UNIVERZITA KARLOVA

Právnická fakulta

Lukáš Přívozník

Trestněprávní a kriminologické aspekty kyberkriminality se zaměřením na útoky typu odepření služby

Diplomová práce

Vedoucí diplomové práce: JUDr. Jiří Krupička, Ph.D.

Katedra: Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 15. května 2019

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 138 806 znaků včetně mezer.

V Praze dne 15. května 2019

Lukáš Přívozník

Obsah

Úvod

Rozvoj moderních technologií přinesl celou řadu nových nástrojů, postupů a zařízení, které nám usnadňují každodenní život, práci a poskytují i zábavu. Spolu s těmito benefity pro náš život rozvoj moderních technologií přinesl i celou řadu úskalí a nových, do té doby neznámých negativních jevů. Mezi ty můžeme řadit i veškeré elektronické útoky, které mohou být vedeny proti informačním a komunikačním systémům i technologiím. Ne všechny útoky jsou však vedeny formou průniku do cílového systému spolu se získáním neoprávněného přístupu. Existuje určitá skupina útoků, které jsou páchány odlišnou formou. Patří k nim útok typu odepření služby, označovaný zkratkou z anglického jazyka DoS, jehož cílem je narušit fungování služby nebo systému, proti kterému je útok veden, a tím službu nebo systém znepřístupnit legitimním uživatelům. K tomu dochází bez potřeby průniku do systému.

Na základě těchto charakteristických vlastností můžeme pojmenovat druh elektronických útoků, kterým je věnována tato práce. Cílem této diplomové práce je provést rozbor trestněprávního posouzení kybernetických útoků typu odepření služby a souvisejících kriminologických aspektů. K tomu, aby bylo možné tyto aspekty podrobněji rozebrat, je potřeba se nejprve zaměřit na technickou charakteristiku těchto útoků, a to proto, že účel, za kterým je útok veden, se odráží v jeho technickém provedení. Toto technické provedení se pak odráží nejen v trestněprávním posouzení páchaného jednání, ale i v souvisejících kriminologických ohledech.

Téma práce bylo autorem zvoleno s ohledem na fakt, že útoky typu odepření služby jsou v dnešním světě závislém na technologiích a dostupnosti informačních systémů stále více aktuální a dále především z důvodu, že trestněprávní posouzení útoku tohoto typu není zcela jednoznačné, a i v rámci odborné veřejnosti nepanuje shoda na tom, zda jsou tyto útoky podle českých trestněprávních norem postižitelné. Jádrem práce je proto právě část věnovaná trestněprávnímu posouzení útoků typu odepření služby.

Při zpracování této práce je k popsání současného stavu využita metoda deskriptivní a metoda výkladová. K rozboru vybraných oblastí a pro formulaci vlastních názorů je pak využita metoda analytická.

Práce je členěna do tří hlavních částí. První část práce je technická, je v ní popsána charakteristika útoku typu odepření služby. Dále je zde popsána také významná vlna útoků tohoto typu, která v roce 2013 citelně zasáhla český kybernetický prostor a způsobila to, že kybernetická bezpečnost začala být v České republice brána vážněji. V této části jsou také popsány jednotlivé typy a související techniky DoS útoku.

Druhá část práce je věnována kriminologickým aspektům kybernetické kriminality se zaměřením zejména na útok typu odepření služby. Některé jevy jsou však rozebrány obecně ve vztahu ke kybernetické kriminalitě. V této části je v obecnější rovině rozebrán rozmach počítačové kriminality a její latence. Další kapitoly této části jsou věnovány pachatelům a obětem DoS útoků, modu operandi a prevenci před těmito útoky.

Ve třetí části práce je věnován prostor definici kybernetické kriminality a historickému vývoji relevantní části trestního práva. Podstatný díl této části je tvořen podrobným rozborem jednotlivých skutkových podstat trojice počítačových trestných činů. Nejdůležitější je pak kapitola věnovaná trestněprávní kvalifikaci DoS útoku, zhodnocení právní úpravy a návrhům de lege ferenda. Jedná se o hlavní část práce, a proto je jí věnován největší rozsah.

1 Technická část

Elektronické útoky mohou být vedeny jak proti informačním a komunikačním systémům, tak i proti technologiím, na jejich základě jsou tyto systémy postaveny. Při těchto útocích typicky dochází k průniku do daného systému, a tedy získání nelegitimního přístupu. Typů elektronických útoků je celá řada. Můžeme je rozdělit na cílené, které jsou vedeny vůči konkrétnímu vytipovanému cíli, a necílené, které jsou vedeny vůči předem neurčenému a neuzavřenému okruhu systémů nebo jejich uživatelů. Útoky mohou být vedeny jak v technické rovině, např. pomocí různých metod hackingu,[1] tak i v netechnické rovině, např. pomocí metod sociálního inženýrství.[2] Jedním z typů technických útoků je útok Denial of Service (DoS), jehož cílem je cílovou službu učinit nefunkční nebo ji znepřístupnit legitimním uživatelům a při jehož realizaci nedochází k průniku do cílového systému. Specifickou vlastností DoS útoku je fakt, že při jeho prosté realizaci nedochází k překonání překážek a získání neoprávněného přístupu k počítačovému systému. Útok ve své podstatě generuje velké množství (jinak legitimních) požadavků, které vedou k vyčerpání systémových zdrojů a následné nedostupnosti systému.

1.1 Charakteristika útoku typu odepření služby

Útok Denial of Service je typem elektronického útok, jehož cílem je cílovou službu učinit nefunkční nebo ji znepřístupnit legitimním uživatelům. Typicky k tomu dochází v prostředí internetu. Útok bývá proveden zahlcením cílového systému požadavky, které cílový systém přetíží a ten je pak nedokáže spolu s legitimními požadavky ostatních uživatelů obsloužit. Útok může být veden např. na webový server tak, že je tento server požadavky útočníka zahlcen a nedokáže pak poskytnout obsah webových stránek ostatním (skutečným) uživatelům.

K zahlcení může dojít na několika úrovních. Může dojít k zahlcení síťových prvků, vyčerpání šířky pásma internetového připojení, k zahlcení serverové aplikace nebo vyčerpání výkonu serveru. Útok se na napadeném systému projevuje neobvyklým zpomalením poskytované

[1] Hacking je činnost spočívající v hledání a využívání zranitelností v počítačových systémech.
[2] Sociální inženýrství je způsob manipulace lidí za účelem realizace určité aktivity nebo získání určité informace. Nejrozšířenější technikou sociálního inženýrství je phishing, tedy podvodný e-mail, který se pomocí manipulace (tváří se, jako by byl odeslán někým jiným) snaží uživatele přimět k provedení určité akce (např. stažení a spuštění škodlivého kódu) nebo sdělení určité informace (např. zadání čísla platební karty).

služby, jejím dočasným nebo déletrvajícím výpadkem a tedy nedostupností (např. se dlouho načítají webové stránky, nebo se nenačtou vůbec).

Protože útok v naprosté většině probíhá prostřednictvím počítačové sítě, můžeme jej blíže rozebrat s využitím ISO OSI modelu.[3] Tento model rozvrstvuje datovou komunikaci na 7 vrstev, od fyzické vrstvy, která představuje fyzické propojení systémů, přes vrstvy linkovou, síťovou (na té se komunikuje pomocí IP paketů), transportní (na té se komunikuje pomocí TCP a UDP paketů), relační, prezentační, až po vrstvu aplikační.[4] Využití OSI modelu je vhodné, neboť k zahlcení může dojít na několika jeho vrstvách. Prakticky v rámci každé vrstvy modelu je možné určitým způsobem službu vyřadit z provozu. Příklady technik vedení útoků na jednotlivé vrstvy a možné způsoby jejich mitigace (zmírnění) jsou uvedeny v tabulce č. 1. Zabezpečení jedné vrstvy však většinou nezabrání útoku na vrstvy ostatní. Z těchto důvodů je nezbytné věnovat pozornost každé vrstvě zvlášť.[5]

Vrstva OSI	**Využívaný protokol a služby**	**Příklad techniky útoku**	**Mitigace uvedeného příkladu**
Aplikační vrstva	FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP	HTTP get/post – přihlašování do aplikace, upload videa, zasílání komentářů	Monitorování aplikace, CAPTCHA. Vzhledem k tomu, že na této vrstvě útoky napodobují lidské konání, obrana je náročnější.
Prezentační vrstva	komprimace, šifrování, konvertování	útok pomocí upravených SSL dotazů	přesměrování SSL dotazů z původní infrastruktury přes nějaký jiný zdroj

[3] Model publikován mezinárodní organizací pro standardy International Organization for Standardization jako Open Systems Interconnection model – norma ISO/IEC 7498-1.
[4] MEZINÁRODNÍ ORGANIZACE PRO NORMALIZACI. *Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. Standards Catalogue* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.iso.org/standard/20269.html.
[5] CZ.NIC, CSIRT.CZ. *Základní principy DoS útoku* [online]. [cit. 1. 3. 2019] https://www.csirt.cz/page/2790/zakladni-principy-dos-utoku.

Relační vrstva	zahájení a ukončení relačního spojení	omezení služeb jinak přístupných přes Telnet	útok je možný v důsledku zranitelnosti, která může být updatem odstraněná
Transportní vrstva	TCP, UDP	SYN flood, Smurf attack. Omezuje počet sítových připojení na zařízeních	informování o blackholingu u svého poskytovatele připojení
Síťová vrstva	směrování a síťové adresování	ICMP flooding	stanovení limitu na ICMP
Linková vrstva	switche a přepínače	MAC flooding	omezení počtu MAC adres, které mohou porty přijmout
Fyzická vrstva	síťové kabely	fyzická manipulace s vedením	omezení fyzického přístupu

Tab. č. 1: Možné útoky na jednotlivých vrstvách OSI modelu[6]

DoS útok zpravidla cílí na servery a jimi poskytované služby. Efektivita útoku je postavená na faktu, že požadavek na server bývá co do objemu i potřebného počítačového výkonu menší než odezva serveru. Například požadavek na zobrazení webové stránky může mít několik desítek bytů, kdežto obsah stránky, kterou server poskytne, může mít několik megabytů.[7] Rozdíl mezi velikostí požadavku a serverovou odezvou tak může být i o několik řádů. I přes tento nepoměr však útočníkovi v dnešní době, vzhledem k řadě důvodů, nestačí vést útok z jednoho běžného počítače. Mezi tyto důvody patří např. možná detekce datového toku z jednoho zdroje provedená na straně cíle útoku nebo značný výkon serverů poskytujících žádané služby, kde je často umístěna celá farma serverů, mezi které jsou požadavky rozdělovány. Proto vedle prostého DoS útoku je velmi rozšířená jeho distribuovaná varianta, kdy k útoku dochází z celé řady počítačových systémů. Taková forma útoku se označuje jako Distributed Denial of Service (DDoS).

Prostý DoS a distribuovaná varianta DDoS jsou základními typy útoku, který cílí na odepření služby či potlačení dat. Typů DoS útoku je však více a jsou podrobněji rozebrány

[6] Tabulka převzata z CZ.NIC, CSIRT.CZ. *Základní principy DoS útoku* [online]. [cit. 1. 3. 2019] https://www.csirt.cz/page/2790/zakladni-principy-dos-utoku.
[7] Jeden megabyte představuje jeden milion bytů (přesněji 1 048 576 bytů).

v kapitole 1.3 Jednotlivé typy DoS útoků a související techniky. Protože je někdy nesnadné rozlišit, zda se jedná o prostou nebo distribuovanou variantu, bývají tyto útoky souhrnně označovány jako (D)DoS.[8]

Kybernetickou bezpečnost obecně chápeme jako zabezpečení dostupnosti, integrity a důvěryhodnosti informací.[9] DoS útoky cílí právě na zabezpečení dostupnosti služeb a s tím spojených dat a informací. Schopnost čelit těmto útokům tak patří mezi prvky zabezpečení provozovaných systémů a poskytovaných služeb. Problém je, že vzhledem k jejich formě je obrana proti DoS útokům velmi náročná. Protože cílem útoku je zahlcení, je možnou obranou naddimenzování počítačového systému tak, aby i při zvýšení počtu požadavků značně nad běžnou mez dokázal všechny tyto požadavky obsloužit. Takové naddimenzování však často není ekonomicky efektivní, neboť je potřeba u každé poskytované služby vážit, zda cena naddimenzování systému vyváží škody způsobené jeho disfunkcí během útoku.

Útočníci si pro distribuovanou verzi útoku mohou na černém trhu útočící stroje také poměrně levně pronajmout, a proto pouhým zvyšováním výkonu serverů a zvyšováním propustnosti internetových linek nelze útoku dostatečně čelit. Padesát virtuálních serverů pro vytvoření méně výkonného DDoS útoku, např. na on-line obchod, si lze pronajmout za 0,325 USD na 1 hodinu.[10]

Dalším problémem souvisejícím s ochranou před tímto útokem je schopnost jeho detekce. Jak má cílový systém rozpoznat, zda požadavek, který má obsloužit, je legitimní, nebo součástí útoku? U určitých forem útoku může být toto posouzení jednoduché, ale u sofistikované formy distribuovaného útoku cílový systém nemá většinou možnost rozeznat, zda je požadavek legitimní či nikoli. V posledních letech určitou ochranu proti DoS útokům nabízejí svým klientům i někteří poskytovatelé internetového připojení.[11] Ale ani ti nemusí být v boji proti DDoS útokům úspěšní. To dokládá tisková zpráva Českého statistického úřadu k DDoS útoku během zpracování výsledků parlamentních voleb v říjnu 2017: *„Bylo zjištěno, že v průběhu*

[8] Tento způsob označování je používán i v této práci.
[9] KOSTIHA, František. Bezpečnost informací. *Ikaros* [online]. 2006, roč. 10, č. 5 [cit. 1. 3. 2019]. Dostupné z: https://ikaros.cz/bezpecnost-informaci. ISSN 1212-5075.
[10] KASPERSKYLAB. *The cost of launching a DDoS attack* [online]. [cit. 1. 3. 2019]. Dostupné z: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/.
[11] Např. operátor T-mobile nabízí DDoS ochranu jako službu, viz http://www.gts.cz/sluzby/security/gts-ddos-ochrana. [cit. 1. 3. 2019].

zpracování došlo k cílenému DDoS útoku na infrastrukturu společnosti O_2 používanou pro zajištění voleb. V důsledku byla dočasně omezena dostupnost serverů volby.cz a volbyhned.cz.“[12]

Protože však úplná ochrana před těmito útoky neexistuje, došlo v ČR ke vzniku projektu FENIX, tzv. ostrovní sítě. *„Projekt FENIX vznikl na půdě českého peeringového uzlu, sdružení NIX.CZ, v roce 2013 jako reakce na intenzivní DoS útoky, kterým v březnu tohoto roku čelila významná česká média, banky nebo operátoři. Smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity.“*[13] Mezi členy týmu projektu FENIX patří zejména významní čeští poskytovatelé internetového připojení, poskytovatelé hostingových služeb a významný český poskytovatel obsahu, spol. Seznam.cz.[14]

1.2 Největší vlna DoS útoků v ČR

Významnou událostí ve vnímání nebezpečnosti DoS útoků v České republice byla série útoků, ke kterým došlo v březnu roku 2013 na známé české servery a jimi poskytované služby. Série útoků byla zahájena v pondělí dne 4. března 2013, kdy útoky cílily zejména na nejznámější české zpravodajské servery, jako jsou novinky.cz, idnes.cz, ihned.cz, lidovky.cz a další. Následující den došlo k útokům na servery společnosti Seznam.cz, tedy na nejrozšířenější český internetový vyhledavač, katalog firem, poskytovatele aplikace mapy.cz a dalších služeb. Ve středu 6. března pak došlo k útokům na webové servery největších českých bank – České spořitelny, Komerční banky, Československé obchodní banky, Raiffeisenbank a některých dalších bank. Spolu se servery komerčních bank byly terčem útoku i webové servery České národní banky. Tyto útoky měly za následek nejen nedostupnost webových stránek bank a internetového bankovnictví, ale vedly i k dílčím výpadkům e-commerce služeb, jako jsou platby platebními kartami. Série útoků byla završena ve čtvrtek dne 7. března, kdy se obětí útoku staly servery dvojice největších mobilních operátorů O2 a T-mobile. Všechny uvedené útoky způsobily výpadky a nedostupnost služeb poskytovaných servery, proti kterým byl útok veden.[15]

---

[12] ČESKÝ STATISTICKÝ ÚŘAD. *Tisková zpráva (22. 10. 2017) – Volební weby byly nedostupné kvůli DDoS útoku* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.czso.cz/csu/czso/volebni-weby-byly-nedostupne-kvuli-ddos-utoku.

[13] NIX.CZ. *O FENIXU* [online]. [cit. 1. 3. 2019]. Dostupné z: https://fe.nix.cz/#about.

[14] NIX.CZ. *ČLENOVÉ TÝMU FENIX* [online]. [cit. 1. 3. 2019]. Dostupné z: https://fe.nix.cz/#members.

[15] CZ.NIC. *Rekapitulace (D)DoS útoků ze dnů 4.3. - 7.3.* [online]. 2013 [cit. 1. 3. 2019]. Dostupné z: http://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf.

Z analýzy, kterou provedlo pracoviště CSIRT.CZ, Národní CSIRT[16] České republiky, vyplynulo, že nelze s jistotou říct, zda se jednalo o prosté DoS útoky nebo jejich distribuovanou variantu. Většina datového toku, který se útoku týkal, přišla do ČR prostřednictvím ruské sítě RETN. Při útocích byly použity níže popsané mechanismy SYN Flood, podvržení zdrojové IP adresy (IP spoofing) a technika odražení. Z analýzy také vyplývá, že ve většině případů útok přetížil systém před samotným cílovým serverem, obvykle firewall nebo load balancer.[17] Série útoků tak odhalila řadu slabých míst v síťových architekturách počítačových systémů, na které byl útok veden.[18]

Útoky tak ukázaly, že i provozovatelé služeb, kteří by měli na bezpečnost a stabilitu svých systémů dbát především, nedokázali útoky ustát bez úhony. A přitom by to podle provedené analýzy pro ně nemusel být takový problém. Proto v následujícím období řada poskytovatelů elektronických služeb začala na kybernetickou bezpečnost mnohem více dbát, rozšířily se nabídky poskytovatelů internetových připojení o služby kybernetické bezpečnosti a v neposlední řadě také došlo ke vzniku projektu FENIX.[19] Nebyly to ale jen tyto útoky, které vedly k celkovému zvýšení kybernetické bezpečnosti v ČR. K tomu přispělo také to, že v té době vzniklo Národní centrum kybernetické bezpečnosti (tehdy jako součást Národního bezpečnostního úřadu, dnes jako samostatný Národní úřad pro kybernetickou a informační bezpečnost) a začal se připravovat zákon o kybernetické bezpečnosti, který byl publikován ve sbírce zákonů jako zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti, s účinností od 1. ledna 2015.[20]

1.3 Jednotlivé typy DoS útoků a související techniky

Typologie útoků typu odepření služby není jednotná. Je to dáno jak dynamickým vývojem v oblasti informačních a komunikačních technologií, tak i tím, že se zabýváme typologií závadového chování, kde těžko bude existovat nějaká standardizace. Útoky můžeme třídit z několika hledisek. Zejména, zda se jedná o prostý nebo distribuovaný útok, a dále podle toho,

[16] Computer Security Incident Response Team, bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů.
[17] Load balancer je zařízení, které slouží k rozložení výkonu mezi několik systémů.
[18] CZ.NIC. *Rekapitulace (D)DoS útoků ze dnů 4.3. - 7.3.* [online]. 2013 [cit. 1. 3. 2019]. Dostupné z: http://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf.
[19] K projektu FENIX podrobněji viz kapitola 1.1 Charakteristika útoku typu odepření služby.
[20] Zákon č. 557/1991 Sb., *zákon, kterým se mění a doplňuje trestní zákon*, zrušen.

jaké nástroje a techniky jsou při jeho realizaci použity. V literatuře tak můžeme najít dělení mírně odlišná. Z hlediska potřeb této práce je následující dělení zaměřeno především na typy a techniky, které se projeví v trestněprávním posouzení útoku.

1.3.1 Prostý DoS útok

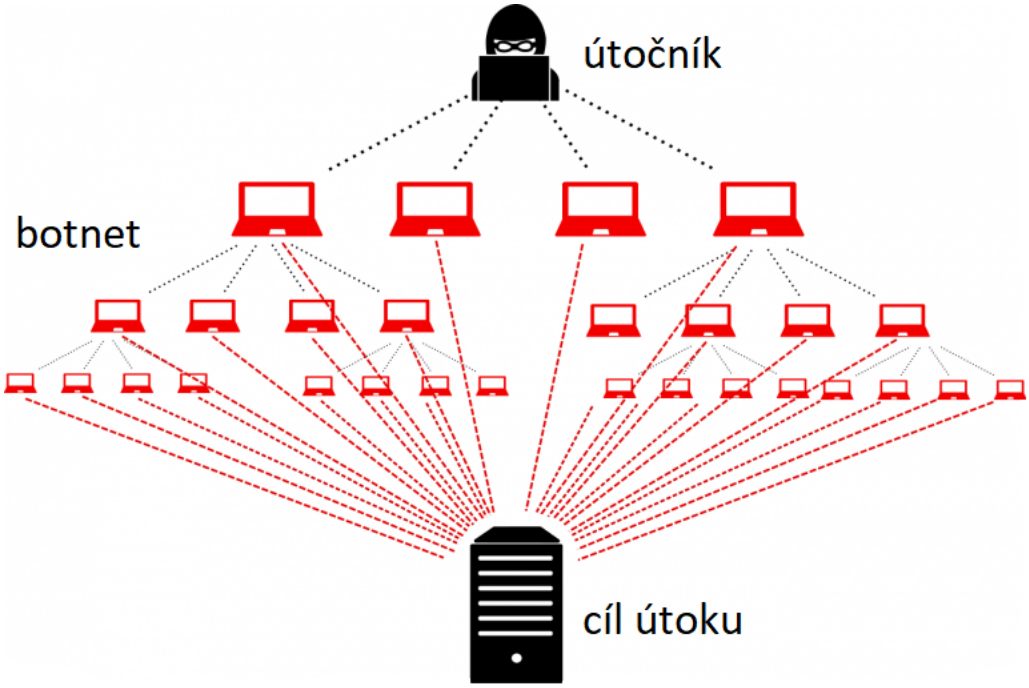
Prostý DoS útok je základní variantou útoku, jehož cílem je znepřístupnit službu nebo způsobit její nefunkčnost. V případě prostého DoS útoku je zdrojem útoku jediný počítač. Veškerá útočná data tak tečou pouze z jednoho zdroje, což usnadňuje detekci a obranu proti takovému útoku. Při tomto typu útoku může být využita některá z níže uvedených doplňujících technik – ICMP záplava, záplava pakety SYN nebo podvržení IP adresy.

1.3.2 Distribuovaný DoS – DDoS

V případě distribuovaného útoku označovaného DDoS dochází k zahlcení útokem napadeného počítačového systému pomocí paketů s požadavky, které jsou odesílány z celé řady počítačových systémů, často z geograficky různě rozmístěných lokalit. To významně ztěžuje detekci samotného útoku a také obranu proti němu, stejně jako identifikaci útočníka.

Za účelem provedení DDoS útoku jsou často využívány sítě zotročených počítačů, tzv. botnety. Při využití botnetu útočník prostřednictvím řídícího serveru zašle jednotlivým zotročeným počítačům úkol, který pak tyto ovládané počítače plní. Schéma útoku je znázorněno na obrázku č. 1. Botnet může útočník za daným účelem buď sám budovat pomocí napadání zranitelných počítačových systémů, nebo si jej za účelem útoku může koupit či častěji spíše pronajmout na černém trhu.[21]

[21] KASPERSKYLAB. *The cost of launching a DDoS attack*. SECURELIST.com [online]. [cit. 1. 3. 2019]. Dostupné z: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784.



Obr. č. 1: DDoS útok pomocí botnetu[22]

K těmto útokům také dochází na základě aktivit různých hacktivistických skupin nebo obecně uživatelů podporujících určitou online kampaň. Hacktivismus můžeme definovat jako *„použití hackerských dovedností a technik k dosažení politických cílů a podpoře politické ideologie.“*[23] V takovém případě je útok proveden jednotlivými osobami, které se prostřednictvím internetu nebo jiného komunikačního kanálu svolají a domluví společný útok na určitý termín. K tomuto typu jednání docházelo i v případě hacktivistického hnutí Anonymous, které bylo formováno v rámci protestů proti dohodě ACTA (Anti-Counterfeiting Trade Agreement) v roce 2012. Za účelem páchání organizovaných DDoS útoků členy hnutí Anonymous a jejich příznivci byly využity softwarové nástroje LOIC (Low Orbit Ion Cannon) nebo HOIC (High Orbit Ion Cannon). Ty umožnily, aby se na útoku podílely i osoby bez detailních technických znalostí o provedení útoku, kterých byla v rámci hnutí Anonymous většina.[24]

[22] Obrázek převzat z https://ruggedtooling.com/what-are-ddos-attacks. [cit. 1. 3. 2019].
[23] JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. 2. vydání. Praha: Policejní akademie ČR v Praze, 2013, s. 41.
[24] ITNEWS.COM.AU. *How dangerous is Anonymous?* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.itnews.com.au/news/how-dangerous-is-anonymous-248990.

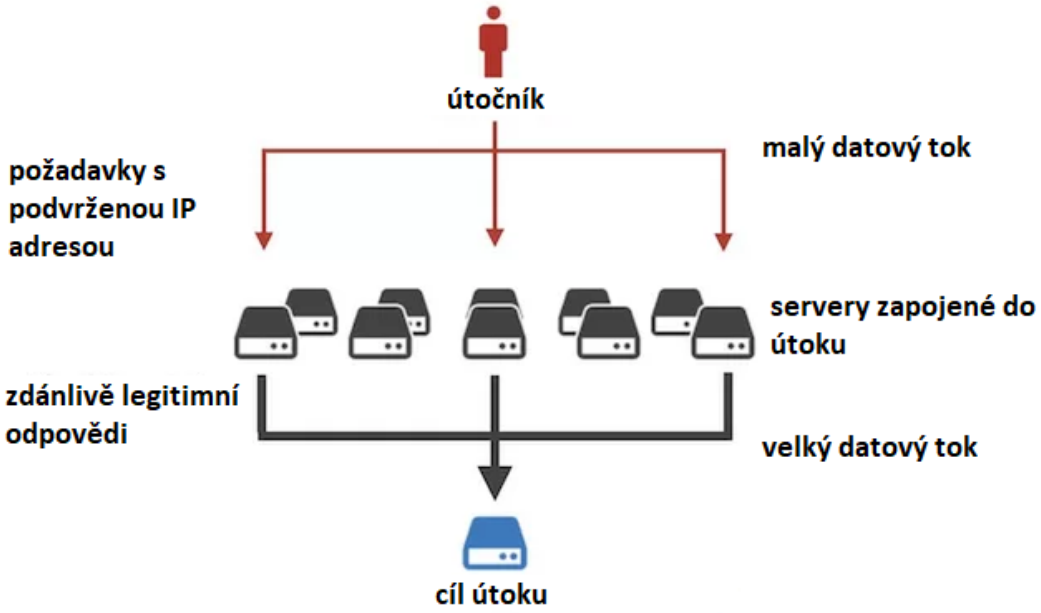
Na podobném principu někdy může dojít také k situaci, která DDoS útok připomíná tím, že dojde k zahlcení cílového počítačového systému, ale o útok se nejedná. K takové aktivitě může dojít např. v reakci na marketingové sdělení, kdy po zveřejnění lákavé časově velmi omezené nabídky, např. prostřednictvím televizní reklamy, dojde k připojení velkého množství uživatelů na inzerovanou webovou stránku a server, který tuto službu poskytuje, nápor nevydrží. Za útok bychom takovou situaci mohli považovat pouze v případě, že by byla vyvolána nějakou za tímto účelem cíleně šířenou dezinformací, např. falešnou lákavou nabídkou levného zboží, která by vedla vlivem zájemců k přetížení serverů domnělého prodejce.

Jinou situací, která je svými projevy DDoS útoku také podobná, přestože se o útok vůbec nejedná, je stav, kdy k zahlcení cílového počítačového systému nebo komunikačních linek dojde v důsledku špatně provedené konfigurace tohoto systému nebo jeho části, popř. z důvodu technické chyby. Typicky může dojít ke špatnému nastavení síťových prvků, v jehož důsledku dochází k cyklení či rozmnožování datových paketů, které cílový systém přetíží.

1.3.3 Distribuovaný odražený DoS (DRDoS)

Technika odražení (reflection nebo bounce traffic) se používá k zesílení útoku. Útok poté označujeme zkratkou DRDoS (Distributed Reflected Denial of Service). Princip spočívá v podvržení zdrojové IP adresy v útočném paketu, kde je jako podvržená IP adresa odesílatele použita adresa serveru, na který je primární útok veden. Jako cílová adresa paketu je použita adresa nějakého internetového serveru. Těchto paketů je generováno velké množství s různými cílovými adresami (tyto pakety jsou poměrně malé). Cílové stroje pak na iniciovanou komunikaci odpoví na uvedenou IP adresu, tedy serveru, který je primárním cílem útoku (paket s odpovědí je výrazně větší, než paket s požadavkem). Do útoku jsou tak zapojeny servery, které o svém zapojení do škodlivé činnosti vůbec neví. Tyto servery útočníkovi pomáhají zesílit datový tok na oběť útoku, který je násobně větší než tok, který emituje útočník. Schéma útoku je znázorněno na obrázku č. 2. Tato technika navíc ztěžuje identifikaci útočníka.[25]

[25] MALWARE PATROL. *DDoS Reflection and Amplification Attacks* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.malwarepatrol.net/ddos-reflection-and-amplification-attacks.



Obr. č. 2: Distribuovaný odražený DoS

Určitým podtypem tohoto typu útoku je DNS zesilující útok (DNS amplification attack), který do odraženého útoku zapojuje otevřené DNS resolvery. To jsou internetové servery, které slouží k překladu doménových jmen na IP adresy, a kterých je v prostředí sítě internet celá řada. Tím, že jich je hodně a jsou veřejně dohledatelné, je provedení útoku s jejich využitím poměrně snadno realizovatelné.[26]

1.3.4 ICMP záplava (Ping Flood)

Program ping (název vznikl zkratkou z anglického názvu Packet Internet Groper) slouží k ověření funkčnosti síťového spojení mezi dvěma síťovými rozhraními, které mohou být představovány počítači nebo síťovými prvky. Program lze využít v síti, která komunikuje pomocí rodiny protokolů TCP/IP, což je v dnešní době naprostá většina počítačových sítí. Na této rodině protokolů je postaven i internet. Program ping pro komunikaci využívá protokolu ICMP (Internet Control Message Protocol). Při prověření spojení je odeslán paket se zprávou ICMP Echo Request. Protistrana odpovídá zprávou ICMP Echo Reply. Program ping při přijetí odpovědi na

[26] CLOUDFLARE.COM. *DNS Amplification Attack* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack.

svůj požadavek také spočítá tzv. odezvu, tedy dobu, jaká uplynula od odeslání výzvy do přijetí odpovědi. Tento údaj se mj. používá pro ověření kvality datových linek.[27]

Útok Ping Flood je jednoduchým DoS útokem, který spočívá v zahlcení cílového systému ICMP Echo Request požadavky. K tomu se využívá také možnosti *„flood"* (záplava), která spočívá v odesílání dalších a dalších požadavků bez čekání na odpověď. Smyslem útoku je zahltit šířku přenosového pásma útočníka, popř. vyčerpat systémové zdroje koncového systému. Aby měl útok smysl, měl by útočník disponovat širším přenosovým pásmem než cíl útoku. Měl by tedy mít kvalitnější internetové připojení a dostatečně výkonný počítač.[28]

Jedná se o starší typ útoku, který je snadno odhalitelný a je možné se proti němu poměrně efektivně bránit. Ochrana může být realizována např. pomocí vhodně nastaveného firewallu na cílovém systému, který dokáže záplavu ICMP Echo Request požadavků detekovat. V takovém případě pak cílový systém nebude na útočící požadavky posílat odpovědi.

1.3.5 Záplava pakety SYN (SYN Flood)

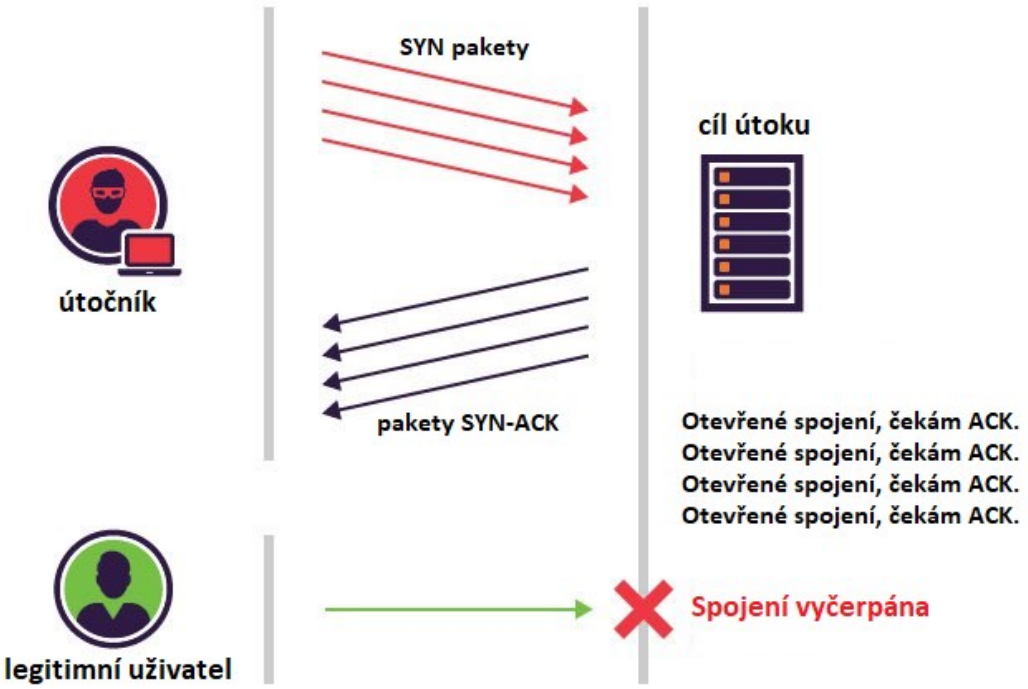
Účelem útoku založeném na SYN Flood je zahltit cílový server nebo síťovou infrastrukturu, která mu předchází, zejména routery a firewally, a vyčerpat jejich systémové zdroje s ohledem na vlastnosti datové komunikace.[29]

V počítačových sítích, které komunikují pomocí rodiny protokolů TCP/IP, se pro komunikaci na 4. vrstvě OSI modelu[30] využívají zejména protokoly UDP a TCP. Protokol UDP je nepotvrzovaný, kdy při komunikaci prostřednictvím tohoto protokolu nedochází k tzv. navázání spojení ani potvrzování přijatých zpráv. Je tak využitelný spíše pro jednodušší a neobjemné přenosy. Protokol TCP je potvrzovaný, kdy při komunikaci jeho prostřednictvím nejprve dojde k navázání spojení pomocí tzv. třícestného handshake. Ze strany A iniciující spojení dojde nejprve k odeslání TCP paketu s příznakem SYN (synchronization – synchronizace). Takový paket představuje žádost o navázání spojení. Přijímající strana B na tento

[27] TECHTERMS.COM. *Ping* [online]. [cit. 1. 3. 2019]. Dostupné z: https://techterms.com/definition/ping.
[28] CLOUDFLARE.COM. *Ping (ICMP) Flood DDoS Attack* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack.
[29] CZ.NIC. *Rekapitulace (D)DoS útoků ze dnů 4.3. - 7.3.* [online]. 2013 [cit. 1. 3. 2019]. Dostupné z: http://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf.
[30] K OSI modelu podrobněji viz kapitola 1.1 Charakteristika útoku typu odepření služby.

paket odpoví straně A paketem TCP s příznaky SYN a ACK (acknowledge – potvrzení). Strana A na přijatý paket odpoví TCP paketem s příznakem ACK. Po odeslání tohoto v pořadí třetího paketu je spojení navázáno. Navázání spojení a následné potvrzování každého doučeného paketu zajišťuje stabilitu spojení a možnost opakování konkrétního paketu v případě jeho nedoručení.

Útok v podobě záplavy pakety SYN (SYN Flood) je formou DoS útoku, kdy útočník posílá cílovému systému (tomu, na který se útočí) pakety s příznakem SYN, ale v takto započaté komunikaci dále nepokračuje. Pokud cílový systém přiděluje prostředky (např. paměťové) těmto polootevřeným spojením a je zaplaven útočnými SYN pakety, může dojít k vyčerpání těchto prostředků. To pak vede k neschopnosti tohoto systému dále komunikovat, k jeho zpomalení anebo k úplnému pádu. Schéma útoku je znázorněno na obrázku č. 3.



Obr. č. 3: Záplava pakety SYN[31]

Tento typ útoku je v popsané základní variantě úspěšný dnes už jen u starších systémů, které neměly dostatek systémových prostředků pro větší počet polootevřených spojení. Moderní systémy jsou lépe dimenzovány a existují možnosti obrany proti tomuto typu útoku. Používaným

[31] Obrázek převzat z https://www.incapsula.com/ddos/attack-glossary/syn-flood.html. [cit. 1. 3. 2019].

způsobem obrany je využívání tzv. SYN cookies[32] nebo omezení počtu nových spojení z jednoho zdroje.[33]

Tento typ útoku ale může být kombinován s níže popsanou technikou podvržení IP adresy (IP Spoofing), čímž se stává o poznání nebezpečnějším.

1.3.6 Podvržení IP adresy (IP Spoofing)

IP protokol je nejrozšířenějším komunikačním protokolem 3. vrstvy OSI modelu[34] a bez jeho existence by internet vůbec nebyl. Nebo alespoň ne v té podobě, jak jej známe dnes. Pro identifikaci zdrojové i cílové strany jsou v hlavičce IP paketu uvedeny jejich adresy – IP adresy. Podle verze protokolu IPv4 (verze 4) a IPv6 (verze 6) rozeznáváme dvě podoby IP adresy. V případě protokolu IPv4 je IP adresa tvořena čtveřicí čísel oddělených tečkou, kde každé z těchto čísel nabývá hodnoty 0 až 255, např. 192.168.0.1. V případě IPv6 existuje několik možných zápisů IP adresy, ale obecně se jedná o řetězec v podobě osmi čtveřic hexadecimálních znaků[35] oddělených dvojtečkou, např. FE80:0000:0000:0000:0202:B3FF:FE1E:8329.

Při technice podvržení IP adresy útočník v IP paketu nahradí svou adresu jako skutečného odesílatele jinou adresou. Ta podle typu útoku může být smyšlená (tím pouze ztíží svou identifikaci) nebo reálná, např. serveru, na který je útok veden pomocí výše uvedeného typu útoku distribuovaný odražený DoS.[36] Cílový systém pak na tyto pakety neodpovídá jejich skutečnému odesílateli, ale v domnění, že uvedená IP adresa odesílatele je pravá, odpovídá na tuto podvrženou adresu. Této techniky lze použít pouze v případě, že útočník nepotřebuje od cílového systému odpověď. Při podvržení zdrojové IP adresy např. není možné dokončit třícestný handshake, podrobně popsaný v bodu 1.3.5 Záplava pakety SYN (SYN Flood). Toto omezení ale útočníkovi v případě DoS útoku většinou nevadí. Jeho cílem je napadený systém pouze zaměstnat a dovést ho k vyčerpání jeho systémových zdrojů nebo přetížit komunikační linku, k čemuž navázání spojení pomocí handshake obecně nepotřebuje.

---

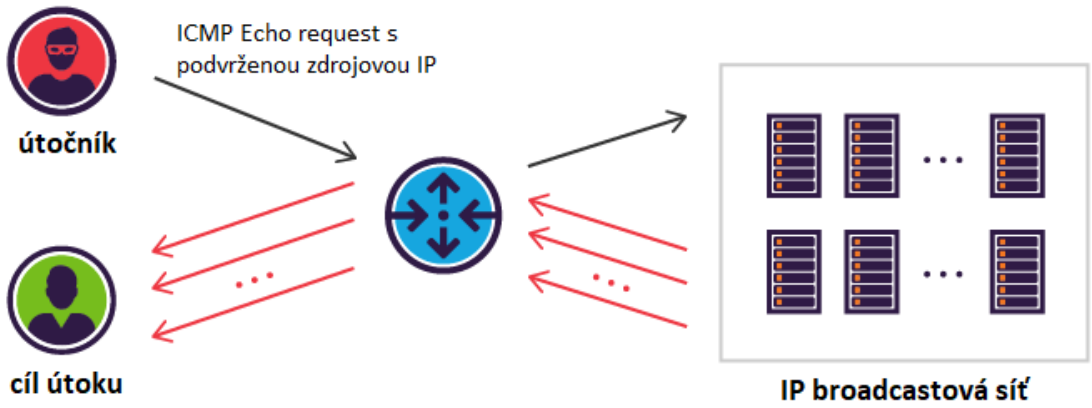
[32] Při použití SYN cookies server po obdržení iniciačního paketu s příznakem SYN protistraně odpoví se uvedením sekvenčního čísla, které je vygenerováno podle stanovených pravidel, a danou žádost odstraní z fronty. Obdrží-li server od protistrany potvrzení jeho odpovědi, tedy paket s příznaky SYN a ACK, je podle uvedeného sekvenčního čísla schopen dovodit, zda se jedná o korektní paket, a jen v takovém případě je spojení navázáno.
[33] BERNSTEIN, Daniel J. *SYN cookies* [online]. [cit. 1. 3. 2019]. Dostupné z: http://cr.yp.to/syncookies.html.
[34] K OSI modelu podrobněji viz kapitola 1.1 Charakteristika útoku typu odepření služby.
[35] Znaky hexadecimální neboli šestnáctkové soustavy jsou číslice 0 až 9 a písmena A až F.
[36] Viz bod 1.3.3 Distribuovaný odražený DoS (DRDoS).

1.3.7 Útok Smurf (Smurf attack)

V počítačových sítích je kromě komunikace s konkrétní jednoznačně identifikovanou stranou (pomocí unikátní adresy) možné komunikovat také pomocí tzv. broadcastů. Ty nejsou doručeny jedné konkrétní straně, ale všem příjemcům broadcastu, což jsou podle typu použitého protokolu obecně všechny počítače v určitém segmentu sítě. Pro broadcastovou komunikaci se do paketu namísto cílové adresy konkrétní protistrany použije adresa broadcastu. Tu je možné určit podle nastavených parametrů síťového rozhraní. Broadcast se používá např. při vzdáleném získávání konfigurace síťového rozhraní.

Útok nazývaný Smurf Attack (český ekvivalent tohoto názvu lze jen těžko hledat) využívá protokolu ICMP a jeho zpráv v podobě ICMP Echo Request[37] v kombinaci s technikou podvržení IP adresy a technikou odražení. U tohoto typu útoku jsou ze strany útočníka odesílány ICMP Echo Request pakety s podvrženou IP adresou odesílatele. Jako zdrojová (odesílající) adresa je uvedena adresa systému, na který je útok veden (jde tak o využití techniky odražení). Tento paket však není adresován konkrétnímu systému, ale jako cílová adresa je uvedena broadcastová adresa. Je tedy určen všem zařízením připojeným k dané části počítačové sítě. Jakmile začnou všechna tato zařízení odpovídat na zaslaný požadavek, nedobrovolně se zapojí do distribuovaného DoS útoku na cílový systém. Princip útoku je znázorněn na obrázku č. 4. Protože zařízení zapojených do sítě může být velké množství, cílový systém je zahlcen mohutným datovým provozem, který je v rámci útoku generován.

[37] K protokolu ICMP podrobněji viz bod 1.3.4 ICMP záplava (Ping Flood).



Obr. č. 4: Útok Smurf[38]

Protože uvedený postup, kdy je zasílán ICMP paket s cílovou broadcastovou adresou, se v legitimním provozu nevyskytuje, je možné útok poměrně snadno identifikovat. Bránit se mu lze preventivně pomocí zákazu odpovědi na ICMP paket s uvedenou broadcastovou adresou. Současně je od roku 1999 standardizováno pravidlo routerů takový provoz nepřeposílat dále. Do té doby pravidla naopak předávání takového provozu vyžadovala.[39]

Tento útok byl pojmenován po souboru smurf.c, který byl součástí zdrojového kódu útočného programu z roku 1997, jenž naprogramoval Dan Moschuk, zvaný TFreak.[40]

Od Smurf útoku byla odvozena varianta tohoto útoku v podobě tzv. Fraggle útoku. Tato varianta se liší tím, že namísto ICMP paketů dochází k odesílání specifických UDP paketů. Adresy jsou nastaveny stejně jako v případě základního Smurf útoku. Tento typ útoku je hůře detekovatelný než základní Smurf útok, a i obrana proti němu je složitější, neboť nelze tak snadno rozlišit legitimní a nelegitimní datový provoz.

Tato varianta útoku je pojmenována také podle názvu souboru zdrojového kódu útočného programu fraggle.c, který opět naprogramoval TFreak.[41]

---

[38] Obrázek převzat z https://www.incapsula.com/ddos/attack-glossary/smurf-attack-ddos.html. [cit. 1. 3. 2019].
[39] SENIE, Daniel. Changing the Default for Directed Broadcasts in Routers. *RFC 2644* [online]. [cit. 1. 3. 2019]. Dostupné z: https://tools.ietf.org/html/rfc2644.
[40] HACKPEDIA.ORG, *Tfreak* [online]. [cit. 1. 3. 2019]. Dostupné z: http://hackepedia.org/?title=Tfreak.
[41] ANONYMOUS. *Maximum Security*. 4. vydání. USA: Sams Publishing, 2003, s. 310.

2 Kriminologická část

Kybernetickou kriminalitu můžeme studovat také z pohledu faktorů, které vedou k jejímu vzniku a udržení, jak je páchána a jaké jsou možnosti její prevence. Nejen těmto tématům je věnována následující část. Při rozboru kriminologických jevů týkajících se pachatele a oběti uvedených v této části se omezíme na (D)DoS útoky.

2.1 Rozmach kybernetické kriminality

Tím, jak počítače a počítačové systémy stále více pronikají do životů všech lidí, do fungování komerčních i veřejných subjektů a států, jsou všude okolo nás. Kromě samostatných počítačů a počítačových sítí je najdeme integrované v domácích spotřebičích, automobilech, starají se o řízení křižovatek, tunelů, letišť a leteckého provozu, vypořádání obchodů a své místo nacházejí v řadě dalších aplikací. Pokud je něčeho mnoho, zvyšuje se v absolutním měřítku i potenciál souvisejících problémů, včetně potenciální trestné činnosti. Pokud se zvyšuje závislost lidí na počítačích, ceníme si uložených dat a jsou prostřednictvím počítačových systémů realizovány transakce o značném finančním objemu, zvyšuje se i zájem útočníků o toto prostředí, neboť realizací elektronického útoku mohou přímo či nepřímo získat finanční prospěch.

Faktorů, které způsobují rozmach kybernetické kriminality, je celá řada. Jedná se o technologické, sociologické, psychologické, historické a další důvody. Přehled těch nejdůležitějších uvádí ve své disertační práci Jiří Krupička: *„globalizace, technologický pokrok, nízké náklady internetové kriminality, nízké právní vědomí obětí a pachatelů, závislost dnešního světa na internetu a počítačích vůbec, absence schopných strážců, anonymita, nízká koupěschopnost obyvatel některých zemí.“*[42]

Z globálního pohledu je zásadní rozsah dostupnosti internetu. Ta dosahuje vysoké úrovně a stále narůstá. Podle odhadů a statistik Mezinárodní telekomunikační unie z prosince 2018 mělo na konci roku 2018 internet užívat 51,2 procent globální populace.[43] To samo se sebou nese

[42] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality* [online]. [cit. 1. 3. 2019]. Praha, 2012. Disertační práce. Univerzita Karlova. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/68976, s. 17-18.
[43] MEZINÁRODNÍ TELEKOMUNIKAČNÍ UNIE. *ITU releases 2018 global and regional ICT estimates. 2018* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx.

vysoký potenciál kybernetické kriminality, neboť tato dobrá dostupnost a snadnost přístupu platí i pro pachatele.

Zaměříme-li se na technologický pokrok, musíme si uvědomit, že nejde jen o pokrok týkající se zlepšování a zrychlování počítačových systémů a datových sítí, ale i nástrojů, které pachatelé při provádění škodlivé činnosti užívají. I jejich nástroje jsou rychlejší, efektivnější a jednodušší na obsluhu.[44] V souvislosti s technologickým pokrokem dochází i ke snižování nákladů na páchání internetové kriminality. Pachateli k páchání závadové činnosti postačí běžný počítač, jehož cena dnes začíná hluboko pod 10 000 Kč. Přitom v roce 1981 byla cena základního osobního počítače IBM 1 565 USD (vlivem inflace by při dnešních cenách šlo o více než 4 000 USD, tedy více než cca 92 000 Kč).[45]

Nízké právní vědomí je faktorem, který se týká jak pachatelů, tak i obětí kybernetické kriminality. Zejména vzhledem k jednoduchosti a dostupnosti některých softwarových nástrojů může dojít k nevědomému páchání trestné činnosti. Často je to ve vztahu k autorskému právu při stahování obsahu prostřednictvím software, který stažený obsah automaticky nabízí ke stažení dalším uživatelům.[46] Neznalost, důvěřivost a často až naivita některých uživatelů internetu způsobuje jejich náchylnost k tomu stát se terčem elektronického útoku. Často způsobí i následné neuvědomění si faktu, že se daný uživatel stal obětí trestného jednání, což má vliv i na latenci kybernetické kriminality. Prostřednictvím internetu dochází k páchání velkého množství trestných činů souvisejících s touto nevědomostí.[47]

Závislost dnešního světa na internetu a počítačích vůbec je kritickým faktorem současné doby. Jedná se nejen o závislost každého z nás, která se projevuje návyky na dostupnost telefonu, instant messagingu,[48] e-mailu, různých informačních zdrojů a dalších informačních a komunikačních kanálů. Vedle toho jde ale i o závislost celospolečenských potřeb, jako je např. veřejná doprava. Jen těžko si lze představit řízení letového provozu a letišť bez počítačů a komunikačních systémů na ně napojených. Závislost se týká i veřejné správy – různé registry a

[44] Zde je možno připomenout např. nástroje LOIC a HOIC uvedené v části 1, kapitole 1.3, bodu 1.3.2 Distribuovaný DoS – DDoS.
[45] 24/7 WALL ST. *The Cost of a Computer the Year You Were Born* [online]. [cit. 1. 3. 2019]. Dostupné z: https://247wallst.com/special-report/2016/04/15/how-much-a-computer-cost-the-year-you-were-born.
[46] Např. stahování prostřednictvím tzv. torrentů.
[47] DIANIŠKA, Gustáv a kol. *Kriminológia*. Plzeň: Aleš Čeněk, 2009, s. 247.
[48] Pojmem instant messaging rozumíme různé komunikační nástroje pro okamžitou komunikaci – Messanger, Viber, Whats App, …

databáze jsou v dnešní době dostupné elektronicky. I v případě, že by existovala jejich klasická (papírová) podoba, doba zotavení a přechodu na tuto papírovou podobu by byla neúnosně dlouhá, následná použitelnost by byla silně obtížná a prováděná činnost značně neefektivní. Prostřednictvím internetu také dochází k vypořádání celé řady obchodů. Jen celosvětový objem on-line nákupů v roce 2017 dosáhl 2,3 bilionu amerických dolarů (cca 52,5 bilionu Kč).[49] Výpadek informačního nebo komunikačního systému tak u zapojených subjektů vede k významným ztrátám. Z této značné závislosti pak pramení velký prostor pro páchání trestné činnosti v kybernetickém prostředí.

Absence schopných strážců souvisí s globálností a decentralizací internetu, jako počítačové sítě, která nemá centrální autoritu a neexistuje tak tzv. červené tlačítko, které by umožnilo internet vypnout. Na provozu internetu se podílí celá řada autorit, které se starají o správu doménových jmen, přidělování IP adres a o další základní potřeby fungování internetu,[50] ale zejména celá řada poskytovatelů internetového připojení, kteří vlastní části přenosových sítí a souvisejících technologií. Tato značně heterogenní síť (jak z hlediska své konstrukce, tak i správy), která se geograficky rozkládá po celé planetě Zemi, bez vlivu stanovených geografických hranic jednotlivých států, tak představuje těleso s obtížnou kontrolou dění, které se v něm odehrává. K tomu také přispívá nejednotnost právních řádů jednotlivých zemí ve vztahu k elektronickým komunikacím a dalším relevantním právním odvětvím. To celkově snižuje možnost kontroly, aplikace protiopatření v případě identifikovaného problému nebo kriminálního jednání, možnost získání relevantních důkazních prostředků atp.

Anonymita působení na internetu je dalším z klíčových faktorů, které mají vliv na kybernetickou kriminalitu. Internet často působí jako anonymní prostředí, kde uživatele bez uvedení jeho podpisu lze jen těžko dohledat. To však není pravda. Anonymita na internetu je pouze relativní. Každý uživatel je identifikován v daném segmentu sítě jedinečnou adresou (v prostředí internetu typicky hovoříme o IP adrese). Existují však nástroje a techniky, které identitu uživatele mohou skrýt nebo nahradit identitou někoho jiného.[51] Na základě použité techniky nebo

[49] STATISTA. *Online-Shopping and E-Commerce worldwide: Statistics & Facts* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.statista.com/topics/871/online-shopping.
[50] V této oblasti je klíčová role mezinárodní neziskové organizace ICANN (Internet Corporation for Assigned Names and Numbers).
[51] Jedná se např. o techniku podvržení IP adresy popsanou v technické části této práce, dále o anonymizační síť TOR, VPN připojení atp.

jejich kombinací může být míra anonymity menší nebo větší, zcela stoprocentní anonymity však lze dosáhnout jen těžce. Telekomunikační operátoři v řadě zemí světa mají povinnost uchovávat provozní a lokalizační údaje o svých zákaznících,[52] podobné údaje uchovávají i provozovatelé různých internetových aplikací a služeb. V případě, že pachatel použije některou z anonymizačních technik, je pro orgány činné v trestním řízení možné z těchto uchovávaných dat čerpat a na jejich základě pachatele deanonymizovat. Úspěšnost odanonymizování však závisí na množství detailu, době uchování a kvalitě provozních záznamů, a často i na ochotě jejich držitele, pokud mu vydání těchto dat nenařizuje zákon. V tomto ohledu je důležitá také mezinárodní justiční spolupráce, neboť útoky i v rámci jedné země jsou často z důvodů znesnadnění dohledání pachatele prováděny s využitím počítačových systému v zahraničí.[53] Tato často relativní anonymita však na pachatele působí, dodává jim pocit bezpečí, který by v reálném prostředí získali jen těžko.[54]

Nízká koupěschopnost obyvatel některých zemí patří ke kriminogenním faktorům, zejména v souvislosti s trestnou činností týkající se práva duševního vlastnictví. Pokud je výše licenčních poplatků neúměrná koupěschopnosti obyvatel dané země, logicky to vede k získání obsahu jinak, než koupí. Vysoká míra porušování autorských práv se týká i České republiky, kdy zejména v 90. letech 20. století a v prvním desetiletí 21. století bývala cena nosičů s autorským obsahem nepřiměřeně vysoká vůči koupěschopnosti obyvatel. Byla také v nepoměru ke snadnosti získání obsahu koupí neoriginální kopie nebo stažením z internetu. Postupem času se však ceny originálních nosičů snížily a došlo ke zvýšení mezd a platů. Placený obsah je také za přijatelnějších podmínek nabízen i on-line. To by mělo vést ke snížení kriminality v této oblasti. Dokládají to i slova Pavla Bodiše z Mezinárodní federace hudebního průmyslu publikovaná v článku iDnes.cz v roce 2012: *„Prodeje hudebních CD v Česku loni po letech poklesů výrazně stouply díky velkému zlevnění.“*[55]

[52] V ČR je tato povinnost dána ustanovením § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, v platném znění.
[53] Např. s využití zahraniční anonymizační VPN služby.
[54] HUNTON, Paul. The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*. Vol. 25. Elsevier B.V., 2009. s. 529, 533.
[55] iDNES.CZ. *Kultura (14. 8. 2012) – Hudební CD v Česku zlevnila a jejich prodej meziročně výrazně stoupl* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.idnes.cz/kultura/hudba/prodej-cd-vyrazne-stoupl.A120814_132600_hudba_ob.

2.2 Latence kybernetické kriminality

Kybernetická kriminalita se vyznačuje vysokou latencí. Patrně jde o nejvíce skrytou kriminalitu vůbec. Je to dáno nízkou schopností a pravděpodobností její detekce, jednoduchostí jejího páchání a častým nezájmem či neochotou obětí tuto trestnou činnost oznamovat. To se týká např. bank, které nechtějí, aby se veřejnost dozvěděla o průniku do jejich informačních systémů a nesnížila se tak jejich kredibilita.[56]

Většina kybernetických trestných činů není vůbec zjištěna, což souvisí s nízkou schopností detekce elektronických útoků. Rozmach počítačových virů, technik hackingu a APT útoků[57] vede postupně k rozvoji detekčních schopností. Ty však stejně jako v jiných odvětvích jsou a budou vždy nejméně několik kroků za útočníky. Že je prevence důležitá si uvědomují výrobci operačních systémů, kteří postupně v nových verzích svých produktů nabízí výchozí nastavení provedená s ohledem na bezpečnost. Dále nabízí řady vlastních nástrojů pro ochranu i možnost integrovat bezpečnostní řešení od jiných dodavatelů nejrůznějších produktů, jakými jsou antivirový program, firewall, management aktualizací software atp. Uvědomují si to i výrobci síťových prvků, kteří ve svých produktech poskytují stále lepší ochranu proti elektronickým útokům a možnost napojení na centralizovanou správu spojenou s dohledem celé sítě. V neposlední řadě existují komplexní nástroje pro analýzu dění v počítačových systémech a sítích, které mohou detekovat anomálie a podezřelé chování. Prevence však musí začít u samotných uživatelů, protože jsou to oni, kdo si bezpečnostní nástroje instalují do svých počítačů a ostatních zařízení, aktualizují operační systémy a další software a celkově se mají chovat bezpečně. V tomto ohledu také dochází k posunu, uživatelé jsou postupem času zodpovědnější. Nicméně počítač nebo telefon je pro běžného uživatele pouze prostředek pro komunikaci, práci či zábavu, a logicky tak nechce trávit mnoho času správou a nastavováním těchto zařízení. Ke zlepšení celkového stavu tak povedou především bezpečnostní prvky, které jsou jednoduché na jejich zavedení i následnou správu.

[56] SVATOŠ, Roman. *Kriminologie*. Plzeň: Aleš Čeněk, 2012, s. 190.
[57] APT (Advanced Persistant Threat) je označení pro útoky založené na sofistikovaných hackerských technikách zaměřených přímo na konkrétní cíl, kterým mohou být velké společnosti či státy. Těchto útoků se užívá zejména při kyberšpionáži.

Kvalitní zabezpečení a schopnost detekce tak ve svém důsledku vedou ke ztížení páchání trestné činnosti. Významnou roli pak hraje také rychlost, resp. včasnost detekce. Řada kybernetických útoků je odhalena s velkým odstupem času, někdy až po řadě let. Např. nedávno zjištěný útok na rezervační systém hotelového řetězce Marriot Hotels, při kterém útočníci získali osobní data až 500 milionů klientů, probíhal bez odhalení po dobu 4 let.[58] Neschopnost včasné detekce usnadňuje pachatelům jejich aktivitu, neboť s odstupem času je v elektronickém světě obtížné přesně identifikovat útočníka, zejména vlivem průběžného odmazávání provozních záznamů a změn topologií počítačových sítí.

K latenci kybernetické kriminality významně přispívá i neochota obětí oznamovat zjištěné trestné činy orgánům činným v trestním řízení. Týká se to zejména komerčních subjektů, které se bojí ztráty své kredibility ze strany klientů, akcionářů nebo i zaměstnanců. S tím se setkáváme nejen u bank, ale i u obchodních společností a řady dalších subjektů. Nejen komerčních subjektů se pak týkají další faktory, které vedou k neoznámení útoku. Jedním z dalších faktorů je strach, jenž má oběť v souvislosti s vyšetřováním činu, které může odhalit, že i ona např. užívá nelegální software nebo jinak porušuje autorská práva. Nebo oběť prostě raději vlastním úsilím překoná problémy způsobené útokem a nemá zájem věc dále řešit. Neméně důležitým faktorem je pak viktimnost, tedy disponovanost jedince či skupiny osob stát se obětí trestného činu.[59] Do viktimnosti řadíme i vnější okolnosti ohrožující jedince, který se pak stává snadněji obětí trestného činu. Oběť se může obávat toho, že spolu se zveřejněním faktu, že se stala cílem elektronického útoku, vyjdou najevo i skutečnosti o nedostatečném zabezpečení jejích počítačových systémů, a to může přilákat jiné útočníky k provedení dalších útoků.

2.3 Pachatelé kyberkriminality zaměřené na útok typu odepření služby

Kybernetická kriminalita je úzce spjata s moderními technologiemi a způsobem jejich obsluhy. Tomu odpovídá i charakteristika uživatelů, kterými byli dříve převážně mladí lidé. Postupem času se ale užívání počítačů a dalších moderních technologií zjednodušuje, první

[58] McCLATCHY WASHINGTON BUREAU. *Hackers lurked undetected on networks now owned by Marriott for 4 years* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.mcclatchydc.com/news/policy/technology/cyber-security/article222437465.html.
[59] SVATOŠ, Roman, *op. cit.*, s. 55.

uživatelé osobních počítačů postupně stárnou, a tak počítače přestávají být dominantou mladých. Pokud se ale zaměříme na pachatele trestné činnosti v této oblasti, ti většinou potřebují detailnější porozumění daných technologií, a tak půjde spíše o uživatele mladšího až středního věku. Vzhledem k uvedené potřebě porozumění také půjde o spíše nadprůměrně inteligentní osoby.[60]

Z hlediska charakterových vlastností pachatelů internetové kriminality je významným faktorem také to, že v souvislosti s počítači se typicky nejedná o násilné trestné činy, které by směřovaly proti životu a zdraví. To uvádí i Josef Požár v publikaci z roku 2007.[61] S rozmachem technologií, ke kterému dochází i v oblasti zdravotnictví, se ale objevují i nová rizika, kdy si lze přímý počítačový útok proti životu nebo zdraví představit. V poslední době jsou diskutovány zranitelnosti kardiostimulátorů nebo inzulinových pump, kde lze špatné zabezpečení využít k bezkontaktnímu útoku na takové zařízení. Tím dojde k přímému útoku na zdraví osoby, která je postiženým zařízením vybavena.[62] Nicméně, v obecné rovině není násilnický typ charakterovým rysem pachatele kybernetické kriminality.

Vedle fyzických osob, jejichž trestní odpovědnost je tradiční, zavedl zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, v platném znění, i trestní odpovědnost právnických osob. Ta se vztahuje na všechny kybernetické trestné činy podle § 230 až 232 trestního zákoníku. Právnické osoby tak jsou za splnění zákonných podmínek za ně trestně odpovědné.

Zaměříme-li se specificky na pachatele útoku typu odepření služby, musíme se soustředit především na jejich motivaci. Řada útoků je páchána s pouhým cílem dokázat si, že útočník vůbec zvládne útok realizovat, a že tedy disponuje potřebnou znalostí a zkušeností potřebnou k provedení útoku. Jinou kategorií motivace je snaha získat provedením útoku prospěch. Motivace finančním nebo jiným prospěchem může spočívat buď v přímém prospěchu, např. formou vydírání při vyhrožování DoS útokem, nebo může jít o prospěch nepřímý. Např. DoS útok vedený na konkurenci ve svém důsledku způsobí přechod klientů k pachateli takového

[60] Ibid., s. 195.
[61] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Policejní akademie České republiky, 2007, s. 129.
[62] EURO. *Light (21. 8. 2018) – Hackování kardiostimulátorů může zabít pacienty. Výrobce to neřeší* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.euro.cz/light/hackovani-kardiostimulatoru-muze-zabit-pacienty-vyrobce-to-neresi-1417780#utm_medium=selfpromo&utm_source=euro&utm_campaign=copylink.

útoku. Útok typu odepření služby může být v neposlední řadě páchán také s cílem poškodit či sabotovat funkci počítačového systému při útoku vedeném státním aktérem proti jinému státu.

Motivem útoku typu odepření služby může být také snaha na sebe nebo na něco upozornit. Tak tomu bylo např. v případě útoků prováděných kyber hacktivistickým hnutím Anonymous. Cílem aktivit tohoto hnutí bylo upozornit na připravovanou mezinárodní dohodu ACTA[63] a protestovat proti jejímu přijetí. Aktivity tohoto hnutí, včetně provádění DoS útoků, byly zejména v roce 2012 zaznamenány v celé řadě států, včetně České republiky.[64]

Právě na útocích v rámci hacktivistického hnutí Anonymous se podíleli především mladí lidé, často ještě trestně neodpovědní, teenageři nebo osoby na hranici zletilosti.[65] To bylo dáno především výše uvedeným tématem, kterému toto hnutí věnovalo pozornost, a dále dostupností nástrojů pro snadné páchání útoků.[66]

2.4 Oběti kyberkriminality zaměřené na útok typu odepření služby

Útok typu odepření služby je svou povahou cílený elektronický útok, který je páchán se záměrem znepřístupnit určitá data či službu. Tomu musí odpovídat i charakteristika oběti takového činu.

Náhodná oběť přichází v úvahu pouze výjimečně. Můžeme ji uvažovat v případě, kdy se útočník připravuje na provedení cíleného útoku, např. s potřebou určitého načasování, a není si jist, zda způsob provedení útoku vyvolá požadovaný efekt. Proto se může uchýlit k otestování útoku na náhodně vytipované oběti. Aby mělo prověření smysl, útok by pachatel i v případě testu měl cílit na systém svou povahou podobný skutečnému cíli útoku. K zasažení náhodné oběti může dojít také při páchání distribuovaného odraženého DDoS útoku,[67] kdy se útok může nepříznivě projevit i na jednom ze serverů nedobrovolně do útoku zapojených.

---

[63] Anti-Counterfeiting Trade Agreement, Obchodní dohoda proti padělání.
[64] RYLICH, Jan. SOPA, PIPA & ACTA aneb Boj o svobodu na Internetu. *Ikaros* [online]. 2012, roč. 16, č. 2 [cit. 1. 3. 2019]. Dostupné z: https://ikaros.cz/sopa-pipa-acta-aneb-boj-o-svobodu-na-internetu. ISSN 1212-5075.
[65] iROZHLAS.cz. *Svět (8. 9. 2012) – Maďarská policie zatkla 16letého šéfa skupiny hackerů hlásících se k Anonymous* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/madarska-policie-zatkla-16leteho-sefa-skupiny-hackeru-hlasicich-se-k-anonymous_201209081408_kbrezovska.
BUSINESSWORLD.CZ. *Novinky (3. 2. 2013) – Nezletilý hacker z Anonymous nemusí do vězení* [online]. [cit. 1. 3. 2019]. Dostupné z: https://businessworld.cz/novinky/nezletily-hacker-z-anonymous-nemusi-do-vezeni-10415.
[66] K tomu blíže viz část 1, kapitola 1.3, bod 1.3.2 Distribuovaný DoS – DDoS.
[67] Viz část 1, kapitola 1.3, bod 1.3.3 Distribuovaný odražený DoS (DRDoS).

V naprosté většině případů však (D)DoS útok bude veden proti konkrétní útočníkem vytipované oběti. Typickou obětí může být stát, či spíše nějaký konkrétní úřad státní, resp. veřejné správy. (D)DoS útoky proti státním úřadům jsou páchány zejména jako jakási forma demonstrace, určitého společenského protestu, jehož cílem je upozornit na určitý jev či nějakou záležitost. S tím jsme se setkali např. při protestech hnutí Anonymous v rámci protestů proti dohodě ACTA v roce 2012.[68] Cílem útoků byly v rámci těchto protestů webové stránky Úřadu vlády ČR, Evropského parlamentu a Ochranného svazu autorského.[69]

V případě, že je obětí stát, nemusí jít ale jen o společenský protest. Může se jednat také o útok vedený jiným státem, resp. státním aktérem. V této souvislosti je nejdiskutovanějším příkladem série DDoS útoků, které se odehrály v roce 2007 v Estonsku. Tamní úřady v roce 2007 tvrdily, že počítačoví hackeři, kteří měli vazbu na ruskou vládu, vedli DDoS útoky proti estonským bankám a vládním agenturám. Tyto kybernetické útoky byly údajně ruskou odpovědí na estonské rozhodnutí přesunout sovětský památník druhé světové války z centra Tallinnu, což vedlo k protestům ruské vlády a etnických Rusů v Estonsku. Ruská vláda však zapojení svého státu do útoku popřela.[70]

Velké množství (D)DoS útoků je vedeno s motivací v podobě získání finančního prospěchu. V takovém případě je obětí typicky poskytovatel konkurenčních služeb. Podle informací Asociace pro elektronickou komerci obraty za prodej zboží on-line dosáhly v ČR v roce 2018 na 135 miliard korun, z toho 45 miliard za celé předvánoční období.[71]

(D)DoS útok vedený v předvánočním období proti konkurenčnímu e-shopu, který způsobí jeho výpadek, logicky povede k přesunu zákazníků k jiným potenciálním dodavatelům, a tedy i k iniciátorovi takového útoku. Z výše uvedených čísel vyplývá, že finanční motivace k provedení

---

[68] Podrobněji viz část 1, kapitola 1.3, bod 1.3.2 Distribuovaný DoS – DDoS.

[69] iDNES.CZ. *Technet (26. 1. 2012) – Anonymous napadli servery OSA, web české vlády i Evropského parlamentu* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.idnes.cz/technet/internet/anonymous-napadli-servery-osa-web-ceske-vlady-i-evropskeho-parlamentu.A120126_134112_sw_internet_nyv.

[70] ACAMSTODAY.ORG. *Cybersecurity: Nation-State Actors, Encrypted Cybercrimes and Man-in-the-Middle Attacks* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.acamstoday.org/nation-state-actors-encrypted-cybercrimes-man-in-the-middle-attacks.

[71] ASOCIACE PRO ELEKTRONICKOU KOMERCI. *Tisková zpráva (6. 1. 2019) – Česká e-commerce překonala očekávání, obraty za prodej zboží on-line dosáhly v roce 2018 na 135 miliard korun* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.apek.cz/clanky/ceska-e-commerce-prekonala-ocekavani-obraty-za-pr.
ASOCIACE PRO ELEKTRONICKOU KOMERCI. *Tisková zpráva (27. 12. 2018) – E-shopy mají za sebou další rekordní Vánoce, nyní startují výprodeje!* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.apek.cz/clanky/e-shopy-maji-za-sebou-dalsi-rekordni-vanoce-nyni.

takového útoku může být poměrně silná. Zvláště v oblastech, kde je dodavatelů daného typu zboží poměrně málo, nebo působí v daném segmentu trhu např. pouze dva, tři významní dodavatelé. Tam lze případný přesun zákazníků poměrně snadno predikovat či útočníkem naplánovat. To, že k takovým útokům reálně dochází, můžeme doložit na případu z roku 2011, kdy právě v předvánočním období došlo k řadě DDoS útoků na elektronické obchody. Útok byl veden ze zahraničí a zaměřoval se na určitou platformu elektronického obchodu, byl tedy cílen na provozovatele systému celé řady e-shopů. Při útoku bylo postiženo zhruba 9 000 domén. Vzhledem k načasování a rozsahu útoku je velmi pravděpodobné, že útoky byly provedeny v rámci konkurenčního boje. V té době však tržby e-shopů v předvánočním období byly třikrát menší, než v roce 2018.[72]

Podobná situace může nastat i u poskytovatelů služeb spojených s elektronickou komercí – dopravců balíkové přepravy. Sérii DDoS útoků čelila v prosinci 2010 také Česká pošta, resp. její systém pro on-line hromadné podání, který využívají zejména provozovatelé e-shopů. Vzhledem k potřebě dodat zboží řádně a včas to samozřejmě řadu e-shopů vedlo ke změně spediční společnosti a balíky v předvánočním období během trvání útoku odeslaly prostřednictvím jiného, konkurenčního, dopravce.[73]

2.5 Modus operandi

V případě cíleného elektronického útoku, ať už je jeho účelem na sebe nebo na něco upozornit, někoho nebo něco poškodit, nebo je účelem získání finančního nebo jiného prospěchu, mívá toto jednání určitý typizovaný průběh, který se skládá z určitých kroků či fází. Tyto fáze jsou uvedeny v tabulce č. 2 a jsou dále podrobněji rozebrány.[74]

[72] LUPA.CZ. *Články (16. 12. 2011) – Tisíce tuzemských e-shopů mělo výpadky, může za to masivní DDoS útok* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.lupa.cz/clanky/tisice-tuzemskych-e-shopu-melo-vypadky-muze-za-to-masivni-ddos-utok.
[73] LIDOVKY.CZ. *Byznys (9. 12. 2010) – Česká pošta čelí útoku hackerů. V ohrožení jsou balíky s vánočními dárky* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.lidovky.cz/byznys/firmy-a-trhy/ceska-posta-celi-utoku-hackeru-v-ohrozeni-jsou-baliky-s-vanocnimi-darky.A101209_191040_firmy-trhy_sm.
[74] WILSON, Clay. Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. *Washington Congressional Research Service* [online]. 2003. [cit. 1. 3. 2019]. Dostupné z: http://www.fas.org/irp/crs/RL32114.pdf.

Fáze	Význam pro (D)DoS útok
Analýza situace (průzkum terénu) ↓	značný
Skenování ↓	omezený
Získání přístupu ↓	žádný
Udržení přístupu ↓	žádný
Zamazání stop	omezený

Tab. č. 2: Fáze elektronického útoku

Analýza situace (průzkum terénu)

V první fázi útoku dochází k získávání maxima informací o předmětu či cíli útoku, tedy o oběti tohoto útoku, o způsobu fungování předmětného počítačového systému, vnitřní struktuře počítačové sítě, o použitých bezpečnostních opatřeních. Tyto informace je možné využít při následném skenování a hledání konkrétních zranitelností využitelných pro provedení útoku. Při tom může útočník využívat různé techniky sociálního inženýrství, jejichž cílem je podvodně vylákat relevantní informace. V případě počítačového systému, který je provozován veřejnoprávním subjektem, může útočník k získání informací využít i dotazu položeném na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění. Může také využít různých specifických programů, které mu se sběrem informací pomohou.[75]

Tuto analýzu většinou provádí útočník i v případě plánování (D)DoS útoku, zejména s ohledem na zjištění výkonnosti serverů a kapacity internetového připojení. Tak, aby mohl stanovit architekturu útočící sítě, potřebný výpočetní výkon a kapacitu internetového připojení na straně útočníka. V případě jednoduchých a méně promyšlených (D)DoS útoků je někdy tato fáze omezena na minimum.

[75] Např. různé spyware nástroje, které z počítače získávají důležité informace bez vědomí uživatele.

Skenování

Ve druhé fázi útočník již disponuje potřebnými vstupními informacemi a nyní hledá a zkoumá jednotlivé možnosti a místa, kterými je možné do cílového systému proniknout. V této fázi také zjišťuje, jaké konkrétní verze programového vybavení jsou v systému využity. K tomu může využít např. techniky skenování portů,[76] nebo různé veřejně dostupné nástroje a databáze, které k podobnému účelu slouží.[77]

Na základě výsledků skenování a provedené předchozí analýzy je možné přistoupit k plánování způsobu provedení útoku, dohledání zranitelností vyplývajících z použitých verzí jednotlivých zapojených systémů, způsobu jejich propojení a konfigurace.

Pokud se budeme zabývat konkrétně (D)DoS útoky, bude tato fáze poměrně omezená. Pro tento typ útoku je potřeba znát zejména adresu cílového systému, případné použité bezpečnostní prvky, výkonnost serverů cílového systému a kapacity jeho internetového připojení. Tato data útočník často získá už provedením analýzy.

Získání přístupu

Po provedení dvojice předchozích fází má útočník již dostatek informací k provedení vlastního útoku, který typicky spočívá v průniku do systému. Útočník na základě získaných informací identifikuje slabé místo a pomocí vhodné metody jej využije. Těchto metod je celá řada. Řadíme mezi ně metodu prolomení přístupového hesla, SQL injection, cross-site scripting, útok man-in-the-middle, přetečení zásobníku a mnohé další metody.[78] Vzhledem k zaměření této práce je však nebudeme podrobněji rozebírat.

U (D)DoS útoku není potřeba do systému proniknout. Specifickou vlastností tohoto typu útoku je to, že při jeho prosté realizaci nedochází k překonání překážek a získání plného přístupu k počítačovému systému. Útok ve své podstatě generuje velké množství (jinak legitimních) požadavků, které vedou k vyčerpání systémových zdrojů a následné nedostupnosti systému.

[76] Technika spočívá v ověření připravenosti komunikace zájmového systému na jednotlivých komunikačních portech IP protokolu, z čehož je možné usoudit, jaké všechny služby tento systém poskytuje nebo využívá.
[77] Např. nástroje shodan.iq nebo censys.io, které shromažďují a poskytují informace o IP adresách a na nich běžících službách.
[78] Více viz např. ENDORF, Carl, SCHULTZ, Eugene, MELLANDER, Jim. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, 355 s.

K tomu může dojít řadou způsobů, které jsou podrobně rozebrány v kapitole 1.3 Jednotlivé typy DoS útoků a související techniky.

Udržení přístupu

Poté, co útočník získá nelegitimní přístup k cílovému systému, snaží se vytvořit možnost, aby si tento přístup udržel a k napadenému systému mohl opakovaně přistoupit bez potřeby opakovat postup původně vedoucí k získání takového přístupu. Důvodem k budování této možnosti může být, že k získání přístupu mohl vést neopakovatelný nebo komplikovaný postup, anebo fakt, že původní při útoku využitá zranitelnost může být ze strany provozovatele systému opravena a stejnou cestou už nemusí být získání přístupu možné. K udržení přístupu se využívají typicky metody zavedení tzv. zadních vrátek (backdoor) nebo se využívá různých rootkitů.[79]

Vzhledem k tomu, že u (D)DoS útoků nedochází k získání nelegitimního přístupu, techniky pro udržení přístupu nepřichází v úvahu. Nebudeme je proto v této práci podrobněji rozebírat.

Zamazání stop

V poslední fázi útoku dochází ze strany útočníka k utajení jeho působení v systému, odstranění nebo zahlazení stop, které postupem útoku zanechal. Pokud nejde o demonstrativní útok, je cílem útočníka přístup si ponechat a zajistit, aby detekce realizovaného útoku byla co nejtěžší, nejlépe nemožná. Maže proto po sobě veškeré stopy, které je možné nalézt v provozních záznamech napadeného systému, pozměněné konfiguraci, historii uživatelských účtů, datech modifikace souborů atp.

V případě (D)DoS útoků je opět tato fáze značně omezena. V rámci této fáze může ze strany pachatele tohoto typu útoku jít nanejvýš o ovlivnění zanechaných stop takovým způsobem, aby byla identifikace útočníka maximálně ztížena. Můžeme proto uvažovat o využití anonymizačních nástrojů nebo techniky podvržení IP adresy, k tomu podrobněji viz bod 1.3.6 Podvržení IP adresy (IP Spoofing).

[79] Více viz např. ibid.

2.6 Prevence

V obecné rovině lze ochranu před kybernetickými útoky chápat ve dvou základních rovinách. V první rovině jde o co nejmenší dostupnost informací o provozovaném počítačovém systému. Je nevhodné zveřejňovat informace o používaném programovém vybavení, jeho verzích, konfiguraci, schématech propojení jednotlivých prvků atp. To vše jsou informace, které útočník může využít pro páchání útoku. Týká se to jak potřeby nezveřejňovat je aktivně, ve smyslu např. jejich publikace v rámci webové prezentace nebo popisu veřejné zakázky, tak i pasivně, ve smyslu odpovídání na dotazy ať už ze strany veřejnosti, novinářů či dodavatelů komponent systému. To se týká i možnosti získat informace na základě dotazu podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, uvedené v kapitole 2.5 Modus operandi. Tento zákon umožňuje ve stanovených případech požadované informace neposkytnout.

Obecně je vždy třeba vzít v úvahu, zda daná žádající osoba či instituce informace skutečně potřebuje, a ještě více je třeba vážit, zda ten, kdo se na informace ptá, je skutečně tím, za koho se vydává. Neboť právě techniky sociálního inženýrství a klamu útočníci často k získání potřebných informací využívají.

Druhá rovina prevence spočívá ve správném zabezpečení provozovaného počítačového systému. To má celou řadu komponent. Tou základní je používání verzí programového i technického vybavení, které má zajištěnu podporu výrobce[80] a má instalovány dostupné bezpečnostní aktualizace. Důležitá je také správná konfigurace takového systému provedená s ohledem na bezpečnost a maximální omezení přístupu pouze na skutečně potřebný rozsah. Veškerá přístupová hesla musí být volena jako komplexní a bezpečná.[81] V neposlední řadě je potřeba používat bezpečnostní programy a zařízení, jako jsou antivirové programy nebo komplexnější anti-malware řešení, firewally, VPN řešení pro vzdálený přístup a různé detekční a záznamové nástroje pro možné upozornění na probíhající útok a pro jeho následnou analýzu.

[80] Podpora spočívá v dostupnosti bezpečnostních i funkčních aktualizací, náhradních dílů, schopnosti řešit problémy uživatelů atp.

[81] Komplexní heslo se skládá z velkých a malých písmen, čísel a speciálních znaků (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/). Bezpečné heslo je komplexní s dostatečnou délkou, která je odvislá od dostupného výpočetního výkonu a bezpečnostních nastavení daného systému.

V oblasti prevence proti (D)DoS útokům se uplatní některé specifické postupy a nástroje. V každém případě je vhodným opatřením naddimenzování kapacity internetového připojení a výpočetního výkonu chráněných serverů. Jak vyplývá z charakteristiky (D)DoS útoků uvedené v technické části, obecná ochrana před nimi není snadná. Proti některým formám útoku existuje opatření, které je vůči danému způsobu provedení útoku účinné a následku v podobě nedostupnosti systému zabrání. Některá z těchto opatření jsou uvedena přímo u jednotlivých typů a technik útoku v kapitole 1.3 Jednotlivé typy DoS útoků a související techniky. Další možné techniky, jak útok zmírnit, jsou uvedeny v tabulce č. 1 v kapitole 1.1 Charakteristika útoku typu odepření služby. Možnou ochranu představuje i provoz sítě v ostrovním režimu.[82]

V obecné rovině je jednou z technik využívaných při obraně proti útokům typu (D)DoS, které přichází zejména z cizích sítí, technika známá jako Remotely-Triggered Black Hole filtering (RTBH filtrování). Tato technika umožňuje zahazovat nežádoucí provoz dříve, než dorazí do cílové sítě a zahltí komunikační linku oběti. Využívá k tomu možností směrovacích protokolů, pomocí kterých komunikují internetové směrovače, když se dohadují na možných cestách, kudy daný datový tok prostřednictvím internetu směrovat.[83]

Další možnou zvláštní technikou je využití specializovaného zařízení, které slouží k ochraně před DDoS útoky. Jedná se svým způsobem o jakousi pračku datového toku, která např. na základě metod umělé inteligence dokáže rozpoznat závadový datový tok od toku legitimního. Závadový datový tok je v této pračce zahozen a směrem k cíli dorazí pouze datový tok legitimní.[84] Zařízení tohoto typu jsou poměrné nová, zda dokážou problém v podobě DDoS útoku účinně řešit ukáže až čas. Těmito zařízeními disponují spíše poskytovatelé internetového připojení než jejich běžní zákazníci. Podobná zařízení pro ochranu svou a svých zákazníků užívají také velcí poskytovatelé datového obsahu a cloudových služeb. Nasazení zařízení nabízí někteří poskytovatelé internetu svým zákazníkům jako zpoplatněnou službu.[85]

---

[82] K ostrovnímu režimu viz projekt FENIX v kapitole 1.1 Charakteristika útoku typu odepření služby.
[83] ROOT.CZ. *Bezpečnost (23. 2. 2015) – Konkrétní ukázka (D)DoS útoku z pohledu peeringového uzlu* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.root.cz/clanky/konkretni-ukazka-d-dos-utoku-z-pohledu-peeringoveho-uzlu.
[84] Jedná se např. o zařízení DDoS Protector™ výrobce Check Point, viz https://www.checkpoint.com/products/ddos-protector. [cit. 1. 3. 2019].
[85] Např. operátor T-mobile nabízí DDoS ochranu jako službu, viz http://www.gts.cz/sluzby/security/gts-ddos-ochrana. [cit. 1. 3. 2019].

Je vhodné poznamenat, že každý mechanismus určený pro ochranu před útoky typu odepření služby je potřeba správně nastavit, zejména se zohledněním běžného provozu, který je specifický pro každou konkrétní službu. Příliš restriktivně nastavená pravidla ochrany mohou vést k odmítnutí požadavků pocházejících z legitimního provozu a ve svém důsledku tak mohou způsobit stejný problém, kterého chce dosáhnout útočník, tedy nedostupnost služby.

3 Právní část

3.1 Definice kyberkriminality

Jednotná definice kybernetické kriminality nebo kybernetického zločinu neexistuje. Dříve, než se ustálil termín *„kybernetická kriminalita“,* nebo zkráceně *„kyberkriminalita“*, se pro trestnou činnost páchanou pomocí počítačové techniky užíval spíše pojem *„počítačová kriminalita“*. V publikaci Vladimíra Smejkala z roku 1995 můžeme nalézt definici počítačové kriminality jako *„různorodou směsici trestných činů, jejichž společným faktorem je počítač, program a data.“*[86]

Pro trestnou činnost páchanou prostřednictvím informačních a komunikačních technologií se v mezinárodním právu používá pojem *„cyber crime“*, tedy v překladu *„kybernetická kriminalita“*. Charakter tohoto pojmu přirovnává Vladimír Smejkal následovně: *„násilná kriminalita, kriminalita mladistvých, ekonomická kriminalita apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).“*[87]

Tomáš Gřivna a Radim Polčák uvádějí kumulativní definici kyberzločinu jako: *„a) trestný čin ohrožující ICT – informační a síťovou bezpečnost (trestný čin proti počítačové integritě nebo také trestný čin v úzkém pojetí), b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se k počítačům) a c) trestný čin vztahující se k obsahu, jako např. dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se k obsahu počítačových dat).“*[88]

Setkáme se i s definicí, kterou používá Policie ČR: *„Kybernetická kriminalita, dříve také označována jako informační kriminalita, je definována v Policii ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí.*

[86] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. 1. vydání. Praha: C. H. Beck/SEVT, 1995, s. 99.
[87] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vydání. Plzeň: Aleš Čeněk, 2015, s. 19.
[88] GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. 1. vydání. Praha: Auditorium, 2008, s. 35.

Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.“[89]

Určitou představu o rozsahu tohoto pojmu můžeme získat i z kategorizace kybernetické trestné činnosti uvedené v Úmluvě o počítačové kriminalitě, viz následující kapitola 3.2 Vývoj trestního práva postihujícího kybernetickou kriminalitu.

Z uvedeného vyplývá, že je vhodné rozlišovat kyberkriminalitu v užším smyslu, jako trestnou činnost, kde předmětem útoku jsou informační a komunikační technologie a obecně data v nich uložená nebo jimi zpracovávaná. Tomuto užšímu pojetí odpovídá označení trestných činů uvedených v § 230 až § 232 zvláštní části trestního zákoníku, jako počítačových nebo kybernetických trestných činů. V širším pojetí pak kyberkriminalita pokrývá také trestné činy vztahující se k obsahu, zejména se jedná o dětskou pornografii a právo duševního vlastnictví. Širší pojetí pokrývá také trestné činy využívající informační a komunikační technologie ke spáchání tradičních trestných činů.

Vzhledem k tématu této práce je pro následující právní rozbor stěžejní zabývat se kyberkriminalitou v užším pojetí, neboť do tohoto pojetí se vejde jednání spočívající v páchání kybernetických útoků v podobě DoS útoku.

3.2 Vývoj trestního práva postihujícího kybernetickou kriminalitu

Informační a komunikační technologie jsou jednou z oblastí, která se velmi rychle vyvíjí, rozvíjí, a navíc zasahuje do stále většího množství lidských činností. Právo, zejména to trestní, však reguluje lidskou činnost ex post. Tedy, nejprve se něco stane, co společnost označí za nežádoucí chování, to se popíše a právní normou zakáže. K tomu, aby určité chování související s počítači či kybernetickým prostorem bylo trestně postižitelné, musí být nejprve popsáno jako trestný čin (zásada zákonnosti, nullum crimen sine lege). Rychlý vývoj v oblasti informačních a komunikačních technologií tak logicky může vést ke stavu, kdy ne každé závadové chování bude trestně postižitelné. Nepomůže nám ani institut právní analogie, která je k tíži pachatele

[89] POLICIE ČR. *Kyberkriminalita* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

v trestním právu hmotném zásadně nepřípustná. Z tohoto důvodu je vhodné skutkové podstaty trestné činnosti související s počítači formulovat spíše obecněji. Formulace však nesmí být příliš vágní a neurčité, neboť by tím také došlo k porušení zásady zákonnosti.[90]

To se týká zejména nových typů útoků, které rozvoj technologií přinesl, a které nemají obdobu v tradičním světě. Vedle toho lze řadu útoků a závadových činností realizovaných za pomoci počítačové techniky nebo proti ní subsumovat pod zákonné ustanovení skutkové podstaty tradičních trestných činů. Např. podvod realizovaný prostřednictvím počítačové techniky je pořád podvodem. Tato technika slouží pouze jako nástroj či prostředek, pomocí kterého byl spáchán.

Díky obrovskému rozmachu internetu, jako světově největší počítačové sítě, a skutečnosti, že většina kybernetických útoků je páchána právě v prostředí internetu, je u kybernetické kriminality často přítomen mezinárodní prvek. Z toho důvodu je potřebné, aby státy, které s kyberkriminalitou chtějí účinně bojovat, přijaly obdobnou trestně právní úpravu, nebo aby byl dodržován alespoň společný minimální standard. To se týká nejen oblasti hmotného práva, ale také práva procesního, neboť při vyšetřování trestných činů v podobě kybernetických útoků je často nezbytná mezinárodní policejní i justiční spolupráce.

Na mezinárodní úrovni je v souvislosti s kybernetickou kriminalitou považován za první významný dokument *„Manuál OSN o prevenci a kontrole trestných činů spojených s počítači“,*[91] který vznikl na základě Osmého Kongresu OSN o prevenci kriminality a zacházení s pachateli, jenž se konal v roce 1990 v Havaně.[92] Na tomto kongresu byla vydána řada doporučení týkajících se adopce vyšetřovacích postupů, důkazních pravidel, mezinárodní spolupráce a dalších záležitostí ve vztahu ke kybernetické kriminalitě.[93]

V celosvětovém měřítku je pak klíčovým dokumentem úmluva Rady Evropy č. 185 - Úmluva o počítačové kriminalitě[94] a dodatkový protokol k ní.[95] Tato úmluva, v Česku

[90] Konkrétně zásady nullum crimen sine lege certa, která vyžaduje přesnou a určitou právní úpravu.
[91] ORGANIZACE SPOJENÝCH NÁRODŮ. *United Nations Manual on the prevention and control of computer-related crime* [online]. [cit. 1. 3. 2019]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf.
[92] Zápis z kongresu je dostupný na https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf.
[93] WESTBY, Jody R. *International Guide to Cyber Security*. USA: American Bar Association, 2004, s. 82.
[94] RADA EVROPY. *Úmluva o počítačové kriminalitě* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

označovaná spíše jako Úmluva o kyberkriminalitě[96] (dále jen *„Úmluva“*), si klade za cíl sjednotit národní právní úpravu v této oblasti. Úmluva byla otevřena k podpisu v listopadu 2001 v Budapešti, v platnost vstoupila dne 1. července 2004 po ratifikaci 5 státy. K 1. březnu 2019 ji ratifikovalo 62 států, včetně řady států, které nejsou členy Rady Evropy. Mezi státy mimo Radu Evropy, které Úmluvu ratifikovaly, patří např. Spojené státy americké, Kanada, Austrálie, Izrael nebo Japonsko. Další 4 státy ji pouze podepsaly, ale zatím neratifikovaly.[97] Česká republika podepsala tuto úmluvu již dne 9. února 2005. Ratifikovala ji ale až 22. srpna 2013 a v ČR vstoupila v platnost dne 1. prosince 2013.[98]

Úmluva obsahuje preambuli a 48 článků členěných do 4 kapitol:

- Užití pojmů
- Opatření, která mají být přijata na vnitrostátní úrovni
    - Sestává se z částí: trestní právo hmotné, procesní právo, soudní pravomoc
- Mezinárodní spolupráce
    - Sestává se z částí: obecné zásady, zvláštní ustanovení
- Závěrečná ustanovení

Z hlediska hmotněprávních norem Úmluva definuje 4 základní kategorie trestných činů:[99]

- Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů
- Trestné činy související s počítačem
- Trestné činy související s obsahem
- Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským

---

[95] RADA EVROPY. *Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

[96] To je přesnější překlad původního názvu úmluvy *„Convention on cybercrime“*, oficiální překlad uvedený ve Sbírce mezinárodních smluv je však *„Úmluva o počítačové kriminalitě“*.

[97] RADA EVROPY. *Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime*. Treaty Office [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[98] Sdělení č. 104/2013 Sb. m.s., *sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě*.

[99] Čl. 2 až 10 Úmluvy.

V rámci těchto čtyřech kategorií jsou pak uvedeny skutkové podstaty celkem devíti trestných činů týkajících se kybernetické kriminality. Úmluva tak svou kategorizací závadového jednání, které považuje za kyberkriminalitu, uvažuje výklad tohoto pojmu v jeho širším pojetí.[100]

Úmluva také obsahuje zakotvení některých obecných hmotněprávních institutů, jako je trestní odpovědnost za pokus a účastenství[101] a trestní odpovědnost právnických osob.[102] Úmluva neobsahuje konkrétní sankce, obsahuje pouze obecné vymezení:

„Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby trestné činy ustavené podle článků 2-11 bylo možno potrestat účinnými, přiměřenými a odrazujícími tresty, včetně trestu odnětí svobody.“[103]

Z hlediska procesněprávních norem Úmluva obsahuje ustanovení týkající se specifických technik a postupů souvisejících se zajišťováním dat a důkazů v oblasti kybernetické kriminality,[104] s ohledem na potřebu v těchto věcech jednat rychle, neboť prodlení může způsobit nenávratnou ztrátu dat, která mohou představovat důležité důkazy. Úmluva se věnuje také otázkám soudní pravomoci.[105]

V další kapitole jsou v Úmluvě řešeny otázky mezinárodní spolupráce týkající se vydávání osob a vzájemné pomoci. Ohledně okamžité vzájemné pomoci Úmluva dává za povinnost zřídit kontaktní místo s nepřetržitou službou.[106]

Dodatkový protokol Rady Evropy č. 189 k Úmluvě o počítačové kriminalitě byl otevřen k podpisu v lednu 2003 ve Štrasburku, v platnost vstoupil dne 1. března 2006 po ratifikaci 5 státy a k 1. březnu 2019 jej ratifikovalo 31 států. Dalších 13 států jej pouze podepsalo, ale zatím neratifikovalo.[107] Česká republika jej podepsala dne 17. května 2013, ratifikovala dne 7. srpna

[100] K výkladu pojmu kyberkriminalita viz kapitola 3.1 Definice kyberkriminality.
[101] Čl. 11 Úmluvy.
[102] Čl. 12 Úmluvy.
[103] Čl. 13 odst. 1 Úmluvy.
[104] Čl. 16 až 21 Úmluvy.
[105] Čl. 22 Úmluvy.
[106] Čl. 35 Úmluvy.
[107] RADA EVROPY. *Chart of signatures and ratifications of Treaty 189 - Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Treaty Office [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures.

2014 a v ČR vstoupil v platnost dne 1. prosince 2014,[108] tedy přesně 1 rok poté, co v platnost v ČR vstoupila Úmluva.

Dodatkový protokol se zabývá kriminalizací činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Rozšiřuje tak okruh činů spočívajících v šíření závadného obsahu, který byl v Úmluvě omezen na dětskou pornografii. Důvodem, proč se i tyto činy nestaly přímou součástí Úmluvy, bylo zejména podepsání a následná ratifikace Úmluvy ze strany USA, kde vlivem širšího pojetí svobod nemusí být projevy rasismu a xenofobie trestným činem.[109] Vzhledem k zaměření této práce není potřeba se Dodatkovému protokolu podrobněji věnovat.

I na poli práva Evropské unie dochází ke snahám právní úpravu týkající se kybernetické kriminality co možná nejvíce sblížit. To se děje za pomoci standardních legislativních aktů evropského práva, jako jsou rámcová rozhodnutí, směrnice a nařízení.

Z pohledu trestního práva lze za stěžejní označit zejména Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům ze dne 24. února 2005[110] (dále jen *„Rámcové rozhodnutí“*), a navazující Směrnici Evropského parlamentu a Rady 2013/40/EU, o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV ze dne 12. srpna 2013[111] (dále jen *„Směrnice“*).

Rámcové rozhodnutí obsahuje mimo jiné vymezení tří skutkových podstat trestných činů: protiprávní přístup k informačním systémům, protiprávní zásah do systému a protiprávní zásah do dat. Součástí tohoto dokumentu je i stanovení minimálních sankcí u trestných činů protiprávního zásahu do systému a protiprávního zásahu do dat, a to tak, že se na ně má vztahovat trest odnětí svobody s horní hranicí trestní sazby nejméně 1 až 3 roky.[112] Pokud ke spáchání všech tří činů, vyjma protiprávního přístupu k informačním systémům bez překonání

[108] Sdělení č. 9/2015 Sb. m.s., *sdělení Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů*.
[109] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, s. 334.
[110] Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 *o útocích proti informačním systémům* [online]. [cit. 1. 3. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32005F0222.
[111] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 *o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV* [online]. [cit. 1. 3. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32013L0040.
[112] Čl. 6 Rámcového rozhodnutí.

bezpečnostního opatření, dojde v rámci zločinného spolčení, má se na ně vztahovat trest odnětí svobody s horní hranicí trestní sazby nejméně 2 až 5 let.[113] Rámcové rozhodnutí také obsahuje zakotvení obecných hmotněprávních institutů, jako je trestní odpovědnost za pokus a účastenství[114] a trestní odpovědnost právnických osob.[115] Jelikož na poli informačních a komunikačních technologií došlo k dalšímu vývoji, bylo Rámcové rozhodnutí nahrazeno výše uvedenou Směrnicí, která je komplexnější a podrobnější.

Směrnice v úvodní části obsahuje definici základních pojmů, kde definuje zejména *„informační systémem“* jako *„jakýkoli přístroj nebo skupinu vzájemně propojených nebo přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových údajů, jakož i počítačové údaje uložené, zpracované, opětovně vyhledané nebo přenesené tímto přístrojem či skupinou přístrojů za účelem jeho či jejich provozu, použití, ochrany a údržby“*[116] a pojem *„neoprávněný“* jako *„jednání uvedené v této směrnici včetně přístupu, zásahu nebo sledování, které není povoleno majitelem či jiným držitelem práv k systému nebo k jeho části nebo které není povoleno vnitrostátním právem.*“[117]

Zejména druhá definice je významná pro beztrestnost provádění tzv. penetračních testů, jejichž účelem je prověření zabezpečení informačních systémů, a jsou prováděny se souhlasem provozovatele systému. Směrnice pak obsahuje zejména vymezení pěti skutkových podstat trestných činů, které na jejím základě musí být včleněny do národních legislativ členských států: neoprávněný přístup k informačním systémům, neoprávněné zasahování do informačních systémů, neoprávněné zasahování do údajů, neoprávněné sledování údajů a vedle toho také trestnost související s určitými formami nakládání s nástroji použitými k páchání trestných činů v podobě počítačového programu, který byl vytvořen nebo přizpůsoben prvotně pro účely spáchání některého ze čtyř uvedených trestných činů, nebo počítačového hesla, přístupového kódu nebo obdobných údajů, které umožňují přístup k celému informačnímu systému nebo k jeho části.[118] Směrnice se rovněž podrobněji zabývá sankcemi. Horní hranice trestu odnětí svobody má být u všech pěti trestných činů nejméně dva roky. U trestných činů neoprávněné zasahování

[113] Čl. 7 Rámcového rozhodnutí.
[114] Čl. 5 Rámcového rozhodnutí.
[115] Čl. 8 Rámcového rozhodnutí.
[116] Čl. 2 a) Směrnice.
[117] Čl. 2 d) Směrnice.
[118] Podrobněji viz Čl. 7 Směrnice.

do informačních systémů a neoprávněné zasahování do údajů má pak být tato hranice při spáchání trestného činu za kvalifikovaných okolností nejméně tři roky, resp. pět let při naplnění závažnějších okolností.[119] Směrnice vyžaduje také trestní stíhatelnost účastenství u všech uvedených činů a pokusu u činů neoprávněné zasahování do informačních systémů a neoprávněné zasahování do údajů.[120] Směrnicí je rovněž vyžadována trestní odpovědnost právnických osob u všech uvedených činů.[121] Po procesní stránce se směrnice věnuje také soudní příslušnosti a výměně informací, kde za tímto účelem dává členským státům za povinnost provozovat národní kontaktní místo s nepřetržitým provozem.[122]

3.3 Vnitrostátní právní úprava

Pokud se zaměříme na zavádění hmotněprávních ustanovení týkajících se kybernetické kriminality do českého právního řádu, neměli bychom vynechat zákon č. 557/1991 Sb., který do tehdy platného trestního zákoníku zavedl jako § 257a novou skutkovou podstatu trestného činu *„poškození a zneužití záznamu na nosiči informací“*. Tato skutková podstata pokrývala i související zásah do technického nebo programového vybavení počítače.[123]

Zásadní změnu v oblasti hmotného trestního práva, nejen ve vztahu ke kybernetické trestné činnosti, ale obecně, pak přinesl zákon č. 40/2009 Sb. – nový trestní zákoník účinný od 1. ledna 2010. Ten ve svých paragrafech 230 až 232 zavedl tři nové skutkové podstaty trestných činů: neoprávněný přístup k počítačovému systému a nosiči informací (§ 230), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232). První dvě skutkové podstaty byly do trestního zákoníku zapracovány na základě Úmluvy o počítačové kriminalitě. Poslední, nedbalostní skutková

[119] Podrobněji viz Čl. 9 Směrnice.
[120] Čl. 8 Směrnice.
[121] Čl. 10 Směrnice.
[122] V ČR zajišťuje národní kontaktní bod pro kybernetickou kriminalitu Sekce kybernetické kriminality Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování.
[123] Podrobněji viz článek I, bod 50. již zrušeného zákona č. 557/1991 Sb.

podstata byla do trestního zákoníku zařazena nad rámec závazků z této Úmluvy, a to na základě požadavků z praxe.[124]

Tyto trestné činy jsou ve zvláštní části trestního zákoníku systematicky řazeny v hlavě V – trestné činy proti majetku. Tvoří určitou podskupinu, někdy nazývanou jako počítačové nebo kybernetické trestné činy. Jejich specifičnost spočívá v tom, že *„od ostatních trestných činů proti majetku, jejichž druhovým objektem jsou majetkové zájmy různorodé povahy, se odlišují právě svým primárním objektem, kterým je společenský, parciální či individuální zájem na důvěrnosti, integritě a dostupnosti počítačových systémů, sítí a počítačových dat, jakož i zájem na zamezení zneužití takových systémů, sítí a dat k páchání trestné činnosti různorodé povahy.“*[125]

Tuto trojici trestných činů můžeme chápat jako kybernetické trestné činy v užším smyslu. V širším smyslu pod kybernetickou kriminalitu řadíme i celou řadu dalších trestných činů, zejména souvisejících s obsahem, např. porušování práv duševního vlastnictví, a také činy využívající informační a komunikační technologie ke spáchání tradičních trestných činů, např. podvod. Záběr tohoto širšího výkladu je dán tím, že kybernetický prostor je specifický prostor, kde se odehrává také celá řada aktivit, které známe z reálného prostředí. Postihování těchto aktivit odehrávajících se v kyberprostoru pomocí klasických trestných činů je žádoucí, neboť vytvářet kazuisticky nové a nové skutkové podstaty trestných činů odrážející vývoj společnosti a technologií není vhodné a nepřispívá přehlednosti už tak rozsáhlého českého právního řádu. Tyto další trestné činy, které můžeme zahrnout pod širší význam pojmu kybernetické trestné činy, se zaměřením této práce souvisí okrajově, a proto v ní nejsou podrobněji rozebrány.[126]

Ustanovení § 230 a § 231 trestního zákoníku byla v roce 2015 novelizována zákonem č. 165/2015 Sb. Novelizace byla provedena v souvislosti s implementací Směrnice Evropského parlamentu a Rady 2013/40/EU, o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.[127] Důvodová zpráva k tomuto zákonu uvádí: *„Česká republika*

[124] Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník. Sněmovní tisk 410/0, část č. 1/9 Vl.n.z. trestní zákoník – EU [online]. [cit. 1. 3. 2019]. Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=410&ct1=0.
[125] DRAŠTÍK, Antonín, FREMR, Robert, DURDÍK, Tomáš, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander aj. *Trestní zákoník: Komentář* [Systém ASPI]. Wolters Kluwer [cit. 1. 3. 2019]. ASPI_ID KO40_2009CZ. Dostupné v Systému ASPI.
[126] K tomu podrobněji viz kapitola 3.1 Definice kyberkriminality.
[127] K této směrnici více viz kapitola 3.2 Vývoj trestního práva postihujícího kybernetickou kriminalitu.

v současné době naplňuje všechny požadavky směrnice o útocích na informační systémy, pokud jde o skutkové podstaty trestných činů. Směrnice žádá, aby členské státy stanovily sankce za útoky na informační systémy. Tyto sankce by měly být účinné, přiměřené a odrazující a jejich součástí by měl být trest odnětí svobody nebo peněžitý trest. Směrnice o útocích na informační systémy stanoví trestní sankce alespoň pro případy, které se nepovažují za méně závažné.“[128] Novelizací tak byly zvýšeny některé horní hranice trestní sazby u trestných činů uvedených v § 230 a § 231 trestního zákoníku. Zvýšení však bylo provedeno nejvýše o jeden rok a úprava je tak spíše pouze kosmetická.

Příprava k trestným činům uvedeným v § 230 až § 232 trestního zákoníku je s ohledem na úpravu trestnosti tohoto vývojového stádia trestné činnosti vyloučena, neboť se ani v jednom případě nejedná o zvlášť závažný zločin.[129]

3.3.1 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230)

Ustanovení § 230 trestního zákoníku obsahuje celkem 5 odstavců. V odstavcích 1 a 2 jsou vymezeny znaky dvou základních skutkových podstat tohoto úmyslného trestného činu.

Odst. 1 zní:

„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“

Individuálním objektem trestného činu vymezeného v odst. 1 je ochrana důvěrnosti počítačových dat, počítačového systému a jeho částí. Trestným je samo o sobě získání neoprávněného přístupu, ke kterému dojde po překonání bezpečnostního opatření. Není současně vyžadován jiný nečestný úmysl pachatele, např. v podobě získání počítačových dat nebo způsobení škody.[130] K tomu můžeme citovat z usnesení Nejvyššího soudu ČR sp. zn. 7 Tdo 1469/2017: *„Ve skutkové podstatě tohoto přečinu tedy není obsažena podmínka, že by obviněný*

[128] Důvodová zpráva k zákonu č. 165/2015 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. Sněmovní tisk 358/0, část č. 1/6 Novela z. - trestní zákoník – EU [online]. [cit. 1. 3. 2019]. Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=358&ct1=0.
[129] Srov. § 20 odst. 1 trestního zákoníku.
[130] Zde ČR nevyužila možnost stanovit tento další současný úmysl pachatele jako podmínku naplnění znaků tohoto trestného činu, kterou Úmluva o počítačové kriminalitě připouští.

musel způsobit jakýkoli negativní následek. K jejímu naplnění postačuje samotné překonání bezpečnostního opatření a následné neoprávněné získání přístupu do počítačového systému nebo jeho části a obviněný svým jednáním tyto podmínky skutkové podstaty naplnil."[131]

Pokud jde o objektivní stránku, jednání pachatele spočívá v překonání bezpečnostního opatření a získání přístupu k počítačovému systému nebo jeho části. Jedná se tak o komisivní (aktivní) formu jednání.

Bezpečnostním opatřením je každé opatření, které je způsobilé plnit ochrannou funkci počítačového systému a slouží tak k zabránění volného přístupu k počítačovému systému nebo jeho části. Může jít o nejrůznější zabezpečovací software, hardware, užívání vstupních a bezpečnostních hesel, systém vymezení uživatelských práv, režim užívání počítačových systémů (bezpečnostní politiku) ve společnostech a stejně tak i ve veřejnoprávních institucích a přístup k nim i k jejich částem, a také zajištění pracovišť s počítačovým systémem pomocí technických zařízení. Bezpečnostním opatřením je rovněž nastavení integrovaného firewallu, který brání neoprávněným průnikům a ovládání počítače prostřednictvím sítě internet.[132]

Neoprávněným rozumíme jednání včetně přístupu, zásahu nebo sledování, které není povoleno majitelem či jiným držitelem práv k systému nebo k jeho části nebo které není povoleno vnitrostátním právem.[133]

Počítačovým systémem rozumíme jakékoli zařízení nebo skupinu propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.[134]

Získání přístupu definuje Jan Kolouch jako *„stav, kdy může pachatel volně disponovat s předmětným počítačovým systémem či nosičem informací, jakož i s daty zde uloženými."*[135] Obsahově stejnou definici nalezneme i v usneseních Nejvyššího soudu ČR sp. zn. 7 Tdo 731/2015 a 7 Tdo 932/2016, kde je uvedeno: *„Získáním přístupu se zde rozumí takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a*

[131] Usnesení Nejvyššího soudu ČR ze dne 29. 11. 2017, sp. zn. 7 Tdo 1469/2017.
[132] DRAŠTÍK, Antonín, FREMR, Robert, DURDÍK, Tomáš, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander aj., *op. cit.*
[133] Čl. 2 písm. d) Směrnice 2013/40/EU.
[134] Čl. 1 písm. a) Úmluvy o počítačové kriminalitě.
[135] KOLOUCH, Jan, *op. cit.*, s. 345.

využití jeho informačního obsahu.“[136] Autor této práce se domnívá, že taková definice je příliš úzká a ve skutečnosti je za získání přístupu potřeba uvažovat nejen stav, kdy pachatel s počítačovým systémem či nosičem informací může volně disponovat, ale i stav, kdy je tato dispozice dílčím způsobem omezena. Například, když pachatel získá přístup pouze k části systému, a ještě s nějakým omezením (to může spočívat mj. v tom, že mu není umožněno data v něm měnit), i tak se jedná o získání přístupu.

Z hlediska aplikace ustanovení odstavce 1 je zcela zásadní výklad pojmů bezpečnostní opatření a získání neoprávněného přístupu, zejména s ohledem na nejrůznější robotické aktivity prováděné v prostředí počítačových sítí, zvláště v síti internet. Existuje celá řada bezpečnostních opatření, jejichž cílem je zabránit robotické aktivitě, např. tzv. captcha,[137] různé limity připojení a opakování přístupů atp. Na druhou stranu existuje množství nástrojů a technik, které umožňují tato opatření překonat, např. specifické nástroje a služby pro překonání captcha ochrany,[138] paralelizace přístupů pro překonání ochrany proti opakování přístupů atp. Pokud při robotickém přístupu dojde k překonání bezpečnostních opatření proti robotům a dojde k získání přístupu k počítačovému systému, lze to považovat za naplnění skutkové podstaty 1. odstavce? Počítačový systém byl v takovém případě otevřen přístupům široké veřejnosti, zabezpečen však byl proti přístupům robotickým. Jedná se tak o neoprávněné získání přístupu? Autor této práce se domnívá, že i v takovém případě je potřeba uvažovat, že k naplnění skutkové podstaty dojde, a to právě s ohledem na výše uvedený možný výklad pojmu získání přístupu, kdy je uvažován nejen stav, kdy pachatel s počítačovým systémem či nosičem informací může volně disponovat, ale i stav, kdy je tato dispozice dílčím způsobem omezena. K této věci však bude potřeba vyčkat až na rozhodovací praxi soudů.

Druhou základní skutkovou podstatu nalezneme v odstavci 2, který zní:

„Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

[136] Usnesení Nejvyššího soudu ČR ze dne 30. 9. 2015, sp. zn. 7 Tdo 731/2015.
Usnesení Nejvyššího soudu ČR ze dne 14. 9. 2016, sp. zn. 7 Tdo 932/2016.

[137] Captcha je test, který se na webových stránkách používá k automatickému odlišení skutečného uživatele od robota.

[138] Např. služba Anti-captcha, viz https://anti-captcha.com. [cit. 1. 3. 2019].

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.“

Individuálním objektem trestného činu vymezeného v odst. 2 je integrita a dostupnost počítačových dat a systémů, včetně neoprávněného užívání dat a programů. U této skutkové podstaty se jedná o následek poruchový.

Pokud jde o objektivní stránku, jednání pachatele spočívá v získání přístupu k počítačovému systému nebo nosiči informací a neoprávněném užití dat; neoprávněném vymazání dat, nebo jejich jiném zničení, poškození, změnění, potlačení, snížení kvality či učinění neupotřebitelnými; padělání nebo pozměnění dat; nebo neoprávněném vložení dat. Jedná se tak o komisivní (aktivní) formu jednání.

Pro naplnění znaků této skutkové podstaty není rozhodující, zda pachatel získal přístup k počítačovému systému nebo nosiči informací oprávněně či neoprávněně. U této skutkové podstaty není vyžadováno překonání bezpečnostního opatření.

Počítačovými daty rozumíme jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.[139]

Nosičem informací rozumíme nosič dat v informační technice, do kterého nebo na který lze zaznamenávat (zapsat) data a z kterého lze data zpět získat (přečíst). Jedná se např. o pevný disk, operační paměť, diskety, CD, DVD nebo Blu-Ray nosič, USB disk, mobilní telefon, počítačový čip a další. Za nosič informací naopak není považován záznam zvuku nebo

[139] Čl. 1 písm. b) Úmluvy o počítačové kriminalitě.

kinematografický záznam, popř. videozáznam, přestože jsou zaznamenány kupř. na magnetické pásce.[140]

Subjekt je u obou základních skutkových podstat obecný. Není vyžadována žádná zvláštní vlastnost pachatele, jeho způsobilost nebo postavení. Pachatelem tak může být jakákoli fyzická nebo právnická osoba. Z hlediska subjektivní stránky je vyžadováno úmyslné zavinění.[141]

Ustanovení o trestném činu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 2 trestního zákoníku primárně nesankcionuje narušení důvěrnosti dat neoprávněným přístupem k počítačovému systému nebo k jeho části, jako je tomu podle odstavce 1. Nezáleží zde totiž na tom, zda takový přístup pachatel získal neoprávněně či naopak, zda pachatel již takovým přístupem z jiného důvodu oprávněně disponoval. Naproti tomu jsou ustanovením podle § 230 odst. 2 trestního zákoníku postižena různorodá jednání uvedená v písm. a) až d), která spočívají především v narušení integrity dat a jejich dostupnosti.[142]

Souběh základní skutkové podstaty uvedené v § 230 odst. 1 trestního zákoníku s druhou základní skutkovou podstatou uvedenou v § 230 odst. 2 je vyloučen z důvodu poměru subsidiarity skutkové podstaty uvedené v odst. 1 vůči skutkové podstatě uvedené v odst. 2. Poměr subsidiarity je dán tím, že ustanovení odst. 1 míří na jednání považovaná za zvláště trestnou přípravu k trestnému činu rozvedenému v odst. 2. Tomu odpovídá i návětí druhého odstavce, které zahrnuje i jednání spadající do prvního odstavce.[143]

Jan Kolouch má názor odlišný a považuje souběh obou skutkových podstat za možný. K tomu uvádí: *„Souběh s § 230 odst. 1 TZK je možný. Je možné si reálně představit situaci, kdy pachatel překoná bezpečnostní opatření, a tím získá přístup k počítačovému systému nebo jeho části a následně provede některé z jednání popsaných § 230 odst. 2 TZK (např. data zničí, vymaže, poškodí aj.).“*[144] Uvedená situace je opravdu reálně možná a pravděpodobně i velmi častá. U úvahy ohledně možného souběhu však v tomto případě zřejmě došlo k opomenutí výše uvedeného vztahu subsidiarity.

---

[140] DRAŠTÍK, Antonín, FREMR, Robert, DURDÍK, Tomáš, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander aj., *op. cit.*
[141] Srov. § 13 odst. 2 trestního zákoníku.
[142] Usnesení Nejvyššího soudu ČR ze dne 23. 8. 2017, sp. zn. 5 Tdo 781/2017.
[143] KRUPIČKA, Jiří, *op. cit.*, s. 88-89.
[144] KOLOUCH, Jan, *op. cit.*, s. 354.

Ustanovení § 230 odst. 2 trestního zákoníku je z hlediska tématu této práce klíčové. Útok typu DoS cílí právě na potlačení či neupotřebitelnost dat uložených v počítačovém systému, tedy jednání uvedené pod písmenem b) v tomto odstavci. Rozbor ohledně naplnění znaků této skutkové podstaty následuje v kapitole 3.4 Trestněprávní kvalifikace (D)DoS útoku.

Odstavce 3, 4 a 5 obsahují kvalifikované skutkové podstaty činů podle odstavce 1 a 2, tedy popisují takové okolnosti spáchání trestného činu, při jejichž splnění trestní zákoník stanoví přísnější trest, než který může být uložen při naplnění pouze základní skutkové podstaty. U útoku typu DoS, pokud je naplněna základní skutková podstata, prakticky vždy dojde k naplnění okolností uvedených v ustanovení odst. 3 písm. b), které vyžaduje úmysl neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Právě tento úmysl je s DoS útoky silně spojen, neboť k jeho naplnění takový útok směřuje. Mezi další okolnosti uvedené v těchto odstavcích patří členství pachatele v organizované skupině, úmysl způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, způsobit značnou škodu nebo škodu velkého rozsahu, získat značný prospěch nebo prospěch velkého rozsahu, způsobit vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci a způsobit vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem. Naplnění nejzávažnějších z těchto okolností (způsobení škody velkého rozsahu nebo získání prospěchu velkého rozsahu) může vést k trestní sazbě odnětí svobody na tři léta až osm let.

Jak již bylo uvedeno výše, trestné činy uvedené v tomto paragrafu byly do českého právního řádu zapracovány na základě Úmluvy o počítačové kriminalitě. Skutková podstata uvedená v odstavci 1 je výsledkem zapracování článku 2 Úmluvy, který zavádí kriminalizaci neoprávněného přístupu k počítačovému systému nebo jeho jakékoli části. Skutková podstata uvedená v odstavci 2 je výsledkem zapracování článků 4, 5 a 7 Úmluvy, které zavádějí kriminalizaci zásahu do dat a do systému a počítačového padělání. K tomu Jan Kolouch uvádí: *„Článek 4 Úmluvy o kyberkriminalitě se věnuje ochraně dat počítačového systému, jejichž narušení nemusí nutně vést k poškození počítačového systém, kdežto článek 5 Úmluvy o kyberkriminalitě chrání fungování počítačového systému jako celku. Nezávažná, drobná či snadno napravitelná narušení fungování počítačového systému by neměla být podle tohoto*

článku postihována.“[145] Zapracování několika článků Úmluvy do dvojice základních skutkových podstat jediného paragrafu činí českou právní úpravu poměrně komplikovanou a hůře srozumitelnou.[146]

3.3.2 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231)

Ustanovení § 231 trestního zákoníku obsahuje celkem 3 odstavce. V odstavci 1 jsou vymezeny znaky jedné základní skutkové podstaty tohoto úmyslného trestného činu.

Odst. 1 zní:

„Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.“

Tato skutková podstata kriminalizuje svou povahou přípravné jednání[147] k uvedeným trestným činům a jedná se tak o tzv. předčasně dokonaný trestný čin.

Individuálním objektem trestného činu vymezeného v odst. 1 je zájem *„na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží ke spáchání trestných činů*

[145] Ibid., s. 355.
[146] K tomu blíže viz kapitola 3.5 Zhodnocení právní úpravy a návrhy de lege ferenda.
[147] Jednání spočívající v držení, výrobě, zpřístupňování nebo jiném nakládání s prostředky, postupy nebo nástroji, užívanými ke spáchání kybernetických útoků.

porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2.“[148]

Zaměříme-li se na objektivní stránku, jednání pachatele je definováno alternativně a spočívá ve výrobě, uvedení do oběhu, dovozu, vývozu, průvozu, nabízení, zprostředkování, prodeji nebo jiném zpřístupnění, opatření sobě nebo jinému nebo přechovávání prostředků uvedených v písmenech a) a b). Navíc za současně splněného předpokladu, že pachatel se uvedeného jednání dopustil v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 1, 2. Jedná se především o komisivní (aktivní) formu jednání, lze si však představit i formu opomenutí (omisivní jednání), např. v situaci, kdy v rozporu se svou povinností do té doby oprávněná osoba nevrátí zařízení nebo neodstraní přístupová data poté, kdy tak měla učinit z důvodu zániku jejího oprávnění. Pokud by uvedený předpoklad ohledně úmyslu naplněn nebyl, pouhé uvedené jednání, bez naplnění fakultativního znaku subjektivní stránky skutkové podstaty tohoto trestného činu, tedy úmyslu spáchat některý z uvedených trestných činů, není trestné. Samotné držení prostředků uvedených v § 230 odst. 1 pod písm. a) a b) trestního zákoníku trestné není. Tyto prostředky jako takové jsou využívány i k legitimní činnosti, např. při vývoji a testování aplikací a systémů.

Subjekt je u této skutkové podstaty obecný. Není vyžadována žádná zvláštní vlastnost pachatele, jeho způsobilost nebo postavení. Pachatelem tak může být jakákoli fyzická nebo právnická osoba. Z hlediska subjektivní stránky je vyžadováno úmyslné zavinění,[149] včetně úmyslu spáchat některý z uvedených trestných činů.

Odstavce 2 a 3 obsahují kvalifikované skutkové podstaty činu podle odstavce 1, tedy popisují takové okolnosti spáchání trestného činu, při jejichž splnění trestní zákoník stanoví přísnější trest, než který může být uložen při naplnění pouze základní skutkové podstaty. Mezi okolnosti uvedené v těchto odstavcích patří členství pachatele v organizované skupině a zisk značného prospěchu nebo prospěchu velkého rozsahu. Naplnění nejzávažnější z těchto okolností (zisk prospěchu velkého rozsahu) může vést k trestní sazbě odnětí svobody na šest měsíců až pět let.

[148] ŠÁMAL, Pavel a kol., *op. cit.*, s. 2317.
[149] Srov. § 13 odst. 2 trestního zákoníku.

I tato skutková podstata byla do českého právního řádu zapracována na základě Úmluvy o počítačové kriminalitě. Skutková podstata uvedená v odstavci 1 je výsledkem zapracování článku 6 Úmluvy, který zavádí kriminalizaci zneužití zařízení, do národní legislativy.

3.3.3 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232)

Ustanovení § 232 trestního zákoníku obsahuje celkem 2 odstavce. V odstavci 1 jsou vymezeny znaky jedné základní skutkové podstaty tohoto nedbalostního trestného činu.

Odst. 1 zní:

„(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,

a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci.“

Individuálním objektem trestného činu vymezeného v odstavci 1 je ochrana počítačového systému, jeho technického i programového vybavení, nosiče informací a dat v tomto systému či na nosiči uložených, před jejich zničením, poškozením, pozměněním či učiněním neupotřebitelnými z hrubé nedbalosti.

Pokud jde o objektivní stránku, jednání pachatele je definováno alternativně a spočívá ve zničení, poškození, pozměnění nebo učinění neupotřebitelnými nebo učinění zásahu. Jednat se může o komisivní (aktivní) formu jednání i o opomenutí (omisivní jednání). Je vyžadováno, aby k uvedenému jednání došlo v důsledku porušení povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo která byla uložena podle zákona nebo je smluvně převzata a současně došlo k účinku v podobě způsobení značné škody na cizím majetku. U této skutkové podstaty se jedná o následek poruchový.

Subjekt je u této skutkové podstaty speciální. Je vyžadováno, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení.[150] Pachatelem může být pouze fyzická či právnická osoba, která vykonává zaměstnání, povolání, je v postavení, má funkci nebo má povinnosti uložené podle zákona nebo smluvně převzaté. V tomto případě půjde především o různé ICT správce, administrátory a jiné pracovníky v oblasti ICT. Z hlediska subjektivní stránky se musí jednat o zavinění nedbalostní, konkrétně o hrubou nedbalost, tedy stav, kdy přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.[151]

Odstavec 2 obsahuje kvalifikovanou skutkovou podstatu činu podle odstavce 1, tedy popisuje takové okolnosti spáchání trestného činu, při jejichž splnění trestní zákoník stanoví přísnější trest, než který může být uložen při naplnění pouze základní skutkové podstaty. Okolností uvedenou v tomto odstavci je způsobení škody velkého rozsahu. Její naplnění může vést k trestní sazbě odnětí svobody až na 2 léta.

V případě ustanovení tohoto paragrafu vztah k Úmluvě o počítačové kriminalitě nenalezneme. Skutková podstata zde obsažená byla v trestním zákoníku vymezena nad rámec Úmluvy.

3.4 Trestněprávní kvalifikace (D)DoS útoku

Trestněprávní posouzení útoku typu odepření služby je poměrně komplikovanou záležitostí. Dokládá to značná rozpornost mezi autory odborných textů, která vyplývá především z ne zcela dobře formulovaných ustanovení zvláštní části trestního zákoníku, jež se týkají kybernetické kriminality.

Pro vedení úvah o možném naplnění skutkové podstaty trestného činu musí před posuzováním formálních znaků určitého trestního činu, a jejich možného naplnění posuzovaným skutkem, předcházet uvážení zásady subsidiarity, resp. naplnění materiální stránky trestného činu v podobě společenské škodlivosti.[152] Budeme-li se proto zabývat trestní odpovědností za útoky typu odepření služby, je i zde nutno nejprve se zaměřit na zásadu subsidiarity zakotvenou v § 12

[150] Srov. § 114 odst. 1 trestního zákoníku.
[151] Srov. § 16 odst. 2 trestního zákoníku.
[152] NOVOTNÝ, František, SOUČEK Josef aj. *Trestní právo hmotné.* 3. vydání. Plzeň: Aleš Čeněk, 2010, s. 89.

odst. 2 trestního zákoníku: *„Trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech společensky škodlivých, ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu.“*[153] K tomuto ustanovení můžeme nalézt následující komentář: *„Je vyjádřením zásady subsidiarity trestní represe a principu trestní odpovědnosti jako ultima ratio, uplatnitelné jen v případech, kde jiné právní prostředky selhávají. Trestněprávní kvalifikaci určitého jednání jako trestného činu je tedy třeba považovat za krajní prostředek, který má význam jen z hlediska ochrany základních celospolečenských hodnot. Jinými slovy řečeno, trestnými činy mohou být pouze závažnější případy protispolečenských jednání, a to ve smyslu zásady, že tam, kde postačí k regulaci prostředky civilního nebo správního práva, jsou trestněprávní prostředky nejen nadbytečné, ale i nepřípustné.“*[154]

U útoků typu odepření služby je potřeba se vzhledem k jejich specifičnosti zabývat zejména intenzitou útoku. U krátkodobých útoků v podobě blokování běžných webových stránek, byť by formálně takový útok nesl znaky některého z trestných činů, pravděpodobně nedosáhne takové míry společenské škodlivosti, jaká je vyžadována ustanovením § 12 odst. 2 trestního zákoníku. V některých případech však i u krátkodobého útoku může dojít ke škodlivým následkům podstatně závažnějším, např. v případě blokování webových stránek obsahujících důležité informace pro výkon společensky potřebných činností nebo týkající se významných obchodů či jiných důležitých legitimních zájmů. Pak lze uvažovat o naplnění potřebné míry společenské škodlivosti, aby bylo možné dané jednání posuzovat jako trestné podle trestního zákoníku.[155]

Pokud se budeme zabývat alternativní možností postihu v rámci přestupkového řízení, narazíme na to, *„že v platném přestupkovém zákoně nenajdeme oporu pro postih, a to ani v případě útoku na server orgánu státu, jakkoli např. lze postihnout pachatele, který zničí, poškodí nebo neoprávněně odstraní veřejnou vyhlášku.“*[156] Dále má tedy smysl se zabývat znaky uvedenými v relevantních skutkových podstatách trestných činů a jejich možném naplnění.

---

[153] § 12 odst. 2 trestního zákoníku.
[154] DRAŠTÍK, Antonín, FREMR, Robert, DURDÍK, Tomáš, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander aj., *op. cit.*
[155] SMEJKAL, Vladimír, SOKOL, Tomáš. K možnostem postihu útoků DoS/DDoS v rámci českého právního řádu. *Data security management*. Roč. XVII., 2013, č. 3, s. 26.
[156] SMEJKAL, Vladimír, SOKOL, Tomáš, *op. cit.*, s. 27. Autoři hovoří o přestupkovém zákoně před komplexní změnou přestupkového práva účinnou od 1. 1. 2017, nicméně jejich slova jsou platná i po účinnosti nové právní úpravy přestupkové odpovědnosti.

V té nejobecnější rovině lze u (D)DoS útoků uvažovat o naplnění skutkové podstaty trestného činu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. b) trestního zákoníku. Zopakujme si znění relevantní části tohoto odstavce:

> *„Kdo získá přístup k počítačovému systému nebo k nosiči informací a*
>
> *a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,*
>
> *b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, …“*[157]

K tomu uvádí Jan Kolouch: *„Avšak zřejmě díky neznalosti technické stránky věci či díky potřebě ‚právního popsání' jednání, které má povahu DoS či DDoS útoků, došlo ke vzniku právní normy, která v praxi postih za provedení útoku DoS či DDoS neumožňuje.“*[158] Že se jedná o věc komplikovanou, dokládá i určitá vnitřní rozpornost u tohoto autora, který ve stejné publikaci na jiném místě k (D)DoS útokům uvádí: *„České trestní právo umožňuje některé z uvedených jednání postihnout dle § 230 odst. 2 písm. a) a b) TZK.“*[159]

Pro naplnění znaků této skutkové podstaty bude u (D)DoS útoků klíčové, aby pachatel získal přístup k počítačovému systému a data uložená v počítačovém systému potlačil, resp. učinil neupotřebitelnými. K pojmu získání přístupu je obecná úvaha uvedena již v kapitole 3.3, bodu 3.3.1 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230). Zaměříme-li se na zkoumaný typ útoků, klíčovou otázkou je, zda zákonodárce získáním přístupu myslí faktický přístup do něj, tedy do jeho nitra, nebo postačí přístup jaksi na povrch, tedy bez nutnosti získání oprávnění k jeho vnitřním částem. Právě především zde se láme posouzení páchání (D)DoS útoků jako trestného jednání nebo jednání, které znaky trestného činu nenaplňuje, neboť v trestním právu je analogie v neprospěch pachatele zásadně nepřípustná.

Vladimír Smejkal a Tomáš Sokol ve vztahu k DoS útoku uvažují možný výklad § 230 trestního zákoníku podpořený textem Úmluvy o počítačové kriminalitě takový, že podle návětí odst. 2 získal pachatel přístup k počítačovému systému, podle písm. b) odst. 2 data uložená v počítačovém systému učinil neupotřebitelnými, a to podle odst. 3 v úmyslu neoprávněně omezit

[157] Podrobněji viz kapitola 3.3, bod 3.3.1 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230).
[158] KOLOUCH, Jan, *op. cit.*, s. 301.
[159] Ibid., s. 353.

funkčnost počítačového systému. K pojmu *„získání přístupu“*, který je uveden v ustanovení § 230 odst. 2 trestního zákoníku, dodávají: *„autoři se zcela neshodnou na tom, zda tím zákonodárce myslel vniknutí dovnitř, nebo zda tak lze kvalifikovat i zadání adresy tohoto počítače.“*[160]

Autor této práce se domnívá, že při výkladu uvedeného pojmu *„získání přístupu“*, při uvažování smyslu zákona, dojdeme k tomu, že postačí přístup na povrch počítačového systému, a není potřeba získání přístupu do jeho nitra. A tedy, že při páchání útoku typu odepření služby dochází k jednání v podobě získání přístupu, které je jedním ze znaků uvedených v této skutkové podstatě trestného činu.

Určitý rozpor můžeme nalézt i v hodnocení pojmu *„data potlačit“*, resp. *„učinit neupotřebitelnými“*. To pramení z toho, že provedení útoku typu odepření služby negarantuje způsobení úplného potlačení nebo neupotřebitelnosti dat. Vznik tohoto následku je závislý nejen na intenzitě útoku, ale také na parametrech systému, proti kterému je útok veden. Pokud by útok nebyl dostatečně intenzivní pro způsobení tohoto následku, ale jeho způsobení by bylo záměrem pachatele, tento stav bychom hodnotili jako pokus příslušného trestného činu podle § 21 trestního zákoníku.

Shrneme-li uvedenou problematiku posouzení trestnosti (D)DoS útoků v obecné rovině, doplněnou o vlastní názor autora, dojdeme k závěru, že provedení útoku tohoto typu je třeba považovat za trestné jednání. Samozřejmě vždy bude potřeba se zabývat konkrétními skutkovými okolnostmi ve vztahu k posouzení společenské škodlivosti dané intenzitou útoku a charakteristikou jeho cíle, a dále také intenzitou útoku ve vztahu k potlačení dat či jejich učinění neupotřebitelnými. Věc je poměrně specifická a ani v dostupné judikatuře soudů nenajdeme řešení této otázky.

V následujícím textu je popsána trestněprávní kvalifikace jednotlivých variant útoku s ohledem na specifičnost jeho technického provedení. Členění textu odpovídá struktuře části 1, kapitoly 1.3 Jednotlivé typy DoS útoků a související techniky, která se věnuje technickému popisu jednotlivých variant útoku. Dále již není uvažována potřeba naplnění společenské škodlivosti daného jednání a intenzity útoku ve vztahu k potlačení dat. Stejně tak dále zpravidla

[160] SMEJKAL, Vladimír, SOKOL, Tomáš, *op. cit.*, s. 27.

není uvažováno naplnění dalších okolností uvedených v kvalifikovaných skutkových podstatách. Cílem je trestněprávně posoudit základní jednání, bez uvažování např. způsobené výše škody nebo prospěchu, zvláštního předmětu útoku atp.

3.4.1 Prostý DoS útok

Provedení tohoto typu útoku naplňuje skutkovou podstatu trestného činu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. b) trestního zákoníku, neboť svým jednáním pachatel získá přístup k počítačovému systému a data uložená v počítačovém systému neoprávněně potlačí, resp. učiní neupotřebitelnými. Současně naplní i kvalifikovanou skutkovou podstatu podle § 230 odst. 3 písm. b), neboť jedná v úmyslu neoprávněně omezit funkčnost počítačového systému, což je prvořadým cílem každého DoS útoku. Pokud při útoku dojde i k překonání bezpečnostního opatření, např. pomocí škodlivého kódu nebo jiných metod hackingu, dojde sice současně i k naplnění § 230 odst. 1 trestního zákoníku, jak ale bylo již rozebráno v kapitole 3.3, bodu 3.3.1 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230), je toto ustanovení ve vztahu subsidiarity k § 230 odst. 2 trestního zákoníku, a proto je jejich souběh vyloučen.

3.4.2 Distribuovaný DoS – DDoS

V případě provedení DoS útoku distribuovanou formou pomocí sítě zotročených počítačů půjde zpravidla o dva samostatné skutky. Skutek je souhrnem všech vnějších projevů vůle pachatele, které jsou příčinou následku významného z hlediska trestního práva, pokud jsou zahrnuty zaviněním. Prvním skutkem je samotné obstarání sítě zotročených počítačů, což se typicky stane překonáním bezpečnostních opatření pomocí hackerského útoku nebo podvodem spáchaným na uživateli. Zde se typicky bude jednat o naplnění znaků trestného činu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 1 trestního zákoníku, a to v případě překonání bezpečnostního opatření pomocí hackerského útoku. V případě podvodného jednání provedeného např. pomocí phishingového e-mailu[161] může dojít k naplnění znaků skutkové podstaty trestného činu podvodu podle § 209 trestního zákoníku, jehož základní

[161] Podvodný e-mail, který se pomocí metody sociálního inženýrství snaží uživatele přimět k provedení určité akce nebo sdělení určité informace.

skutková podstata zní: *„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“*[162] Obohacením se rozumí *„neoprávněné rozmnožení majetku (majetkových práv) pachatele nebo někoho jiného, ať již jeho rozšířením nebo ušetřením nákladů, které by jinak byly z majetku pachatele nebo někoho jiného vynaloženy.“*[163] Obohacení pachatele lze spatřovat i v tom, že získá možnost čerpat výpočetní výkon cizího počítače a úkolovat jej tak, aby prováděl činnost podle pachatelových pokynů. Problematické však může být naplnění znaku způsobení následku ve formě škody nikoli nepatrné, tedy dosahující částky nejméně 5 000 Kč.[164] K tomuto následku povětšinou nedojde, a proto útokem vedeným pomocí sociálního inženýrství skutková podstata trestného činu podvodu podle § 209 trestního zákoníku často naplněna nebude.

Při obstarání sítě zotročených počítačů za účelem provedení DDoS útoku může pachatel využívat *„zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části,“*[165] a tím dojde k naplnění znaků trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 odst. 1 písm. a) trestního zákoníku. Podvodným jednáním si pachatel může při obstarávání sítě zotročených počítačů, podle povahy tohoto jednání, opatřit a dále přechovávat počítačové heslo, a tím naplnit znaky trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 odst. 1 písm. b) trestního zákoníku. K budování takové sítě zotročených počítačů zpravidla nedochází s cílem provedení konkrétního DDoS útoku. Takovou síť si útočník buduje pro další využití k různým útokům. Bude se proto zpravidla jednat o samostatný skutek. Druhým skutkem je potom provedení vlastního DDoS útoku. Zde bude trestněprávní kvalifikace stejná, jako v případě prostého DoS útoku. To, zda se jedná o souběh vícečinný či jednočinný posoudíme

[162] § 209 odst. 1 trestního zákoníku.
[163] DRAŠTÍK, Antonín, FREMR, Robert, DURDÍK, Tomáš, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander aj., *op. cit.*
[164] Srov. § 138 odst. 1 trestního zákoníku.
[165] § 231 odst. 1 písm. a) trestního zákoníku.

podle toho, zda se jedná o jeden či více skutků. K řešení této otázky se musíme zabývat vůlí pachatele. Pokud se jedná o dva samostatné skutky, půjde o vícečinný souběh.[166]

Síť zotročených počítačů si pachatel také může pronajmout na černém trhu. V takovém případě pachatel bude disponovat prostředkem, pomocí něhož lze získat přístup k počítačovému systému (systému zotročeného počítače) a dojde tak k naplnění znaků trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 odst. 1 písm. b) trestního zákoníku. Ovšem, trestný čin podle § 231 trestního zákoníku není možné spáchat v jednočinném souběhu s trestným činem podle § 230 trestního zákoníku, a to z důvodu subsidiarity, neboť se jedná o zvláště trestnou přípravu. V tomto případě zpravidla půjde o součást jediného jednání (pronájem sítě zotročených počítačů a provedení DoS útoku jejich pomocí) a právní kvalifikace tak bude odpovídat prostému DoS útoku.

Pokud je distribuovaný útok proveden na základě spolupráce pachatelů v rámci hacktivistické skupiny, bude se jednat opět o trestný čin neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. b) a odst. 3 písm. b), tentokrát však spáchaný ve spolupachatelství podle § 23 trestního zákona. V tomto případě bude důležité také uvažovat společný cíl tohoto jednání, související zejména s intenzitou útoku, zda bude taková, že povede k potlačení, resp. znepřístupnění dat. K tomu blíže Vladimír Smejkal a Tomáš Sokol uvádějí: *„V případě zorganizování demonstrace využívající předem neznámý a nekvantifikovatelný okruh účastníků by zřejmě nebylo zcela jednoznačné prokázání úmyslu zcela zlikvidovat funkčnost serveru, a tím učinit informace, které zobrazuje, neupotřebitelnými. A contrario – pachatel by mohl namítat, že mu šlo pouze o omezení provozu (zpomalení práce serveru), a takové jednání nelze podle stávající definice skutkové podstaty postihnout.“*[167]

3.4.3 Distribuovaný odražený DoS (DRDoS) a podvržení IP adresy (IP Spoofing)

Specifikum distribuovaného odraženého DoS útoku spočívá mimo jiné v použití techniky podvržení zdrojové IP adresy. Jednání spočívající v neoprávněné záměně IP adresy je sice závadným jevem, který může iniciovat nežádoucí datové toky v počítačových sítích, samo o sobě

[166] NOVOTNÝ, František, SOUČEK Josef aj., *op. cit.*, s. 221-223.
[167] SMEJKAL, Vladimír, SOKOL, Tomáš, *op. cit.*, s. 28.

však zřejmě nebude trestným jednáním. Jedná se o prostředek, jak dosáhnout cíle a trestně postižitelným jednáním tak bude opět samotný DoS útok, který bude spočívat ve značném množství paketů s podvrženou IP adresou, které budou schopné způsobit odepření přístupu legitimním uživatelům.

3.4.4 ICMP záplava (Ping Flood), záplava pakety SYN (SYN Flood)

Záplavy ICMP pakety nebo pakety SYN jsou jedněmi z technik prostého DoS útoku. Trestněprávní kvalifikace tak bude odpovídat tomuto typu útoku, bez dopadu konkrétní techniky na změnu trestněprávní kvalifikace.

3.4.5 Útok Smurf (Smurf attack)

Svou podstatou je Smurf útok variantou distribuovaného odraženého DoS útoku včetně použití techniky podvržení IP adresy. Pro trestněprávní kvalifikaci tak platí vše, co bylo uvedeno v bodu 3.4.3 Distribuovaný odražený DoS (DRDoS) a podvržení IP adresy (IP Spoofing).

3.5 Zhodnocení právní úpravy a návrhy de lege ferenda

Páchání kybernetických útoků představuje stále ještě poměrně nový typ kriminálního jednání. Počítačová kriminalita má své specifické vlastnosti, dané zvláštností kybernetického prostředí. K řadě aktivit v kyberprostoru neexistuje paralela v reálném prostředí. Kybernetické útoky, jako nástroj organizovaného zločinu nebo jako prostředek použitý v souvislosti s ekonomickými zájmy, mohou způsobit značné škody. V případě kybernetických útoků nemusí jít jen o přímé ekonomické škody. Jejich páchání může dojít také k ohrožení funkce kritické infrastruktury státu, a nejen v této souvislosti může dokonce dojít k přímému ohrožení lidských životů. Výše uvedený rozbor příslušných ustanovení trestního zákoníku nám dává jasný závěr, že i při naplnění těch nejzávažnějších okolností je horní hranice trestu odnětí svobody u nejzávažnějšího z těchto činů stanovena na 8 let. Tato trestní sazba neodpovídá závažnosti a možným následkům vyvolaným jednáním v podobě kybernetických útoků. Pro možnost účinnějšího postihu, zvláště těch nejzávažnějších forem tohoto jednání, by bylo vhodné, aby došlo ke zvýšení této horní hranice trestní sazby.

Pokud se zaměříme na formulaci jednotlivých ustanovení § 230 až § 232 trestního zákoníku, nelze než konstatovat, že by bylo velmi potřebné tato ustanovení formulovat lépe, jasněji a srozumitelněji. Exemplárním příkladem je výčet možných jednání ohledně nakládání s daty uvedený v § 230 odst. 2 písm. b), který obsahuje povětšinou synonyma, a mohl by doznat významné redukce.

Problematický je také výklad pojmu *„získat přístup“* a v určitém kontextu může být sporné, zda lze dané jednání považovat za překonání *„bezpečnostního opatření“*. Obtíže související s těmito pojmy jsou rozebrány v kapitole 3.3, bod 3.3.1 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230).

Jak již bylo uvedeno výše, trestné činy uvedené v § 230 a § 231 trestního zákoníku byly do českého právního řádu zapracovány na základě Úmluvy o počítačové kriminalitě, konkrétně čtyř jejích článků. Zkombinovat čtyři trestná jednání definovaná Úmluvou do dvojice trestných činů našeho právního řádu jeho přehlednosti nepřispívá. Právní úprava je komplikovaná, nepřehledná a těžko srozumitelná. Navíc dostatečně jasně nepokrývá trestnost právě DoS útoků. To je dáno také ne zcela korektním zapracováním článku 4 Úmluvy o počítačové kriminalitě. Tento článek se totiž neomezuje na potřebu *„získání přístupu“*, což je jeden ze znaků uvedených v stanovení § 230 odst. 2 trestního zákoníku.[168]

Zaměříme-li se na trestnost kybernetického útoku typu DoS, pak, vzhledem k výše uvedeným výkladovým obtížím a obtížné srozumitelnosti ustanovení § 230 trestního zákoníku, je více než žádoucí doplnit zvláštní část trestního zákoníku o jasně formulované ustanovení kriminalizující tento typ útoku. K tomu se vyjadřuje i autorská dvojice Vladimír Smejkal a Tomáš Sokol: *„Z dikce zákona vyplývá, že jeho autoři jako hrozbu vnímali situaci, kdy někdo pronikne dovnitř systému a data změní nebo smaže, čemuž je vše podřízeno. Nejspíš ani neuvažovali, že by někdo mohl škodit, aniž by datům a tomuto systému jako takovému nějak ublížil.“*[169]

Úprava zvláštní části trestního zákoníku by mohla být provedena zavedením nové skutkové podstaty trestného činu, která by jasně kriminalizovala útoky typu odepření služby.

[168] Čl. 4 odst. 1 Úmluvy o počítačové kriminalitě zní: *„Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat.“*
[169] SMEJKAL, Vladimír, SOKOL, Tomáš, *op. cit.*, s. 28.

Skutková podstata takového trestného činu by mohla být založena na poměrně jednoduchém znění: *„Kdo bez oprávnění potlačí počítačová data…“*

Závěr

Tato diplomová práce se věnuje tématu kyberkriminality se zaměřením na útoky typu odepření služby. Téma bylo v práci zkoumáno z mnoha úhlů. V práci bylo postupováno od technického popisu tohoto specifického druhu útoků přes kriminologické aspekty kybernetické kriminality až po rozbor trestněprávních aspektů tohoto druhu kriminality se zaměřením na útoky typu odepření služby.

Při zpracování práce autor narazil na určité problémy, nejednoznačnosti a rozpory, zejména týkající se trestněprávního posouzení některých činů v kybernetickém prostoru. Konkrétně pak právě útoku typu odepření služby, kterému je práce věnována především. Tyto problémy jsou dány především stále ještě novostí tématu kybernetické kriminality a celkově neustálým vývojem v oblasti informačních a komunikačních technologií, který se projevuje především zrychlováním počítačů, navyšováním objemu telekomunikačních linek a souvisejícím vznikem nových technologií a s tím vším i nových rizik.

Úvodní část práce byla věnována technickým aspektům DoS útoků, spolu s popisem jednotlivých typů tohoto útoku a souvisejících technik. Těch je celá řada, ale v základu můžeme útok dělit zejména na prostý DoS a jeho distribuovanou variantu.

Další část práce byla věnována kriminologickým aspektům kybernetické kriminality se zaměřením zejména na útoku typu odepření služby. V této části došlo také k popisu možností prevence před těmito útoky. Efektivní a zcela spolehlivá ochrana však neexistuje.

Stěžejní obsah práce nalezneme v její třetí části, která se věnuje právním otázkám. Právě zde autor narazil na řadu problémů, které počínají už v nejednoznačné definici pojmu *„kyberkriminalita“*. Na komplikace narazíme při hledání správného výkladu některých znaků skutkových podstat kybernetických trestných činů a v neposlední řadě právě při trestněprávním posouzení páchání útoků typu odepření služby.

Uvedené nesnáze jsou shrnuty v závěrečné kapitole práce, kde jsou také uvedeny návrhy de lege ferenda pro zpřehlednění, zpřesnění a doplnění právní úpravy tak, aby postih kybernetické kriminality nevyvolával tolika otázek a trestní sazba byla adekvátní následkům, které mohou být kybernetickými útoky způsobeny.

Jako cíl této práce autor zvolil provedení rozboru trestněprávního posouzení kybernetických útoků typu odepření služby a souvisejících kriminologických aspektů. Pro naplnění tohoto cíle se v práci důkladně zabýval zkoumáním technických, kriminologických a trestněprávních aspektů tohoto typu útoku. V práci se rovněž věnoval kybernetické kriminalitě obecně a dále také technikám, pomocí kterých lze útoku typu (D)DoS čelit. Při zpracování této práce byla k popsání současného stavu využita metoda deskriptivní a metoda výkladová. K rozboru vybraných oblastí a pro formulaci vlastních názorů byla využita metoda analytická. S využitím uvedených postupů došlo k naplnění stanoveného cíle práce.

Závěrem je tak možné konstatovat, že i když útok typu odepření služby není kazuisticky popsán v žádné ze skutkových podstat trestných činů uvedených ve zvláštní části trestního zákoníku, lze jej na základě způsobu jeho provedení a souvisejících projevů trestně postihnout. Úpravou ustanovení § 230 až § 232 trestního zákoníku by však bylo možné dosáhnout vyšší určitosti, srozumitelnosti a tím i právní jistoty ve vztahu ke kybernetickým trestným činům.

Seznam zkratek

ACTA Obchodní dohoda proti padělatelství (Anti-Counterfeiting Trade Agreement)

APT Označení pro útoky založené na sofistikovaných hackerských technikách zaměřených přímo na konkrétní cíl, kterým mohou být velké společnosti či státy (Advanced Persistant Threat)

CSIRT Bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů (Computer Security Incident Response Team)

ČR Česká republika

DoS Útok typu odepření služby (Denial of Service)

DDoS Distribuovaný útok typu odepření služby (Distributed Denial of Service)

(D)DoS Prostý nebo distribuovaný útok typu odepření služby

DRDoS Distribuovaný odražený útok typu odepření služby (Distributed Reflected Denial of Service)

ICANN Mezinárodní nezisková organizace, která dohlíží nad některými databázemi, jmennými a číselnými prostory důležitými pro fungování internetu (Internet Corporation for Assigned Names and Numbers)

ICMP Internetový protokol pro kontrolu komunikace (Internet Control Message Protocol)

ICT Informační a komunikační technologie (Information and Communication Technologies)

LOIC Softwarový nástroj pro páchání DoS útoků (Low Orbit Ion Cannon)

HOIC Softwarový nástroj pro páchání DoS útoků (High Orbit Ion Cannon)

RTBH Technika používaná při obraně proti DDoS útokům (Remotely-Triggered Black Hole)

Seznam použitých zdrojů

Monografie, učebnice, komentáře

ANONYMOUS. *Maximum Security*. 4. vydání. USA: Sams Publishing, 2003, 945 s. ISBN 0-672-32459-8.

DIANIŠKA, Gustáv a kol. *Kriminológia*. Plzeň: Aleš Čeněk, 2009, 326 s. ISBN 978-80-7380-198-4.

DRAŠTÍK, Antonín, FREMR, Robert, DURDÍK, Tomáš, RŮŽIČKA, Miroslav, SOTOLÁŘ, Alexander aj. *Trestní zákoník: Komentář* [Systém ASPI]. Wolters Kluwer [cit. 1. 3. 2019]. ASPI_ID KO40_2009CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

ENDORF, Carl, SCHULTZ, Eugene, MELLANDER, Jim. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. 1. vydání. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. 2. vydání. Praha: Policejní akademie ČR v Praze, 2013, 200 s. ISBN 978-80-7251-397-0.

KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, 522 s. ISBN 978-80-88168-15-7.

NOVOTNÝ, František, SOUČEK Josef aj. *Trestní právo hmotné.* 3. vydání. Plzeň: Aleš Čeněk, 2010, 393 s. ISBN 978-80-7380-291-2.

POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Policejní akademie České republiky, 2007, 219 s. ISBN 978-80-7251-250-8.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vydání. Plzeň: Aleš Čeněk, 2015, 640 s. ISBN 978-80-7380-501-2.

SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. 1. vydání. Praha: C. H. Beck/SEVT, 1995, 264 s. ISBN 80-7179-009-5.

SVATOŠ, Roman. *Kriminologie*. Plzeň: Aleš Čeněk, 2012, 290 s. ISBN 978-80-7380-389-6.

ŠÁMAL, Pavel a kol. *Trestní zákoník I + II. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, 3632 s. ISBN 978-80-7400-428-5.

WESTBY, Jody R. *International Guide to Cyber Security*. USA: American Bar Association, 2004, 330 s. ISBN 978-1-59031-332-9.

Odborné články

BERNSTEIN, Daniel J. *SYN cookies* [online]. [cit. 1. 3. 2019]. Dostupné z: http://cr.yp.to/syncookies.html.

HUNTON, Paul. The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*. Vol. 25. Elsevier B.V., 2009. s. 528-535.

KOSTIHA, František. Bezpečnost informací. *Ikaros* [online]. 2006, roč. 10, č. 5 [cit. 1. 3. 2019]. Dostupné z: https://ikaros.cz/bezpecnost-informaci. ISSN 1212-5075.

RYLICH, Jan. SOPA, PIPA & ACTA aneb Boj o svobodu na Internetu. *Ikaros* [online]. 2012, roč. 16, č. 2 [cit. 1. 3. 2019]. Dostupné z: https://ikaros.cz/sopa-pipa-acta-aneb-boj-o-svobodu-na-internetu. ISSN 1212-5075.

SENIE, Daniel. Changing the Default for Directed Broadcasts in Routers. *RFC 2644* [online]. [cit. 1. 3. 2019]. Dostupné z: https://tools.ietf.org/html/rfc2644.

SMEJKAL, Vladimír, SOKOL, Tomáš. K možnostem postihu útoků DoS/DDoS v rámci českého právního řádu. *Data security management*. Roč. XVII., 2013, č. 3, 51 s. ISSN 1211-8737.

WILSON, Clay. Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. *Washington Congressional Research Service* [online]. 2003. [cit. 1. 3. 2019]. Dostupné z: http://www.fas.org/irp/crs/RL32114.pdf.

Internetové zdroje

24/7 WALL ST. *The Cost of a Computer the Year You Were Born* [online]. [cit. 1. 3. 2019]. Dostupné z: https://247wallst.com/special-report/2016/04/15/how-much-a-computer-cost-the-year-you-were-born.

ACAMSTODAY.ORG. *Cybersecurity: Nation-State Actors, Encrypted Cybercrimes and Man-in-the-Middle Attacks* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.acamstoday.org/nation-state-actors-encrypted-cybercrimes-man-in-the-middle-attacks.

ASOCIACE PRO ELEKTRONICKOU KOMERCI. *Tisková zpráva (27. 12. 2018) – E-shopy mají za sebou další rekordní Vánoce, nyní startují výprodeje!* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.apek.cz/clanky/e-shopy-maji-za-sebou-dalsi-rekordni-vanoce-nyni.

ASOCIACE PRO ELEKTRONICKOU KOMERCI. *Tisková zpráva (6. 1. 2019) – Česká e-commerce překonala očekávání, obraty za prodej zboží on-line dosáhly v roce 2018 na 135 miliard korun* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.apek.cz/clanky/ceska-e-commerce-prekonala-ocekavani-obraty-za-pr.

BUSINESSWORLD.CZ. *Novinky (3. 2. 2013) – Nezletilý hacker z Anonymous nemusí do vězení* [online]. [cit. 1. 3. 2019]. Dostupné z: https://businessworld.cz/novinky/nezletily-hacker-z-anonymous-nemusi-do-vezeni-10415.

CLOUDFLARE.COM. *DNS Amplification Attack* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack.

CLOUDFLARE.COM. *Ping (ICMP) Flood DDoS Attack* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack.

CZ.NIC. *Rekapitulace (D)DoS útoků ze dnů 4.3. - 7.3.* [online]. 2013 [cit. 1. 3. 2019]. Dostupné z: http://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf.

CZ.NIC, CSIRT.CZ. *Základní principy DoS útoku* [online]. [cit. 1. 3. 2019] https://www.csirt.cz/page/2790/zakladni-principy-dos-utoku.

ČESKÝ STATISTICKÝ ÚŘAD. *Tisková zpráva (22. 10. 2017) – Volební weby byly nedostupné kvůli DDoS útoku* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.czso.cz/csu/czso/volebni-weby-byly-nedostupne-kvuli-ddos-utoku.

EURO. *Light (21. 8. 2018) – Hackování kardiostimulátorů může zabít pacienty. Výrobce to neřeší* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.euro.cz/light/hackovani-kardiostimulatoru-muze-zabit-pacienty-vyrobce-to-neresi-1417780#utm_medium=selfpromo&utm_source=euro&utm_campaign=copylink.

HACKPEDIA.ORG, *Tfreak* [online]. [cit. 1. 3. 2019]. Dostupné z: http://hackepedia.org/?title=Tfreak.

iROZHLAS.cz. *Svět (8. 9. 2012) – Maďarská policie zatkla 16letého šéfa skupiny hackerů hlásících se k Anonymous* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/madarska-policie-zatkla-16leteho-sefa-skupiny-hackeru-hlasicich-se-k-anonymous_201209081408_kbrezovska.

iDNES.CZ. *Kultura (14. 8. 2012) – Hudební CD v Česku zlevnila a jejich prodej meziročně výrazně stoupl* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.idnes.cz/kultura/hudba/prodej-cd-vyrazne-stoupl.A120814_132600_hudba_ob.

iDNES.CZ. *Technet (26. 1. 2012) – Anonymous napadli servery OSA, web české vlády i Evropského parlamentu* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.idnes.cz/technet/internet/anonymous-napadli-servery-osa-web-ceske-vlady-i-evropskeho-parlamentu.A120126_134112_sw_internet_nyv.

ITNEWS.COM.AU. *How dangerous is Anonymous?* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.itnews.com.au/news/how-dangerous-is-anonymous-248990.

KASPERSKYLAB. *The cost of launching a DDoS attack* [online]. [cit. 1. 3. 2019]. Dostupné z: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784.

LIDOVKY.CZ. *Byznys (9. 12. 2010) – Česká pošta čelí útoku hackerů. V ohrožení jsou balíky s vánočními dárky* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.lidovky.cz/byznys/firmy-a-trhy/ceska-posta-celi-utoku-hackeru-v-ohrozeni-jsou-baliky-s-vanocnimi-darky.A101209_191040_firmy-trhy_sm.

LUPA.CZ. *Články (16. 12. 2011) – Tisíce tuzemských e-shopů mělo výpadky, může za to masivní DDoS útok* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.lupa.cz/clanky/tisice-tuzemskych-e-shopu-melo-vypadky-muze-za-to-masivni-ddos-utok.

MALWARE PATROL. *DDoS Reflection and Amplification Attacks* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.malwarepatrol.net/ddos-reflection-and-amplification-attacks.

McCLATCHY WASHINGTON BUREAU. *Hackers lurked undetected on networks now owned by Marriott for 4 years* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.mcclatchydc.com/news/policy/technology/cyber-security/article222437465.html.

MEZINÁRODNÍ ORGANIZACE PRO NORMALIZACI. *Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. Standards Catalogue* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.iso.org/standard/20269.html.

MEZINÁRODNÍ TELEKOMUNIKAČNÍ UNIE. *ITU releases 2018 global and regional ICT estimates. 2018* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx.

NIX.CZ. *ČLENOVÉ TÝMU FENIX* [online]. [cit. 1. 3. 2019]. Dostupné z: https://fe.nix.cz/#members.

NIX.CZ. *O FENIXU* [online]. [cit. 1. 3. 2019]. Dostupné z: https://fe.nix.cz/#about.

POLICIE ČR. *Kyberkriminalita* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

RADA EVROPY. *Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime*. Treaty Office [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

RADA EVROPY. *Chart of signatures and ratifications of Treaty 189 - Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Treaty Office [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures.

ROOT.CZ. *Bezpečnost (23. 2. 2015) – Konkrétní ukázka (D)DoS útoku z pohledu peeringového uzlu* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.root.cz/clanky/konkretni-ukazka-d-dos-utoku-z-pohledu-peeringoveho-uzlu.

STATISTA. *Online-Shopping and E-Commerce worldwide: Statistics & Facts* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.statista.com/topics/871/online-shopping.

TECHTERMS.COM. *Ping* [online]. [cit. 1. 3. 2019]. Dostupné z: https://techterms.com/definition/ping.

Právní předpisy

RADA EVROPY. *Úmluva o počítačové kriminalitě* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

RADA EVROPY. *Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 *o útocích proti informačním systémům* [online]. [cit. 1. 3. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32005F0222.

Sdělení č. 104/2013 Sb. m.s., *sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě*.

Sdělení č. 9/2015 Sb. m.s., *sdělení Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů*.

Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 *o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV* [online]. [cit. 1. 3. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32013L0040.

Zákon č. 557/1991 Sb., *zákon, kterým se mění a doplňuje trestní zákon*, zrušen.

Zákon č. 106/1999 Sb., *zákon o svobodném přístupu k informacím*, v platném znění.

Zákon č. 127/2005 Sb., *zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)*, v platném znění.

Zákon č. 40/2009 Sb., *trestní zákoník*, v platném znění.

Zákon č. 418/2011 Sb., *zákon o trestní odpovědnosti právnických osob a řízení proti nim*, v platném znění.

Zákon č. 181/2014 Sb., *zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*, v platném znění.

Zákon č. 165/2015 Sb., *zákon, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.*

Judikatura

Usnesení Nejvyššího soudu ČR ze dne 29. 11. 2017, sp. zn. 7 Tdo 1469/2017.

Usnesení Nejvyššího soudu ČR ze dne 23. 8. 2017, sp. zn. 5 Tdo 781/2017.

Usnesení Nejvyššího soudu ČR ze dne 30. 9. 2015, sp. zn. 7 Tdo 731/2015.

Usnesení Nejvyššího soudu ČR ze dne 14. 9. 2016, sp. zn. 7 Tdo 932/2016.

Ostatní

Důvodová zpráva k zákonu č. 165/2015 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. Sněmovní tisk 358/0, část č. 1/6 Novela z. - trestní zákoník – EU [online]. [cit. 1. 3. 2019]. Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=358&ct1=0.

Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník. Sněmovní tisk 410/0, část č. 1/9 Vl.n.z. trestní zákoník – EU [online]. [cit. 1. 3. 2019]. Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=410&ct1=0.

KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality* [online]. [cit. 1. 3. 2019]. Praha, 2012. Disertační práce. Univerzita Karlova. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/68976.

ORGANIZACE SPOJENÝCH NÁRODŮ. *United Nations Manual on the prevention and control of computer-related crime* [online]. [cit. 1. 3. 2019]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf.

Seznam tabulek a obrázků

Tabulky

Obrázky

Trestněprávní a kriminologické aspekty kyberkriminality se zaměřením na útoky typu odepření služby

Abstrakt

Cílem této diplomové práce je provést rozbor trestněprávního posouzení kybernetických útoků typu odepření služby (DoS) a souvisejících kriminologických aspektů. Autor se v práci zabývá nejprve technickou charakteristikou a typologií útoku tohoto typu. Rozebírá jeho jednotlivé varianty, neboť způsob provedení útoku se odráží i v jeho trestněprávním posouzení. V práci jsou popsány také skutečnosti týkající se největší série DoS útoků, ke kterým v České republice došlo v roce 2013. Autor se dále věnuje kriminologickým aspektům kybernetické kriminality, a to jejímu rozmachu a latenci, pachatelům a obětem útoku typu odepření služby, modu operandi i související prevenci, včetně technik a způsobů, jak se lze proti tomuto útoku bránit. Ve stěžejní části práce provádí rozbor trestněprávních aspektů tohoto specifického druhu kriminality. Zde se zabývá vývojem práva v této oblasti na mezinárodní úrovni, v rámci Evropské unie i na národní úrovni. Dále se věnuje rozboru skutkových podstat kybernetických trestných činů uvedených v § 230 až § 232 trestního zákoníku a trestněprávnímu posouzení jednotlivých variant útoku. V práci jsou rozebrány související problematické body, počínaje nejednotnou definicí kybernetické kriminality, přes nejasný výklad některých pojmů, až po trestněprávní kvalifikaci kybernetického útoku typu odepření služby, kterou také nelze provést bez obtíží. Závěrem autor konstatuje, že i když útok typu odepření služby není kazuisticky popsán v žádné ze skutkových podstat trestných činů uvedených ve zvláštní části trestního zákoníku, lze jej na základě způsobu jeho provedení a souvisejících projevů trestně postihnout. Úpravou ustanovení § 230 až § 232 trestního zákoníku by však bylo možné dosáhnout vyšší určitosti, srozumitelnosti a tím i právní jistoty ve vztahu ke kybernetickým trestným činům.

Klíčová slova: kyberkriminalita, útok, odepření služby

Criminal and criminological aspects of cybercrime with a focus on denial of service attacks

Abstract

The aim of this master thesis is to analyze the criminal law assessment of denial of service (DoS) cyber-attacks and related criminological aspects. The author deals with the technical characteristics and typology of this type of attack. He analyzes its individual variants, as the way of performing the attack, that is reflected in its criminal assessment. The thesis also describes the facts concerning the largest series of DoS attacks that occurred in the Czech Republic in 2013. Next, the author deals with the criminological aspects of cybercrime, namely its expansion and latency, the perpetrators and victims of the denial of service attack and related prevention, including techniques and methods of defense against this attack. In the main part of the thesis, the author analyzes the criminal law aspects of this specific type of crime. The thesis deals with the development of law in this area at international level, within the European Union and at national level. It also deals with the analysis of the factual situation of cybercrime provided for in Sections 230 to 232 of the Criminal Code and the criminal law assessment of individual variants of the attack. The thesis deals with related problematic points, starting with the non-uniform definition of cybercrime, despite the unclear interpretation of some terms, to the criminal law classification of denial of service cyber-attack, which can also not be done without difficulty. In conclusion, the author states that although the denial of service attack is not casuistically described in any of the factual situation of cybercrime set out in the special section of the Criminal Code, it can be criminally penalized based on the manner of its execution and related manifestations of the conduct. However, by modifying the provisions of Sections 230 to 232 of the Criminal Code, it would be possible to achieve greater accuracy, clarity and thus legal certainty in relation to cybercrime.

Keywords: cybercrime, attack, denial of service