Legislativní pohled na napadání sítí v České republice

Vložil/a czokl [1], 22 Červenec, 2010 - 17:29

- Hacking [2]

V jednom svém školním projektu jsem zpracovával téma tykajícího se legislativního pohledu na napadení počítačových sítí. Zabýval jsem se konkrétními modelovými případy, na kterých jsem demonstroval výklad trestního zákoníku. Rozhodl jsem se text zveřejnit pro veřejnost a tak máte nyní možnost se seznámit s výsledky mého snažení.

Ještě než se pustíte do čtení, rád bych upozornil na skutečnost, že nemám žádné právnické vzdělání ani jsem text s žádnou osobou znalou práva nekonzultoval. Jde tedy čistě o můj subjektivní výklad trestního zákoníku, tykajícího se zločinů spachaných pomocí počítače. Proto tento text neberte nijak směrodatně, pouze informativně.

Napadání počítačových sítí v ČR

Kazuistika a konkrétní legislativní rámec

20.4.2010

Abstrakt

Tato práce se zabývá legislativou napadání počítačových sítí v ČR. V úvodu práce jsou vysvětleny pojmy v zadání (napadení sítě,
kazuistika). Dále jsou představeny konkrétní § trestního zákoníku, které definují trestní činnost v této oblasti a její postih. Největší
části práce jsou konkrétní demonstrační situace napadení sítě nebo koncových zařízení v sítí. Součástí každé situaci je uveden
komentář, která část trestního zákoníku postihuje uvedenou situaci, z čeho by mohl být pachatel obviněn a jaké tresty mu hrozí za
konkrétní neoprávněnou činnost.

Klíčová slova

napadení sítě, počítačová kriminalita, kazuistika, trestní zákon, hacker, cracker

1 Úvod

Nejdříve je potřeba zaměřit se na samotné zadání a vymezit, o čem tato práce bude pojednávat. Pojem napadení počítačové sítě znamená získání neoprávněného přístupu k počítačové síti nebo systému uvnitř této sítě. Lidé provádějící tuto činnost jsou často označováni pojmy hacker nebo cracker.

Pojem hacker má ve světě informatiky dva významy. První význam je pozitivní, například o zakladateli hnutí GNU (viz [5]) Richardovi Stallmanovi se často tvrdí, že je to poslední skutečný hacker. V takovém kontextu toto slovo vystihuje člověka velice znalého oboru. Druhý význam je negativní a v podstatě se slučuje s významem slova cracker. Označuje člověka, který překonáváním

bezpečnostních ochran připojuje do cizích počítačových systémů. V dalším textu bude tedy používáno pouze označení cracker, aby nemohlo dojít k omylu.

Systém uvnitř sítě může být libovolný síťový prvek (switch, router) umožňující vzdálenou konfiguraci nebo libovolný počítač v síti. Sítí nejsou myšleny pouze LAN sítě (lokální sítě o velikosti maximálně desítek počítačů), ale třeba i celosvětová sít internet.

Existuje mnoho různých způsobů, jak napadnout síť. Mezi nejčastější z nich patří přístup pomocí neoprávněně získaných přístupových údajů. Takové údaje lze získat například odposlechnutím nešifrované komunikace. Dalším velmi častým způsobem je využití chyby v programu chránící síť před neautorizovaným přístupem. Důvody jsou také různé, jedním z nejčastějších je distribuce spamu [2].

Pojem kazuistika má podle výkladového slovníku ABZ.cz [1] právnický význam: „Výklad práva se zřetelem ke konkrétnímu individuálnímu případu, (přen. knaccording.) formalistické překrucování, chytrácké odůvodňování“.

Tento článek bude pojednávat o právní úpravě ke konkrétním modelovým případům napadání počítačů, které jsou připojeny k síti (například celosvětové síti internet). Nebude se zabývat důvody ani technickými aspekty útoků, pokud nebude taková znalost potřebná pro výklad legislativy nebo pro objasnění konkrétního příkladu čtenáři.

2 Počítačová kriminalita a její současná úprava trestním zákonem

Informace v této kapitole pocházejí ze sumarizace (zaměřenou na počítačovou kriminalitu) trestního zákonu provedenou advokátem Tomášem Sokolem a universitním profesorem Vladimírem Smejkalem [3]. Nejdříve je potřeba definovat samotný pojem počítačová kriminalita. Počítačová kriminalita je souhrnný pojem pro následující trestní činnosti (převzato z [3]):

- protiprávní přístup,
- protiprávní zachycení informací,
- zásah do dat,
- zásah do systému,
- zneužití zařízení,
- falšování údajů souvisejících s počítači,
- podvod související s počítači,
- trestné činy související s dětskou pornografií,
- trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

Do 31.12.2009 platila v České Republice jediná norma, §257a trestního zákona (zákon č. 140/1961sb.). Od 1.1. 2010 platí nový trestní zákon č. 40/2009 sb. (on-line si lze celý trestní zákon prohlédnout například na [4]). Tato práce pojednává především o následujících § z tohoto zákona:

§230 – Neoprávněný přístup k počítačovému systému a nosiči informací - zabývá trestnou činností v průběhu napadení. To znamená,
že řeší situace, kdy útočník napadne síť, provede například nějakou škodu, ale informace dále nezneužije.
§231 – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat – doplněk k předchozímu, ošetřuje případy, kdy pachatel zneužije neoprávněně získané informace a nebo je poskytne třetí osobě.
§231 - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti – ošetřuje speciální případ, kdy zanedbání pravidel vede k poškození sítě (nejedná se tedy o napadení sítí útočníkem).

Všechny § jsou umístěny v hlavě V., která se týká trestných činů proti majetku, napadnutí sítě tedy majetková trestná činnost. Ačkoli data nepředstavují hmotný majetek, poškození dat může vést ke

ztrátě hmotného majetku.

Výše uvedené § trestního řádu nejsou jediné, za který může být pachatel trestně stíhán v souvislosti s nějakým útokem popsaným níže. Ale jsou jediné, které se přímo zabývají napadáním informačním systémů, proto se práce zabývá pouze jimi.

3 Kazuistika

Aplikace práva z výše představených § bude předvedena na příkladech. Každý se skládá ze dvou částí. První částí je popis modelové situace (všechny údaje uváděné v práci jsou smyšlené a nemají žádnou návaznost na skutečné události). Druhá část se týká legislativy
a popisuje právní dopady takového jednání. V jednom příkladě se tyto dvě části opakují, nejdříve je popsána základní situace, která je potom upravena nebo rozšířená o další detaily.

Ještě bych rád upozornil na fakt, že výklad práva vždy záleží na konkrétní situaci, případně schopnostech účastníků právních řízení, proto i v případě realizace některého z modelových příkladů by mohl být prokázán například jiný trestný čin, než je uvedeno v této práci. Příklady slouží výhradně jako demonstrace k jednotlivých § trestního zákona.

3.1 Příklad 1 – Neoprávněná autorizace

V tomto příkladě vystupují tři subjekty, subjekt BFU (běžný Franta uživatel), útočník A a S , webový server uvnitř privátní sítě, na kterém má BFU svoje personální stránky. Webový server je přístupný z vnější sítě pro protokol HTTP a z vnitřní sítě pomocí
protokolu FTP. Subjekt A získá neoprávněným způsobem přístupové údaje subjektu BFU k privátní síti a subjektu S. Subjekt A se k serveru S připojí pomocí protokolu FTP . Zjistí, že uživatel BFU tam nemá kromě pár statických HTML stránek žádná data, odpojí
se a přístupové údaje zapomene.

V takovém případě se subjekt A dopustil trestného činu podle §230, odst. 1 trestního zákona. Pokud by se zjistilo, že útočník A takové napadnutí provedl (citace z výše zmíněného zákona): „...bude potrestán odnětím svobody až na jeden rok, zákazem činnosti
nebo propadnutím věci nebo jiné majetkové hodnoty“.

Útočník A zajde dále a pozmění soubor index.html (tento soubor se návštěvníkovi webu zobrazí když zadá pouze adresu webu).
Obsah souboru smaže a vepíše do něj „Hacked by A“.

Nyní se již dopustil trestného činu i ve smyslu odst. 2 písm b) a d) stejného § a nyní mu hrozí odnětí svobody na dva roky, zbylé formy postihu zůstávají stejné.

3.2 Příklad 2 – Zneužití chyby ve webové aplikaci krajského soudu

V dnešní době je velká část dat dostupná přes webové aplikace. Mezi crackery je populární jejich napadání. V §230, odst. 1 trestního zákona se píše přesně: „Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části“. Důležitá je zde poslední část citace, tedy, že získání neoprávněného přístupu pouze k části systému, například webové aplikaci, je trestný čin. Navíc se může stát, že díky chybě ve webové aplikaci a nedostatečnému nastavení práv může útočník získat přístup k celému počítači nebo celé síti.

Existují dva subjekty, webová aplikace krajského soudu WA a útočník A. Útočník díky chybě ve webové aplikaci vloží na server svůj vlastní skript, pomocí něho dostane přístup k příkazové řádce s právy administrátora. Dále uhádne administrátorské heslo, změní ho a server vypne. Tím znemožní přístup k webovému serveru krajského soudu po několik hodin.

Pachatel se v takovém případě spáchal trestný čin ve smyslu §230 odst. 1, 2 písm. b) a d) a dokonce odstavce 4 písmene c), kde se píše „způsobí-li takovým činem vážnou poruchu v činnosti orgánu

státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci„. Odstavení serveru na několik hodin by se dalo považovat za vážnou poruchu, za to pachateli hrozí odnětí 1 až 5 let nebo peněžitý trest. Pokud by ovšem porucha nijak činnost krajského soudu neovlivnila, hrozil by útočníkovi stejný trest jako v příkladě 1.

3.3 Příklad 3 – Neoprávněné připojení k internetu

V tomto příkladě figuruje bezdrátová síť WIFI a útočník A a uživatel BFU. WIFI je připojena k síti internet. Je zabezpečena slabým šifrovacím algoritmem, který útočník prolomí a získá tak přístupové informace k této síti. Útočník A začne využívat WIFI pro
připojení k síti internet a přístupové údaje poskytne uživateli BFU.

Útočník A se v této chvíli dopustil trestného činu ve smyslu §230 odst. 1, 2 písm a), dále odst. 3) písm. a), protože získá prospěch tím, že využívá síť internet zadarmo (plátcem je poškozený vlastník WIFI), navíc tak páchá škodu poškozenému. Útočník by mohl
tímto jednáním spáchat trestný čin stejného § odst. 3 písm b), protože by mohl omezovat ostatní uživatele na síti (například stahováním dat). Pokud by takovou síť používal delší dobu, dopustil by se trestného činu stejného § odst. 4 písm. b) a d), kde je
uvedeno: „způsobí-li takovým činem značnou škodu“ resp: „získá-li takovým činem pro sebe nebo pro jiného značný prospěch“.

V článku [3] je uvedeno: „podle § 138 trestního zákona se značnou škodou rozumí škoda dosahující částky nejméně 500 000 Kč“, ačkoli tato částka by byla asi jen těžko prokazatelná. Prokazatelné je ale spáchání trestného činu ve smyslu §231 odst. 1 písm. b). V tomto případě lze útočníka potrestat (citace z odstavce zákona): „odnětím svobody na jeden rok, propadnutím věci nebo jiné majetkové hodnoty“. Uživatel BFU ovšem podle výše uvedených § trestně odpovědný není.

Dejme tomu, že uživatel BFU není jeden, ale velká skupina nelegálních odběratelů, kteří ovšem nevědí nic o tom, že porušují zákon. Internet „kupují“ od útočníka A stejným způsobem, jako od klasického poskytovatele připojení, který nelegálně využívá přípojku
internetového poskytovatele nebo velké společnosti.

V takovém případě je samozřejmě již částky 500 000 Kč dosáhnout, potom může být pachatel potrestán (citace z §231 odst. 4): „Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty“.

3.4 Příklad 4 - Pharming

Pharming označuje internetový podvod – podstrčení falešné webové stránky místo skutečné. První částí podvodu je napadení lokálního DNS serveru (služba DNS se stará o překlad doménových jmen na IP adresy a nazpátek) na stíti nebo jiný způsob přenastavení překladu doménových jmen na IP adresy. Útočník změní tento překlad tak, aby se po zadání doménového jména webový prohlížeč připojoval na server útočníka a nikoli na skutečný. Útočník na svém serveru udělá kopii webových stránek ze skutečného serveru, takže uživatel nemá na první šanci zjistit, že jde o podvod.

Zde vystupuje pět subjektů. Server pro překlad adres DNS, útočník A, uživatel BFU, internetový obchod elektronikou ES a útočníkův server AS. BFU má nastaven jako server pro překlad doménových jmen na adresy server DNS. útočník tento server napadne a zajistí, že požadavky na doménové jméno obchodu ES budou směřovat na server AS. Na tom má útočník připravenou identickou kopii internetového obchodu. Uživatel si v obchodě chce zakoupit zboží, útočník tak získá přihlašovací údaje, provede nákup v obchodě, ale zboží nechá zaslat sobě.

V tomto případě porušil zákon ve smyslu §230 odst. 2 písm. c), kde stojí, že pokud pachatel, cituji: „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“, což je naplněno tím, že pozmění data na DNS serveru. Dále lze pachatele žalovat ve smyslu odst. 3 písm. a) z důvodu způsobení ujmy uživateli BFU. Za to mu hrozí peněžitý trest, odnětí svobody na šest

měsíců až tři roky nebo propadnutí majetku.

3.5 Příklad 5 – DoS a DDoS

DoS je typ útoku, kdy útočník zahltí server požadavky a nebo využije chybu v programu, která zapříčiní pád služby nebo celého serveru. Tím odepře službu provozovanou na serveru. DDoS je distribuovaná verze DoS. To znamená, že útočník posílá požadavky
serveru z více počítačů. Pokud jich má k dispozici dostatečný počet, i korektními dotazy může server zahltit a ten není schopen obsloužit korektní uživatele služby.

V tomto příkladě vystupuje vystupují tři subjekty, server S patřící komerční společnosti, útočník A a napadená síť NET, kterou ovládá útočník. Útočník nainstaloval na všechny počítače v síti NET software, pomocí kterého ovládá hromadně počítače. V jeden okamžik všechny počítače začnou odesílat sekvence SYN paketů na server S, čímž ho zahltí. Tím odepře službu běžným uživatelům serveru S. Útok neprovede jednorázově, ale pravidelně každou hodinu způsobí několika minutový výpadek na serveru. Takto útočí na server opakovaně po dobu dvou měsíců.

Tímto činem útočník A spáchá trestný čin ve smyslu §230 odst.3 písm b), kde se píše, že pokud měl útočník: „v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.“. Jelikož útok není jednorázový a evidentně poškozuje komerční společnost, dopustil se ještě trestného činu ve smyslu stejného § odst. 4 písm. e), která přesně takovou situaci ošetřuje. Útočníkovi pak hrozí trest odnětí svobody na jedno až pět let nebo peněžitý trest.

3.6 Příklad 6 – Programátor testuje aplikaci na produkčním serveru

V tomto příkladě se nejedná o napadení počítačové sítě v pravém slova smyslu, protože zde chybí útočník. Jde o poškození sítě či její části z nedbalosti. Vystupují zde dva subjekty, programátor R a produkční server S. Programátor R právě dokončil úpravy na
aplikačním serveru, který jeho společnost provozuje. Upravenou verzi nepředal QA oddělení (quality assurance – oddělení kontroly kvality), ale rovnou jí nasadil na produkčním serveru. Tím urychlil nasazení novinky, na které pracoval. Ale ve zdrojovém kódu bylo několik chyb, které zapříčinili pád systému a celé sítě. Ta sloužila jako interní síť důležitého světového přístavu a než se podařilo systém obnovit do původního stavu, musel přístav přerušit svůj provoz. Díky tomu přišel přístav o zisk v hodnotě deseti miliónů korun.

Zaměstnanec se dopustil nedbalosti. Zákon definuje nedbalost následujícím způsobem (převzato z [3]):“§ 16 Nedbalost (1) Trestný čin je spáchán z nedbalosti, jestliže pachatel
a) věděl, že může způsobem uvedeným v trestním zákoně porušit nebo ohrozit zájem chráněný takovým zákonem, ale bez přiměřených důvodů spoléhal, že takové porušení nebo ohrožení nezpůsobí, nebo

b) nevěděl, že svým jednáním může takové porušení nebo ohrožení způsobit, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl.

(2) Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem." Zaměstnanec se tedy podle §16 odst.2 dopustil hrubé nedbalosti. Poškození počítačového systému (například sítě) ošetřuje §232. Programátor se dopustil trestného činu ve smyslu odst. 1 písmene a), a protože škoda přesáhla částku 5 000 000, dopustil se trestného činu podle odst. 2 stejného §.Tam je uvedeno, cituji (z §232 odst. 2): „Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.“. Programátor může tedy strávit až dva roky za mřížemi.

3.7 Příklad 7 - Vyrobení programu typu červ

Červ je zvláštní typ škodlivého software, který zpravidla využívá chybu v zabezpečení systému nebo

konkrétní chyby v programu, pomocí které se šíří sítí a napadá jednotlivé počítače. Tyto programy v sobě pak často mají různé rutiny, například v jednotný den
a čas odesílají požadavek na určitý server a provádějí tak DDoS útok.

V tomto příkladě vystupuje subjekt autor červu A. Ten nalezne v operačním systému Windows chybu a napíše pro něj již zmíněný program typu červ. Kromě vlastní funkce napadání počítačů zapojených v síti má v sobě naprogramován náhodný restart stroje. To
znamená, že po startu stroje program vygeneruje náhodné číslo a za tento vygenerovaný počet minut se počítač vypne. Červ se snadno rozšíří po celém světě, kde působí značné potíže.

Pachatel spáchal trest ve smyslu §231 odst. 1 písm. b), za který mu hrozí odnětí svobody až na jeden rok nebo majetková ujma. Další trestné činy záleží na prokázané škodě. Protože se červ rozšířil po celém světě, může být trestně odpovědným ve stejném § odst. 2 písm. b) nebo dokonce odstavci 3. V prvním případě by musela škoda překročit 500 000 Kč, v druhém 5 000 000 Kč. Pokud by se tento poslední scénář naplnil (což je velmi pravděpodobné), je vrchní hranice trestu odnětí svobody na pět let.

3.8 Příklad 8 – napadení počítačové sítě velké společnosti skupinou útočníků

Crackeři často nepracují osamoceně, ale ve skupinách po vzoru rčení „víc hlav víc ví“. V posledním příkladě vystupuje jako jeden subjekt skupina crackerů C a počítačová síť velké společnosti, například pojišťovny. Crackeři napadnou síť pojišťovny a odnesou si
databázi klientů. Na svém webu potom zveřejní část seznamu a prozradí i rozluštěná hesla správců sítě pojišťovny.

V tomto případě pachatelé spáchali trestný čin ve smyslu §230 odst. 4. a), který pokrývá odst. 1 a 2, s tím, že zločin provedl člen organizované skupiny. Za to hrozí trest ve výši až pěti let nebo peněžní pokuta. Dále mohou být, v případě dopadení, pachatelé
obžalování pro spáchání trestného činu ve smyslu §231 odst. 2 písm. a), protože pachatelé naplnili skutkovou podstatu trestného činu ve smyslu stejného § odst. 1 písm. b) a pachatelem je jeden z členů organizované skupiny. Za to hrozí pachateli propadnutí majetku, zákaz činnosti a nebo vězení ve výši až třech let.

Crackeři ale často nenapadají sítě pouze pro samotný akt napadení, často tuto činnost provádějí kvůli zisku z prodeje ukradených dat. Příklad bude tedy upraven tak, že crackeři se rozhodli odcizený seznam klientů prodat konkurenci za cenu přesahující částku pět miliónů korun českých.

Prodejem dat rozšířili množinu spáchaných trestných činů o odst. 5 písm b) prokazatelně, protože získali ve svůj prospěch velkého rozsahu (nad 5 000 000 Kč). Dále by mohli být žalování ve smyslu písmene a), protože tím zdiskreditovali pojišťovnu a ta potom v
důsledku útoku může přijít o částku přesahující pětimilionovou hranici. Tím hrozí pachatelům odnětí svobody na tři až osm let. Dále by mohli být obviněni z trestného činu ve smyslu §231 odst. 3 ze stejného důvodu. Za to pachatelům hrozí trest odnětí svobody na šest měsíců až pět let.

4 Závěr

Tento článek měl posloužit jako přehled legislativního rámce při napadání počítačových sítí. Netýká se ovšem pouze a jenom napadení sítě, ale i dalších praktik s nimi souvisejících. Snahou autora bylo představit několik běžných typů útoků a jejich ošetření trestním zákonem. Jednotlivé § byli představeny na základě situací, které byli sestavovány se zřetelem na reálné případy.

Samotný akt napadení cizího počítače nebo sítě není českou legislativou trestán příliš přísně (za napadení je horní hranice trestu jeden rok odnětí svobody). Trestní zákon se zaměřuje více na to, jak pachatel s daty získanými při napadení sítě naloží. Počítačová
kriminalita je součástí majetkové trestné činnosti, čím větší škoda je napáchána poškozenému, tím vyšší trest si pachateli hrozí. Zákon neopomíná ani skupinovou trestnou činnost, s tím jak roste její

společenská nebezpečnost roste i horní hranice trestů.

Osobně mě mírnost trestů, většina trestů nabízí kromě odnětí svobody i alternativní řešení v podobě pokut, postoupení majetku či zákazu činnosti. Až nejtěžší tresty, kdy dochází k velkým škodám (které lze dle mého názoru v naprosté většině případů velmi
obtížně dokázat) hrozí pachateli odnětí svobody řádově několika let. Na druhou stranu je zajímavé zjištění, že jakýkoli neoprávěný přístup alespoň do části cizího systému už může být klasifikován jako trestný čin.

5 Literatura

[1] ABZ : slovník cizích slov [online]. 2006 [cit. 2010-04-20]. Pojem kazuistika. Dostupné z WWW: .
[2] KRUTÝ, Karel. Napadené počítače stále častěji slouží k rozesílání spamu. PCWorld [online]. 13.05.2009, [cit. 2010-04-20].
Dostupný z WWW: .
[3] SOKOL, Tomáš; SMEJKAL, Vladimír. Postih počítačové kriminality podle nového trestního zákona. Právní rádce [online].
22.7.2009, n. 5, [cit. 2010-04-20]. Dostupný z WWW: .
[4] Zákon č. 40/2009 Sb.. 2009. Dostupný také z WWW: .
[5] The GNU Operating system [online]. 2010 [cit. 2010-04-23]. The GNU Operating system. Dostupné z WWW: .

Text naleznete také v přiloženém PDF.

URL článku:
https://security-portal.cz/clanky/legislativn%C3%AD-pohled-na-napad%C3%A1n%C3%AD-s%C3%ADt%C3%AD-v-%C4%8Desk%C3%A9-republice

Odkazy:
[1] https://security-portal.cz/users/czokl
[2] https://security-portal.cz/category/tagy/hacking