National Cyber Bureau, s pracovištěm Cyber Attaché ve Washingtonu D.C., Tel Avivu a Brusel a spolu s Ministerstvem zahraničních věcí zastupuje ČR v OSN, OBSE, OECD, ITU apod. co se týče oblasti kyberbezpečnosti.

CZ.NIC (viz níže) spolupracuje s ICANN, mezinárodní organizací pro správu internetu.

Směrnice NIS

Účelem Směrnice NIS, o bezpečnosti sítí a informací, jakožto Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. 7. 2016 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii, účinné od 8. 7. 2016, je harmonizovat právní úpravu členských státu EU a sjednotit standard úrovně kybernetické bezpečnosti. Směrnice především ukládá členským státům povinnost přijmout národní strategii pro bezpečnost sítí a informačních systémů, ustavuje bezpečnostní týmy CSIRT, skupinu pro strategickou spolupráci mezi členskými státy, zavádí bezpečnostní požadavky na hlášení incidentů a přijetí bezpečnostních opatření pro provozovatele základních služeb a poskytovatele digitálních služeb.

Prováděcí nařízení EK č. 2018/151 ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb.

Směrnice NIS2

Směrnice NIS2 je nová směrnice (novelizovaná NIS) EU o bezpečnosti sítí a informací ze dne 27. 12. 2022, účinná od 16. 1. 2023, která ustanovuje změny, jež by měly jednotlivé členské státy aplikovat. V současnosti zatím v ČR směrnice není provedena, avšak v její návaznosti se očekává přijetí novely Zákona o kybernetické bezpečnosti, a to do září nebo října roku 2024 (konkrétně musí vejít v účinnost do 16. 10. 2024).

Významnými změnami dle této směrnice bude rozšíření počtu povinných osob, regulovaných odvětví a služeb (např. digitální služby o službu cloud computingu), změna způsobu identifikace povinných osob, povinné vzdělávání vrcholového vedení organizace a větší odpovědnost managementu za zajišťování kybernetické bezpečnosti, dobrovolné hlášení bezpečnostních incidentů, další požadavky na vedení registru internetových domén nejvyšší úrovně a jejich poskytovatelů, důraz na sdílení informací mezi povinnými organizacemi, spolupráce mezi povinnými organizacemi a regulátorem a vyšší peněžité sankce za nedodržení uložených povinností, které by mohlo přispět ke konceptu odstrašení.

V současné době NÚKIB ve spolupráci se zpravodajskými službami připravuje návrh zákona o snižování rizik spojených s dodavateli informačních a komunikačních technologií, který by měl zvýšit ochranu kritické infrastruktury před kybernetickou špionáží a útoky (zákon o dodavatelských řetězcích).

Národní strategie kybernetické bezpečnosti ČR na období let 2021-2025

Národní strategie kybernetické bezpečnosti na období let 2021-2025 je zásadní rámcový dokument vydaný NÚKIB a schválený vládou ČR. Strategie pokračuje v naplňování vizí předchozích strategií z let 2015-2020, 2012-2015 a přináší vize nové. Jejím záměrem je mj. aby Česká republika v oblasti kybernetické bezpečnosti neustále vylepšovala stávající model identifikace a detekce

kybernetických hrozeb, jejich následné analýzy a reakce, vzdělávala experty v oboru kyberbezpečnosti, navyšovala odolnost proti hrozbám u povinných subjektů, důrazně sledovala a analyzovala zabezpečení ICS a SCADA systémů, zajišťovala nejvyšší stupeň zabezpečení a sebevědomou včasnou reakci na útoky (koncept odstrašení), rozvíjela ve společnosti znalost bezpečného pohybu na internetu (digitální hygiena) atd.

Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021-2025

Akční plán znázorňuje konkrétní úkoly k provedení vizí Národní strategie kybernetické bezpečnosti. Stanovuje jaké úkoly, který orgán a v jakém časovém období má splnit.

Vybrané úkoly:

- v rámci vize společného přístupu ke kyberbezpečnosti např. úkol NÚKIB do posledního čtvrtletí 2021 zpracovat návrh národní politiky koordinovaného zveřejňování zranitelností
- v rámci vize úpravy a aktualizace regulatorního rámce např. úkol NÚKIB do třetího čtvrtletí 2022 vytvořit regulatorní rámec bezpečnosti cloud computingu
- v rámci vize bezpečné infrastruktury např. úkol NÚKIB a Ministerstva zdravotnictví průběžně skrze tvorbu metodických materiálů, realizaci cvičení a dalšími uvedenými způsoby navyšovat kybernetickou bezpečnost zdravotnického sektoru

Zákony a vyhlášky

Zásadními předpisy v oblasti kyberbezpečnosti jsou především:

- Zákon č. 181/2004 Sb., o kybernetické bezpečnosti, včetně pozdějších novel.

- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (prováděcí vyhláška k zákonu č. 181/2004 Sb.).
- Zákon č. 153/1994 Sb., o zpravodajských službách ČR včetně pozdějších novel.
- Zákon č. 154/1994 Sb., o bezpečnostní informační službě včetně pozdějších novel.
- Zákon č. 289/2005 Sb., o vojenském zpravodajství včetně pozdějších novel.
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce včetně pozdějších novel.
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti včetně pozdějších novel.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné zprávy včetně pozdějších novel.
- Zákon č. 127/2005 Sb., o elektronických komunikacích včetně pozdějších novel.
- Zákon č. 121/2000 Sb., autorský zákon, včetně pozdějších novel.
- Zákon č. 40/2009 Sb., trestní zákoník včetně pozdějších novel.
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek včetně pozdějších novel.

Nejdůležitějšími zde jsou z pohledu kyberkriminality a kyberterorismu:

- Zákon o kybernetické bezpečnosti, který upravuje práva a povinnosti osob (zejm. správce a provozovatele systému kritické informační infrastruktury KII nebo významného informačního systému VIS, provozovatele základní služby PZS a poskytovatele digitální služby PDS) a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, zapracovává příslušné

předpisy EU a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Stanovuje i některé druhy přestupků spojenými s povinnostmi osob.

- Trestní zákoník, který stanovuje trestné činy (TČ) a sankce za ně – především: TČ proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství (§ 180 neoprávněné nakládání s osobními údaji, § 182 porušení tajemství dopravovaných zpráv, § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí), TČ proti majetku (zejm. § 230 a 232 neoprávněný přístup k PC systému a nosiči informací a neoprávněný zásah do PC systému nebo nosiče informací, § 231 opatření a přechovávání přístupového zařízení a hesla k PC systému a jiných takových dat), TČ proti průmyslovým právům a proti autorskému právu (§ 268-271: porušení práv k ochranné známce, průmyslových práv, autorského práva nebo padělání a napodobení výtvarného díla), TČ obecně nebezpečné (§ 272 a 273 obecné ohrožení, § 276 a 277 poškození a ohrožení provozu obecně prospěšného zařízení), TČ proti ČR, cizímu státu a mezinárodní organizaci (§ 311 teroristický útok, § 312a účast na teroristické skupině, § 312d financování terorismu, § 312e podpora a propagace terorismu, § 312f vyhrožování teroristickým trestným činem, § 314 sabotáž, § 316 vyzvědačství, § 317 a 318 ohrožení utajované informace).
- Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. 3. 2017, o boji proti terorismu a Směrnice EP a Rady (EU) 2013/40/EU z 12. 8. 2013 o útocích na informační systémy.

Pro využití v oblasti kybernetické bezpečnosti byly také zpracovány metodiky pro efektivní správu informačních systémů (COBIT, ITIL, ISMS), normy a standardy které stanovují základní požadavky na certifikaci, klasifikaci, posuzování apod. informačních systémů – např. norma ISO 27039 nabízející doporučení ohledně

zavedení systémů pro odhalení a prevenci nežádoucích aktivit v počítačových sítích, tzv. systémů IDPS (Intrusion Detection and Prevention System). Běžným standardem v ČR je ISO 27001 (ČSN EN ISO/IEC 27001:2014) a ISO 27002 (ČSN EN ISO/IEC 27002:2014). ISO 27001 koresponduje s prováděcí vyhláškou č. 82/2018 Sb. k zákonu o kybernetické bezpečnosti.

Aktualizované právní předpisy aj. dokumenty, které odpovídají potřebám institucí a jejich stavu bezpečnosti napomáhají vhodnému nastavení informačních systémů jejich provozovateli a včasné reakci na bezpečnostní incidenty, avšak nejsou všespásné. V rámci represe umožňují spravedlivé potrestání pachatelů kyberkriminality.

3.2 Orgány ČR pro zajišťování kyberbezpečnosti

- Vláda ČR – Výbor pro kybernetickou bezpečnost
- Ministerstvo zahraničních věcí – Odbor kybernetické bezpečnosti
- Národní bezpečnostní úřad (NBÚ) – ústřední správní úřad pro ochranu utajovaných informací
- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) – ústřední správní úřad pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany; ředitel úřadu je oprávněn k vyhlášení stavu kybernetického nebezpečí dle § 21 zákona o kybernetické bezpečnosti
- Národní centrum kybernetické bezpečnosti (NCKB) – výkonné oddělení úřadu NÚKIB
- Vládní CERT (GovCERT.cz, součást NCKB) – řeší bezpečnostní incidenty v PC sítích KII, VIS a státní správy
- Národní CERT (CSIRT.cz) – bezpečnostní tým, který má na starost zájmové sdružení právnických osob CZ.NIC, a na základě veřejnoprávní smlouvy

s NÚKIB koordinuje řešení bezpečnostních incidentů v PC sítích po ČR nespadajících do přímé působnosti GovCERT.cz

- BIS – bezpečnostní informační služba
- Ministerstvo vnitra – Policie ČR a Národní centrála proti organizovanému zločinu, Úřad pro zahraniční styky a informace, Odbor centrálních informačních systémů sekce eGovernmentu
- Ministerstvo obrany – Agentura komunikačních a informačních systémů, úřad Velitelství kybernetických sil a informačních operací a Centrum CIRC (Computer Incident Response Capability), Národní centrum kybernetických operací Vojenského zpravodajství
- Ministerstvo průmyslu a obchodu
- Český telekomunikační úřad
- Ministerstvo školství, mládeže a tělovýchovy – vzdělávací funkce
- Povinné osoby a orgány dle ZKB
- Soukromé organizace a jednotlivci, sdružení, bezpečnostní týmy, výrobci programového vybavení atd.

3.3 Organizační opatření

Organizačním opatřením je:

- zavedení Systému řízení informační bezpečnosti ISMS (Information Security Management Systém) nebo jiné metodiky pro řízení bezpečnosti informačního systému v organizaci
- udělování přístupových oprávnění pouze k takovým systémům nebo software, příp. jejich částem, korespondujícím s náplní práce konkrétního zaměstnance

- oddělení útvaru bezpečnosti informačních a komunikačních technologií od útvaru zajišťujícího provoz informačních a komunikačních technologií (tzv. podmínka neslučitelnosti)
- v případě kybernetických útoků je užitečné mít předem připravené krizové a havarijní plány pro jejich zvládání a v rámci jejich zpracování mít odpovědi na tyto otázky:
  1) Kdo bude obranu proti útoku řešit, tzn. jaká jednotka a kdo bude jejím velitelem?
  2) S kým bude spolupracováno a jaké finanční prostředky budou použity na odvracení útoku?
  3) Které systémy se budou primárně udržovat v chodu?
  4) Jsou-li data zálohována, tak na jakém místě?
  5) V jakém pořadí se budou systémy a data obnovovat?
  6) Kdo a jakým způsobem bude komunikovat s veřejností?
  7) Jaká bude primární reakce podniku na útok?[23]

3.4 Technická opatření

Do systému technické ochrany můžeme zařadit preventivní a detekční technická zařízení a zařízení tzv. protišpionážní.

- mechanické zabranné prostředky – zámky, bezpečnostní a protipožární dveře, zabezpečení areálu plotem, uzamykací systémy a bezpečnostní úschovné objekty, trezory, zdi,…
- poplachové a tísňové systémy
- kamerové systémy

[23] https://www.kybez.cz/opomijena-rizika-7-chybejici-krizovy-plan/

- bezpečnostní a nouzová svítidla
- nouzová zvuková zařízení a hlásiče
- systémy kontroly vstupu
- detektory odposlechů a kamer
- rušičky odposlechů
- hardwarový typ firewallu (síťový firewall)

Obrázek 7 - Kamery

3.5 Fyzická opatření

Fyzická opatření zahrnují přímý dohled a kontrolu vstupů a výstupů osob a vjezdů a výjezdů vozidel z areálu strážnými nebo vzdálený dohled prostřednictvím kamerového systému. Z pozice jednotlivce je možné považovat za fyzické opatření chování při pohybu na internetu. Znalost bezpečného chování na internetu, tzv. digitální hygieny, je preventivním opatřením před kybernetickými hrozbami.

3.6 Režimová opatření

- kontrola vstupů a výstupů osob do areálu nebo budovy – zaměstnanců, cizích osob, dodavatelů (např. dle čipu zaměstnance, průkazu totožnosti osoby, kontrola průchodem detekčním rámem, kontrola ručním detektorem, fyzická kontrola)
- kontrola vjezdů a výjezdů motorových vozidel do areálu
- kontrola pohybu osob a vozidel v objektu
- režim obsluhy kamerových systémů a jiných technických zařízení
- způsob nakládání s čipovými kartami aj. identifikačními prvky – např. uzávěra v bezpečnostní schráně
- evidence majetku a kontrola přesunů majetku
- metodiky pro mimořádné situace
- pravidelná školení zaměstnanců a kontrola znalostí získaných školením
- proškolování v práci se softwarem a v případě přecházení na nový software

3.7 Softwarová opatření

Vzhledem k charakteru kybernetických hrozeb je nejdůležitějším prvkem kvalifikovaná práce se softwarovým vybavení.

Řekněme si, co je možné provést v rámci preventivních opatření.

Zabezpečení počítače

Nejlepší obranou informačního systému je dbát na prevenci před kybernetickými hrozbami a nemuset řešit následky po napadení kybernetickým útokem. Operační systém a další programové vybavení zařízení je tedy nutno udržovat aktuální a včasně reagující na změny.

Primárně bychom měli, pokud chceme mít aplikace opravdu bezpečné, zkoumat splnění bezpečnostních požadavků na software. Společnosti OWASP Foundation nebo Microsoft nabízí vývojářské a dokumentační metodiky, které se zabývají tím, jakým způsobem co nejkvalitněji vyvíjet webové aplikace a jiný software a jak tyto aplikace zabezpečit, a to včetně požadavků na bezpečné kódování. OWASP Foundation také každé 3-4 roky zveřejňuje seznam TOP 10 zranitelností webových aplikací, kterých by si měl být každý vývojář aplikací vědom.

Top 10 zranitelností roku 2021:

1) Nedostatečná kontrola přístupu
2) Kryptografická selhání
3) Vsunutí kódu – SQL, XSS apod.
4) Nezabezpečený design
5) Chybná konfigurace
6) Zranitelné a zastaralé komponenty
7) Identifikační a autentizační selhání
8) Selhání software a integrity dat – včetně nezabezpečeného procesu deserializace (převod dat souboru do kódu v průběhu procesu programování aplikace)
9) Selhání bezpečnostního protokolování (tzv. logování) a monitorování
10) Padělání požadavků na straně serveru (tzv. SSRF útoky)

Je-li nalezena zranitelnost v již existující vydané aplikaci, která by mohla být zneužita k útoku, je potřebné na ni reagovat tím, že výrobce vydá pro tuto zranitelnost záplatu, což se bohužel nemusí uskutečnit ani po dlouhém časové období. Stejně tak je potřeba sledovat vstupy do aplikace např. prostřednictvím formulářů a všechny tyto vstupy náležitě zajistit kódem – důležitá aktivita zejména pro prevenci XSS, SQL, ShellCode Injection atd.

Včasná detekce

Pro prevenci a detekci narušení bezpečnosti je dále ve společnostech nebo domácnostech využíváno několik druhů bezpečnostního software nebo systémů umožňujících kontrolu v reálném čase.

Antivirový software je program k identifikaci, přesunutí do karantény či odstranění malware prohlížením souborů na disku a v paměti RAM, shoduje-li se se známým malware v databázi antiviru, nebo odstranění malware při detekci a analýze podezřelého a nebezpečného chování programů v počítači a dalšími metodami. Velmi používaná je ochrana tzv. ***whitelistingem***, kdy správce systému antivirem umožní spouštění pouze programům, které jsou na tzv. white listu (bílém seznamu), ostatní programy jsou preventivně blokovány, dokud je správce na tento seznam v antiviru nepřidá.[24]

Antispywarový software je program, který odstraňuje nebo blokuje detekovaný spyware, škodlivý sledovací software.

Firewallový software je program, který analyzuje, filtruje a zabezpečuje přicházející a odcházející síťový provoz (datové pakety) na základě nadefinovaných pravidel. Firewall odděluje místní síť od sítě širšího internetu, a tím pomáhá zabezpečit domácí zařízení. Při použití samotného software je nutné, aby si byl uživatel dostatečně vědom, které programy a aplikace povolit, které blokovat a které filtrovat. Pro nejlepší ochranu společnosti je z tohoto důvodu vhodné použít firewall hardware pro jednu firemní síť a firewall software na počítač každého zaměstnance.

[24] Antivirový program. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Antivirov%C3%BD_program

Antiadwarový software je programový nástroj, který detekuje a odstraňuje obtěžující reklamní aplikace (vyskakovací okna, banery atd.) nebo zbytečný předinstalovaný software od výrobce.

Mnoho společností kombinuje funkce těchto programů v jednom a poskytuje ochranu proti hrozbám všeho druhu. Antimalwarové společnosti (Norton, ESET, Avast, AVG, Kaspersky, BitDefender apod.) zároveň neustále aktualizují databáze hrozeb k co nejoptimálnější detekci nových hrozeb.

Zabezpečení koncových bodů

Zabezpečení koncových bodů je zabezpečení fyzických zařízení připojených k síti např. mobilního telefonu, zařízení IoT, notebooku, počítače apod. K zabezpečení se využívají tyto nástroje: antimalware, firewall, proxy server, správa aplikací a opravy, řízení přístupu k síti, white listy, black listy, VPN a anonymní procházení sítě, potřeba šifrování dat a emailů atd. Ze známých např. software GFI LAN Guard. Je velmi důležité dbát na zabezpečení těchto bodů, neboť mohou být vstupem do firemní sítě.

Sofistikované systémy včasné detekce

Ve rozsáhlých korporátech se vyjma hardware firewallů a antivirů používají speciální obranné systémy.

Intrusion Detection System, česky systém detekce průniku, je systém prostřednictvím senzoru monitorující síťový provoz a odhalující neobvyklé aktivity, které by mohly narušit bezpečnost systému nebo firemní sítě. Intrusion Detection System je schopný aktivně zasáhnout proti všem podezřelým nálezům, kam spadá příprava na útok např. skenováním portů, snaha o narušení přístupových oprávnění, ale také neoprávněný vstup do databáze, DDoS útoky, malware apod. Intrusion Detection System reaguje na útoky z vnitřní i externí sítě. Po detekci generuje varování, zaznamená o této aktivitě log do systému, upozorní na ni

správce a následně ji zastaví, bude-li možné. [25]Může být dvojího charakteru – buďto se jedná o systém HIDS nebo NIDS. HIDS, Host-Based Intrusion Detection Systém, česky na hostitele orientovaný systém detekce průniku, může být pouze softwarového typu a monitoruje pouze systém počítače, na kterém je nainstalován. NIDS, Network-based Intrusion Detection System, česky na síť orientovaný systém detekce průniku, monitoruje veškerý síťový provoz sdílený několika hostiteli. Pro zajištění nejvyššího stupně ochrany je ideální jejich kombinace.

Intrusion (Detection and) Prevention System, česky systém (detekce a) prevence průniku, vznikl rozšířením systému IDS o monitoring aktivit operačního systému, které by mohly směřovat k narušení bezpečnosti. Ve spolupráci s firewallem filtruje škodlivé pakety, blokuje provoz ze škodlivé IP adresy, vyvolává poplach atd. Druh útoku detekuje buďto na základě vlastní databáze (HIPS), odhalováním anomálií v provozu porovnáváním vzorku běžného provozu a aktuálního provozu (HIPS, NBA) nebo odhalováním anomálií v lozích porovnáváním záznamů logů z běžného provozu a z aktuálního provozu (HIPS, NIPS, WIPS). Aktuálně existují 4 druhy: na hostitele orientovaný HIPS (Host-based IPS), na síť orientovaný NIPS (Network-based IPS), bezdrátový WIPS (Wireless IPS) a NBA (pro analýzu síťových aktivit).

V průmyslových a řídicích systémech ICS a systémech pro dohledové řízení a sběr dat tzv. SCADA se výše uvedené systémy hojně využívají, ku příkladu pokročilý systém GreyCortex Mendel, který je využíván také v neprůmyslových institucích (Ministerstvo zahraničních věcí) pro monitoring vlastní sítě.

[25] Intrusion Detection System. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2021-5-18]. Dostupné z: https://cs.wikipedia.org/wiki/Intrusion_Detection_System

Síťový monitoring a analýza sítě

Síťový monitoring a analýzu své sítě je oprávněn provozovat poskytovatel síťového připojení, telefonní operátor nebo správce sítě (zaměstnavatel) v podniku k ochraně zájmů podniku. Dále Bezpečnostní informační služba nebo Vojenské zpravodajství mohou monitorovat telekomunikační, radiokomunikační nebo jiný obdobný provoz bez odposlechu jeho obsahu, popřípadě zjišťování údajů o tomto provozu.

Monitoring a analýza sítě jsou prováděny pomocí softwarových a hardwarových nástrojů – programy např. NetFlow, Nessus, Kismet, NetStumbler, Traceroute NG, Network Scanner, LAN Scan, Retina; sondy, síťové odposlechy TAPy, SPAN analyzátory, síťové odbočovače aj.

Data Loss/Leak Prevention (DLS) System, česky systém pro prevenci ztráty/úniku dat, je speciálně sestavený systém nástrojů a procesů, který kombinuje standardní řešení (softwarové nástroje ochrany koncových bodů, monitoring, hardware firewall apod.) a pokročilá řešení typu umělá inteligence, strojové učení a automatizace. Cílem je odhalovat anomální činnost a zabránit ztrátě nebo úniku dat.

Deep Packet Inspection (DPI) Software, česky hloubková kontrola paketů, je pokročilá metoda zkoumání a řízení síťového provozu prostřednictvím filtrování paketů, která lokalizuje, identifikuje, klasifikuje, přesměrovává nebo blokuje pakety se specifickými datovými a kódovými příznaky, jež běžná kontrola paketů není schopná detekovat. Program, který tuto metodu v rámci monitoringu využívá je např. český software GreyCortex. Hloubkovou kontrolu paketů využívají také proxy servery. Proxy server je softwarový (např. program Fiddler) nebo

hardwarový komunikační prostředník mezi uživatelem a serverem a bývá za účelem zvýšení zabezpečení používán pro oddělení provozu lokální sítě internetu (domácí LAN nebo intranet firmy) od širší sítě internetu.

Skenovací nástroje na odhalení chyb v systému nebo síti

Softwarové skenovací nástroje na odhalení chyb v systému nebo síti, nebo také skenery zranitelností, se využívají pro identifikaci slabých míst v PC systému nebo síti. Obvykle zkoumají otevřené porty, analyzují služby, které na nich běží nebo automaticky vyhledávají potenciální zranitelnosti v aplikacích.

Kontrola logů

Aktivity kyberútočníků většinou zanechávají v systému záznamy, tzv. logy, které mohou na škodlivou aktivitu upozornit. Manuální kontrola je příliš náročná na čas, kontrola logů se proto provádí automaticky pomocí IDS, IPS nebo software na kontrolu logů, které logy shromažďují do centrální databáze a následně analyzují. Příkladem software pro podnikové sítě je LOGmanager společnosti Sirwisa.a.s.

Ochrana dat zálohováním a archivací dat

Zálohování je aplikováno na data, systémy nebo celé servery, přičemž umožňuje rychlé obnovení dat. Archivace se provádí u dat, u kterých není potřeba jejich případná okamžitá dostupnost. Zálohování dat nebo archivace probíhá na paměťová média (magnetická páska, pevný disk, Network Attached Storage – úložiště disku/disků připojené k síti, optické disky, USB flash disk atd.) nebo vzdálená cloudová úložiště (např. společnosti Azure, Google Cloud, OneDrive,

BaaS, Oracle,). Prevencí před zničením serverů a datových úložišť povodní nebo požárem může být také umístění serverů a úložišť dat do jiné vzdálené budovy mimo pracoviště. Způsob zálohy je ideální uzpůsobit dle potřeby využívání dat. Typy záloh: nestrukturovaná, úplná a inkrementální, úplná a rozdílová, zrcadlová a reverzně přírůstková, průběžná, úplná.

Využívání systémů RAID

Možnost selhání pevného disku lze pokrýt metodou RAID (Redundant Array of Independent Disks), kdy se data rozloženě ukládají na několik nezávislých disků.

Kryptografie

Pro zajištění bezpečnosti jsou využívány asymetrické šifrovací mechanismy založené na matematickofyzikálních algoritmech a jsou prozatím považovány za dostačující, přesto útoky Man in The Middle, ARP poisoning a podsunutí vlastního certifikátu útočníka jsou velkou hrozbou. Jinou hrozbou je možný blížící se nástup kvantových počítačů, které využívají jiný druh šifrovacího algoritmu. Čím dál častěji se také vstupuje do sítě vzdáleně z domova, což přináší další ohrožení. Pro vzdálený přístup je vhodné používání ***VPN***, která vytvoří chráněný tunel mezi domácím počítačem a sítí společnosti, neboť šifruje data a maskuje IP adresu, ze které je přistupováno.

Ochrana hesel v databázích

Pro efektivnější hašování se využívají další způsoby ochrany hesel v databázi. Ideální je ukládat heslo do databáze v podobě hashe. Při přihlášení pouze stačí,

když dojde ověření shody hashe zadaného hesla a hashe v databázi. Útočníci jsou v současné době schopni prostřednictvím výše uvedených metod (např. Rainbow Tables) odhalit hesla z hašů ukradených dat z databáze. Aby se útoku na odcizená data zamezilo, správci systémů hašují hesla dohromady s tajnými přísadami, tzv. kryptografickou solí nebo pepřem (tajnou solí). Kryptografická sůl je několik náhodných bitů přidaných před nebo za heslo, se kterým se zahašuje. V databázi je sůl v podobě čistého textu uložena vedle zahašovaného hesla a je pro každého uživatele jedinečná. Jestliže je tedy kompromitováno jedno z hesel, nemusí zákonitě dojít ke kompromitaci jiného hesla. K heslu a soli může být pro zvýšení zabezpečení před celým hašováním použit také kryptografický pepř (kryptografická tajná sůl), který je na rozdíl od soli pro každého uživatele nebo skupinu uživatelů stejný a není uložen v databázi, ale v oddělené a dobře zabezpečené části webu (např. pevně zakódován ve zdrojovém kódu webové aplikace). Účinné může být též pomalé hašování s pomocí algoritmů Bcrypt nebo PBKDF2, neboť by mohlo být schopno částečně zbrzdit útočníka v případě, že by prováděl prolomení zahašovaného hesla, event. opakované zahašování hesla.

3.8 Expertní a vzdělávací opatření

Penetrační testování

Penetrační testování je metoda hodnocení aktuálního zabezpečení počítačových zařízení, systémů nebo aplikací v kontrolovaných podmínkách. Je prováděno zkušenými hackery testováním a simulací potenciálních útoků z interního nebo externího prostředí na systém nebo aplikaci.

K penetračnímu testování se využívají software: Metasploit, Burp Suite, Nexpose, Kali Linux…

Honeypots nástrahy

Honey pot, česky hrnec medu, je software nebo systém vytvořený a včleněný do sítě úmyslně jako návnada pro útočníky s cílem analýzy jejich chování.

Cvičení kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti (NCKB) pořádá nebo se účastní za účelem zdokonalování prevence a obrany proti kybernetickým útokům technických, table-top, procesních, komunikačních a hybridních cvičení.[26]

V rámci technických cvičení (např. Cyber Czech, Crossed Swords) je simulován kybernetický útok, na který reagují techničtí experti. Table-top cvičení (např. Electro Czech 2019) jsou netechnického typu a jsou konstruována pro vzdělávání veřejných zaměstnanců a osvětu odborné veřejnosti prostřednictvím diskuzí nad krizovými scénáři. Procesní cvičení (např. Cyber Coalition) jsou zaměřena na reakce organizací a jejich interní postupy během možného kybernetického útoku. Komunikační cvičení (např. Comm Czech) ověřují efektivnost a rychlost komunikace pro případ krize. Hybridní cvičení (např. Locked Shields) spojuje všechny tyto typy do jednoho a simulují tím reálný útok.

Znalostní základna technik, metod a taktik

[26] Typy cvičení. *NÚKIB* [online]. [cit. 2023-03-12]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/cviceni/typy-cviceni/

Americká nezisková organizace The MITRE Corporation spravuje webové stránky https://attack.mitre.org/, se seznamy mnohých technik a metod. Považuji za důležité pokusit se vytvořit podobnou znalostní základnu i v ČR.

Firemní úprava

Samozřejmostí je dodržování firemních pokynů zaměstnanci, neboť někdy nepřítel nemusí stát za dveřmi, ale přímo uvnitř. Toto platí o zaměstnancích, kteří surfují na nezabezpečených stránkách nebo strčí nakažený flash USB disk do firemního počítače.

Závěr

Shrnula bych nejpodstatnější kroky, které by dle mého názoru měla organizace zajišťovat. Nejdůležitější částí je vzdělávání zaměstnanců, neboť společnost je teoreticky tak slabá jako její nejslabší článek a nelze podceňovat možný útok zevnitř organizace. Podnik může zabránit zaměstnancům v rizikovém chování řádným proškolováním o obecné a kybernetické bezpečnosti a jejich následnou kontrolou otestováním nebo prováděním bezpečnostních cvičení. A dále omezením přístupu k internetu z firemní sítě např. Proxy Firewallem a v případě navštívení podezřelé stránky ukončením síťového spojení. Dalším zásadním krokem je zavést IDS nebo IPS systémy, pokud je firma nepoužívá, a také zálohování některých dat na místech mimo pracoviště. Možností sledování a útoků na internetu s digitální dobou stále přibývá, hackeři dále vymýšlí, jak by mohli narušit uživatelské sítě a ukrást data, velké společnosti zkoumají, jakým způsobem co nejlépe cílit reklamu a ovládnout myšlení populace. Nejlepší způsob, jak bychom mohli zabránit zneužívání sledování a narušování soukromí ve velkém, je zvyšovat si neustále gramotnost na poli internetové bezpečnosti (tzv. znalost digitální hygieny) a být obezřetní vůči novým bezpečnostním hrozbám.

Seznam obrázků a tabulek

Obrázky a tabulky

Seznam použitých zdrojů

ALEXANDER, Philip. *Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers. USA, Praeger Security International*: 2008. ISBN 978-0-313-34558-6.

BRZYBOHATÝ, M. Současný terorismus. In: FOLTIN, Pavel a David Řehák. Důvody realizace a formy terorismu [online]. MOČR 2005 [cit. 12.03.2023]. Dostupné Vojenské rozhledy: http://www.mocr.army.cz/mo/obrana_a_strategie/1-2005cz/foltin.PDF

FOLTIN, Pavel a David Řehák. Důvody realizace a formy terorismu [online]. MOČR 2005 [cit. 12.03.2023]. Dostupné Vojenské rozhledy: http://www.mocr.army.cz/mo/obrana_a_strategie/1-2005cz/foltin.PDF

FRYČ, Bc. Martin. *Audit informační bezpečnosti: Význam auditu informační bezpečnosti v procesu zavádění bezpečnostního standardu PCI v organizaci* [online]. Praha, 2009 [cit. 2023-03-12]. Dostupné z: is.ambis.cz. Diplomová práce. Bankovní institut vysoká škola Praha - informační technologie a management.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Česká pobočka AFCEA, 2013, s. 57. ISBN 9788072513970

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

KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS: kompletní průvodce analýzou a diagnostikou sítí*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

KREMLING, Janine a Amanda M. Sharp PARKER. *Cyberspace, cybersecurity, and cybercrime: kompletní průvodce analýzou a diagnostikou sítí*. Los Angeles: London, [2018]. ISBN 978-1-5063-4725-7.

MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu*. Praha: Linde, 2006. ISBN 80-7201-614-8.

OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí*. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. Epravo [online]. EPRAVO.cz, c1999-2021, 16. 10. 2019 [cit. 2023-03-12]. ISSN 1213-189X. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

SINGER, P.W., EMERSON T. Brooking. LikeWar: The Weaponization of Social Media. Boston, NY: 2018. ISBN 978-1-328-69574-1.

SINGER, P.W., FRIEDMAN Allan. Cybersecurity and Cyberwar: what everyone needs to know. USA: 2014. ISBN 978-0-19-991809-6.

VALERIANO, Brandon, MANES, Ryan C. Cyber War versus Cyber Realities. *Oxford*: 2015. ISBN 978-0-19-020479-2.

Bezpečnostní strategie ČR 2003

Ministerstvo vnitra Odbor bezpečnostní politiky [online]. In: Vnitřní bezpečnost a veřejný pořádek. Krizové řízení. Praha 2005. [cit. 2023-03-12]. Dostupné z: https://docplayer.cz/20919444-Ministerstvo-vnitra-odbor-bezpecnostni-politiky.html

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

1.3 Models of Security – CIA Parkerian Hexad. *ENG LIBRE TEXTS*[online]. [cit. 2023-03-12]. Dostupné z: https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.3_Models_of_Security_-_CIA___Parkerian_Hexad

Analýza rizik. *ACRESIA* [online]. [cit. 2023-03-12]. Dostupné z: https://acresia.com/index.php/sluzby/69-analyza-rizik

Antivirový program. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Antivirov%C3%BD_program

ARP Poisoning. *VARONIS* [online]. [cit. 2023-03-12]. Dostupné z: https://www.varonis.com/blog/arp-poisoning

ARP Spoofing. *VERACODE* [online]. [cit. 2023-03-12]. Dostupné z: https://www.veracode.com/security/arp-spoofing

Intrusion Detection System. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2021-5-18]. Dostupné z: https://cs.wikipedia.org/wiki/Intrusion_Detection_System

Denial of service. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: Denial of service – Wikipedie (wikipedia.org)

DNS Cache Poisoning. *CLOUDFLARE* [online]. [cit. 2023-03-12]. Dostupné z: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Email Hijacking. *DOUBLE OCTOPUS* [online]. [cit. 2023-03-12]. Dostupné z: https://doubleoctopus.com/security-wiki/threats-and-tools/email-hijacking/

DNS Hijack. *IPSHU* [online]. [cit. 2023-03-12]. Dostupné z: https://cs.ipshu.com/dns_hijack

DNS Hijack. *IPSHU* [online]. [cit. 2023-03-12]. Dostupné z: https://www.veracode.com/security/arp-spoofing

IDS vs IPS. *SPICEWORKS* [online]. [cit. 2023-03-12]. Dostupné z: https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/

Internet věcí – Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_v%C4%9Bc%C3%AD

Learning. *CLOUDFLARE* [online]. [cit. 2023-03-12]. Dostupné z: https://www.cloudflare.com/learning/

Man in the Middle Attack MitM. *TECHTARGET* [online]. [cit. 2023-03-12]. Dostupné z: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

MITRE ATT&CK. *MITRE* [online]. US: The Mitre Corporation, c2015-2022 [cit. 2023-03-12]. Dostupné z: https://attack.mitre.org/
Zkopírovat citaci

OWASP. *OWASP* [online]. US: The OWASP Foundation, c2023 [cit. 2023-03-12]. Dostupné z: https://owasp.org/

Password Cracking Techniques. *DIGITALPRIVATEVAULT* [online]. [cit. 2023-03-12]. Dostupné z: https://www.digitalprivatevault.com/blogs/password-cracking-techniques

Password Security Hashing Salting Peppering. *GEARBRAIN* [online]. [cit. 2023-03-12]. Dostupné z: https://www.gearbrain.com/password-security-hashing-salting-peppering-2647766220.html

Phreaking. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Phreaking

Sociální inženýrství (bezpečnost). Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_in%C5%BEen%C3%BDrstv%C3%AD_(bezpe%C4%8Dnost)

Špionáž. *Global Politics: Internet Archive* [online]. [cit. 2023-03-12]. Dostupné z: https://web.archive.org/web/20080203202457/http://www.globalpolitics.cz/clanek/spionaz.html

Terminologický slovník - krizové řízení a plánování obrany státu. In: *MV ČR* [online]. Praha: MV ČR, 2016 [cit. 2023-03-12]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

Types of Computer Malware. *TITANFILE* [online]. [cit. 2023-03-12]. Dostupné z: https://www.titanfile.com/blog/types-of-computer-malware/

Typy cvičení. *NÚKIB* [online]. [cit. 2023-03-12]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/cviceni/typy-cviceni/

Understanding and Stopping MultiVector DDoS Attacks. *CORERO* [online]. [cit. 2023-03-12]. Dostupné z: https://www.corero.com/understanding-and-stopping-multi-vector-ddos-attacks/

What are SSL Stripping Attacks. *KEYFACTOR* [online]. [cit. 2023-03-12]. Dostupné z: https://www.keyfactor.com/blog/what-are-ssl-stripping-attacks/

Válka. In: *MV ČR* [online]. Praha: MV ČR, 2016 [cit. 2023-03-12]. Dostupné z: https://www.mvcr.cz/mvcren/docDetail.aspx?docid=21281162&docType=ART

What are the different types of Malware? COMTACT [online]. London: Comtact, 2021, 14.3.2019 [cit. 2023-03-12]. ENG. Dostupné z: https://comtact.co.uk/blog/what-are-the-different-types-of-malware

What is cookie hijacking. *GEEKS FOR GEEKS* [online]. [cit. 2023-03-12].

Dostupné z: https://www.geeksforgeeks.org/what-is-cookie-hijacking/

Wikimedia Foundation, 2001-, 16. 2. 2021 [cit. 2023-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Denial_of_service

Zdroje obrázků

Obrázek 1: https://www.usnews.com/object/image/0000017e-8d03-de57-a57e-bdb7a7310000/istock-1127637966.jpg?update-time=1643043407037&size=responsive970

Obrázek 2: https://www.internetembezpecne.cz/wp-content/uploads/2017/07/phishing-mail.png

Obrázek 3: https://upload.wikimedia.org/wikipedia/commons/0/03/Wireshark_screenshot.png

Obrázek 4: https://www.akamai.com/site/en/images/callout/2022/what-is-ddos-protocol.png

Obrázek 5: https://documents.trendmicro.com/images/tex/articles/defacement-03.png

Obrázek 6: https://www.researchgate.net/publication/349633101/figure/fig8/AS:1007310012960771@1617172830307/Stuxnet-computer-virus-attack.png

Obrázek 7: https://www.mall.cz/i/44194698/1000/1000

Příloha č. 1

Dynamická IP adresa je adresa, která se může změnit s každým přístupem na internet. Je zapůjčována pomocí protokolu a serveru DHCP. Většina zařízení s dynamickou adresou však upřednostňuje opětovné zapůjčování stejné adresy. Pokud je stále možné ji přidělit, DHCP přidělí tuto adresu, tzv. klientem preferovanou IP adresu. Nelze-li ji zapůjčit, přidělí se na základě požadavku na DHCP jiná adresa.

Statická IP adresa je adresa zařízení, která se v čase nemění. Běžně ji využívají tiskárny, směrovače, servery DHCP a FTP. Výhodná je pro možnost vzdáleného přístupu k zařízení, nevýhodná z hlediska možné zranitelnosti vůči útokům.

Veřejná IP adresa je adresa viditelná na síti. Každá z adres musí být unikátní a neshoduje se s žádnou další.

Privátní (neveřejná) IP adresa je adresa na síti neviditelná, určená pro jednotlivá zařízení v místní síti, která jsou skrytá za veřejnou adresou – např. adresou směrovače. Stejnou privátní IP adresu může mít mnoho zařízení po celém internetu, musí být jedinečná pouze v rámci lokální sítě.

MAC (z angl. Media Access Control) adresa je unikátní identifikační adresa přidělovaná každému síťovému hardware výrobcem.

Maska sítě se podobá IP adrese verze 4 a je přidělována protokolem DHCP. Slouží k rozdělení sítě do podsítí a zvyšuje efektivitu směřování provozu, konkrétně zajišťuje, že hostitelé ve stejné fyzické síti spolu můžou komunikovat bez routeru.

DNS, tzv. Domain Name System, česky systém doménových jmen, překládá pomocí protokolu DNS a DNS serveru doménová jména na IP adresy a obráceně. Teprve jakmile počítač uživatele obdrží od DNS serveru informaci překlad webové URL adresy (doménového jména) na IP adresu, může být navázáno spojení.

IP verze 4 je původní komunikační protokol, který nabízí 32 bitové adresy. Vzhledem k tomu, že již od roku 2011 dochází k jejich vyčerpání, vznikl **IP verze 6**, který umožňuje připojit o mnoho větší počet zařízení, k čemuž využívá 128 bitové adresy.

NTP (Network Time Protocol) je protokol určený k synchronizaci nastavení času všech počítačů v síti. Čas jednotlivé počítače nastavují pomocí dotazů směřovaných na tzv. NTP servery pracující s tímto protokolem.

ICMP (Internet Control Message Protocol) je protokol určený k odesílání chybových hlášení. Bývá zneužit zejména pro DoS útoky nebo odposlech komunikace.

SMTP (Simple Mail Transfer Protocol) je protokol používaný pro přenos zpráv e-mailů (elektronické pošty) včetně jejich příloh mezi odesílatelem a příjemcem.

FTP (File Transfer Protocol) je protokol sloužící k přenosu souborů mezi počítači prostřednictvím sítě. Protokol FTP se zabezpečením pomocí SSL/TLS se nazývá FTPS.

SFTP (SSH File Transfer Protocol) je protokol pro přenos souborů po síti, avšak se zabezpečením protokolem SSH (Secure Shell).

POP3 (Post Office Protocol 3) je protokol pro stahování e-mailové pošty ze vzdáleného serveru do e-mailového klienta (Outlook apod.), přičemž po stažení dat ze serveru na lokální počítač data ze serveru zmizí.

IMAP (Internet Message Access Protocol) je protokol, díky kterému lze k e-mailové schránce vzdáleně přistupovat pomocí e-mailového klienta (Outlook apod.). Na rozdíl od POP3 při stažení emailu nedochází k jeho smazání ze serveru.

HTTP (Hypertext Transfer Protocol) je protokol umožňující zobrazení webové stránky načtené z webového serveru v prohlížeči uživatele.

HTTPS (Hypertext Transfer Protocol Secure) je protokol se zabezpečením SSL/TLS, který zajišťuje autentizaci, dostupnost a integritu přenášených dat webových stránek.

SPDY (SPeeDY) a QUIC (Quick UDP Internet Connections) jsou experimentální přenosové síťové protokoly, které by měly zajistit rychlejší přenos. Na základě těchto protokolů byly vyvinuty protokoly pro komunikaci s webovými stránkami HTTP/2 a HTTP3.

Síťové modely slouží pro znázornění síťové architektury a existují dva – TCP/IP a ISO/OSI referenční model.

Model TCP/IP obsahuje 4 vrstvy – 1. vrstvu síťového rozhraní, 2. síťovou (IP) vrstvu, 3. transportní (TCP/UDP) vrstvu a 4. aplikační vrstvu.

Model ISO/OSI je rozvrstvenější než model TCP/IP a obsahuje na rozdíl od něj 7 vrstev – 1. fyzickou, 2. linkovou, 3. síťovou, 4. transportní, 5. relační, 6. prezentační a 7. aplikační. Fyzická a linková vrstva spadá do vrstvy síťového rozhraní, relační, prezentační a aplikační do aplikační vrstvy, jinak se shoduje s modelem TCP/IP. Fyzická vrstva znázorňuje médium, signál a binární přenos. Na linkové vrstvě probíhá fyzické adresování ve fyzické paměti zařízení. Síťová vrstva je určena pro nastavení směru a logického adresování požadavku v síti. Transportní vrstva slouží ke spolehlivému přenosu dat z jednoho konce sítě na druhý. Smyslem relační vrstvy je organizace a synchronizace výměny dat s relační vrstvou jiného systému v síti. Prezentační vrstva provádí dešifrování (příp. šifrování) a úpravu dat tak, aby byla čitelná pro aplikační vrstvu. Aplikační vrstva poskytuje aplikacím v počítači přístup ke komunikačnímu systému.

Server je výkonně konstruované hardwarové zařízení připojené k internetové síti, které běží nepřetržitě a pomocí vlastního server software zpracovává požadavky klienta vysílajícího požadavky na server, tj. aplikaci, kterou ovládá uživatel. Serverem může být teoreticky klasický počítač, avšak hardware takového počítače není určen na výkonnostní zátěž, kterou běžně zvládají servery.

Klient-server síťová architektura je typ počítačové sítě, kde probíhá komunikace mezi aplikací a serverem. S ostatními uživateli klient komunikuje též prostřednictvím serveru.

Klient-klient síťová architektura nebo též Peer-to-Peer architektura je komunikace mezi dvěma uživateli, kteří spolu komunikují a vyměňují si data. Klient

současně vystupuje v pozici klienta i serveru pro jiné klienty. Tato struktura sítě je využívána zejména pro distribuci torrent souborů.

Síťový uzel je zařízení v počítačových sítích, které je určeno k jejich propojení (přepínače – tzv. switche, směrovače – tzv. routery, ethernetové rozbočovače – tzv. huby, opakovače – tzv. repeatery, mosty – tzv. bridge atd.) nebo vystupuje jako koncový bod (počítač, mobilní telefon, kapesní počítač atd.).

Kryptografie, česky šifrování, je v informatice proces utajování dat jejich převedením pomocí speciálního algoritmu do podoby čitelné pouze se znalostí specifického klíče. Opačný proces, kdy dochází k opětovnému přečtení utajených dat, se nazývá dešifrování. Při **symetrickém šifrování** je pro zašifrování i dešifrování použit stejný klíč, základem **asymetrického šifrování** je veřejný klíč pro šifrování a privátní klíč pro dešifrování. Původ veřejného klíče bývá zpravidla ověřen certifikátem, který vydává certifikační autorita.

Kryptoměna je druh digitálních (elektronických) peněz, využívající asymetrické šifrování, která je vyráběna těžením pomocí energie z výpočetního výkonu.

Hash je unikátní řetězec znaků, který byl vytvořen procesem kryptografického hašování hesla (viz níže Kryptografické hašování).

Strojový kód je řada strojových instrukcí, které provádí procesor počítače. Strojový kód je v počítačové paměti uložen jako posloupnost bitů, jež jsou na nejnižší grafické úrovni v aplikaci znázorněny binárními čísly 0 a 1.

Assembler je software, který překládá kód programu napsaný v jazyce symbolických adres, tzv. assembly kódu, do strojového kódu podporovaného procesorem.

Disassembler je opakem assembleru – strojový kód převádí do kódu symbolických adres.

Bug je výraz označující programátorskou chybu v aplikaci.

Debugger, česky ladič, je softwarový nástroj, který se používá k vyhledávání chyb v software ve fázi ladění zdrojového kódu programu. Může být zneužit hackery k hledání zranitelností programů.

Kompilátor, též překladač, je software pro překlad kódu napsaného v jednom programovacím jazyce do jiného programovacího jazyka. Úžeji je definován jako software pro převod programovacího jazyka vyšší úrovně do jazyka nízkoúrovňového – tj. assembly kódu, strojového nebo objektového kódu. Dekompilátor se naopak pokouší o překlad kódu z nízkoúrovňového programovacího jazyka do vyššího programovacího jazyka.