Univerzita Pardubice

Fakulta ekonomicko-správní

Rizika elektronického terorismu

Adéla Jedličková

Bakalářská práce
2013

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Adéla Jedličková**
Osobní číslo: **E10831**

Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Management ochrany podniku a společnosti**
Název tématu:	**Rizika elektronického terorismu**
Zadávající katedra:	**Ústav regionálních a bezpečnostních věd**

Zásady pro vypracování:

Práce se bude zabývat obecnou problematikou terorismu a specificky terorismem elektronickým. Dále bude obecně popsáno tržní prostředí akciových společností a jeho současný stav z hlediska napadení elektronickým terorismem. Bude analyzována míra napadení v rámci akciových společností. Na závěr budou uvedeny hlavní poznatky a případná doporučení.

Problematika terorismu obecně.
Soudobé projevy terorismu.
Akciové trhy obecně.
Elektronický terorismus a současné společnosti.
Analýza dopadů elektronického terorismu na tržní ocenění společností.
Hlavní poznatky a doporučení.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 30 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

COLARIK, M., Andrew. Cyber Terrorism : Political and Economic Implications. 1st Edition. London : IGI Publishing, 2006. 172 s. ISBN 978-1599040219.
JIRÁK, Jan, KÖPPLOVÁ Barbara. Média a společnost : Stručný úvod do studia médií a mediální komunikace. Vyd. 1. Praha : Portál, 2003. 208 s. ISBN 80-7178-697-7.
KISLINGEROVÁ, Eva. Oceňování podniku. 2. přepracované a doplněné vyd. Praha : C. H. Beck, 2001. 367 s. ISBN 80-7179-529-1.
KUBANOVÁ, Jana. Statistické metody pro ekonomickou a technickou praxi. 2. vyd. Bratislava : Statis, 2004. 249 s. ISBN 80-85659-37-9.
MUSÍLEK, Petr. Trhy cenných papírů. 2., aktualiz. a rozš. vyd. Praha : Ekopress, 2011. 520 s. ISBN 978-80-86929-70-5 (váz.).

Vedoucí bakalářské práce: **doc. Ing. Radim Roudný, CSc.**
Ústav regionálních a bezpečnostních věd

Datum zadání bakalářské práce: **30. září 2012**
Termín odevzdání bakalářské práce: **30. dubna 2013**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Ivana Kraftová, CSc.
vedoucí ústavu

V Pardubicích dne 3. října 2012

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 30. června 2013 Adéla Jedličková

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala svému vedoucímu práce, kterým je doc. Ing. Radim Roudný, CSc. za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce. Dále bych zde chtěla poděkovat svým blízkým a rodině, kteří mě podporovali po celou dobu mého studia.

ANOTACE

Práce se bude zabývat obecnou problematikou terorismu a specificky terorismem elektronickým. Dále bude obecně popsáno tržní prostředí akciových společností a jeho současný stav z hlediska napadení elektronickým terorismem. Bude analyzována míra napadení v rámci akciových společností. Na závěr budou uvedeny hlavní poznatky a případná doporučení.

KLÍČOVÁ SLOVA

Terorismus, útok, společnost, akcie, hodnota, cena, riziko

TITLE

Risks of cyber terrorism

ANNOTATION

The work will address the general issue of terrorism and specifically electronic terrorism. Furthermore, the market environment is generally described corporations and its current status in terms of electronic attack terrorism. It analyzed the rate of infestation within corporations. At the conclusion will be the main findings and any recommendations.

KEYWORDS

Terrorism, attack, company, share, value, price, risk

OBSAH

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM ZKRATEK

ČR	Česká republika
EU	Evropská unie
FES	Fakulta ekonomicko-správní
a. s.	Akciová společnost
KKK	Ku-klux-klan
THA	tržní hodnota akcie
ČS	Česká spořitelna
ČSOB	Československá obchodní banka
KB	Komerční banka

ÚVOD

Téma práce bylo vybráno vzhledem k významu kybernetického terorismu v současnosti a dále proto, že se o toto téma zajímám.

Tato práce se zabývá terorismem obecně, dále uvádí základní informace o akciových trzích a konkrétní informace o akciových trzích přímo v České republice. V další kapitole pojednává o elektronickém neboli kybernetickém terorismu, dále si vysvětlíme, kdo je pachatelem kybernetického terorismu a jakým způsobem se toto děje. V praktické části se práce zabývá již uskutečněnými kybernetickými útoky, které se svým charakterem řadí do kategorie elektronického terorismu. Tyto útoky jsou rozebrány a zanalyzovány. Zjišťujeme, zda tyto kybernetické útoky měly nebo stále ještě mají vliv na akciové společnosti, které se pohybují na burze cenných papírů a hlavně, zda mají nějaký vliv na tržní hodnoty akcií těchto společností. Jsou tedy sledovány tržní hodnoty akcií společností a jejich pohyby.

Obecná část práce byla zpracována na základě literárního průzkumu, další, praktická část má induktivní charakter a vychází z dat získaných z internetu.

Cílem práce je obecný popis terorismu, zejména terorismu kybernetického a jednoduchý popis trhu s akciemi. Dalším cílem je zjištění jak kybernetické útoky ovlivňují hodnoty akcií vybraných institucí v ČR a v zahraničí.

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

V této kapitole se zaměříme na definici a cíle terorismu, dále na historii terorismu. Další důležitou podkapitolou jsou ideologie terorismu, typy terorismu a hlavně používané metody terorismu.

1.1 Definice a cíle terorismu

Terorismus je podle jedné z definic vymezen jako předem připravené, politicky motivované násilí směřující proti civilním a jiným cílům, osobám či skupině osob, prováděné extremistickými skupinami nebo jednotlivci se snahou zastrašit, způsobit značnou škodu nebo usmrtit osoby k dosažení politického cíle. [13]

Další definice říká, že jde o organizované použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím mají být splněny politické, náboženské nebo ideologické požadavky jak ve vnitrostátním, tak v mezinárodním měřítku. [22]

Podle jiné definice je terorismus plánované použití násilí nebo hrozby násilí, zpravidla zaměřené na širokou masu nezúčastněných lidí. Cílem je vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus obsahuje i kriminální zločiny, které jsou však jen cestou k dosažení jiných cílů, než na který je kriminální čin zaměřen. [8]

Prvotním cílem terorismu je působení na psychiku lidí, a to prostřednictvím strachu. Nezúčastnění lidé jsou v teroristických akcích zabíjeni jenom proto, že existují a že jejich smrt může být psychologicky a politicky využita. Nerespektuje žádné geografické a politické hranice. Boj proti němu tedy musí být na široké, celospolečenské frontě a na mezinárodní úrovni. Pouze spolupráce mezi státy, vládami a jejich institucemi může přinést pozitivní výsledky. Boj proti terorismu však nelze omezit pouze na technickou stránku věci, za kterou odpovídá policie nebo vládní úřady. Strategickým cílem musí být odstranění jeho příčin, tzn. stabilizovaná a prosperující společnost. Dosažení takového cíle je tedy pouze ideálem, ke kterému se můžeme více či méně přiblížit. Z tohoto důvodu nelze boj s terorismem nikdy vyhrát. Vzestup či pokles vlny terorismus je citlivý barometr stavu dané společnosti.

Cíle útoků jsou vybírány tak, aby jejich napadení vyvolalo masový a dlouhodobý zájem informačních médií se zajištěním maximální publicity. K překonání obranných opatření využívají momentu překvapení. Správně načasovaný a dobře naplánovaný útok může prakticky překonat každou ochranu. K tomu ovšem musí mít teroristé dostatek přesných

informací, prostředků a technické zázemí. [21]

1.2 Historie terorismu

1.2.1 Raný terorismu

Rané skupiny spojované s terorismem byly vedeny náboženskými pohnutkami a operovaly primitivními zbraněmi. V prvním století našeho letopočtu se do dějin terorismu zapsala židovská náboženstvo-politická skupina zélotů-sikariů, která existovala patrně pouze několik desítek let. Aktivita zélotů-sikariů byla ve svém důsledku kontraproduktivní, jejich metody kruté - připomínající dnešní teroristy vedené náboženským fanatismem. O sedm set let později se do dějin terorismu zapsali thugové - indická hinduistická sekta aktivní od 7. do poloviny 19. století. V 90. letech 19. století sekta zcela ukončila svou činnost a dnes už je pouze námětem mnoha filmů a knih. Mezi nevýznamnější teroristické skupiny zaštiťující se náboženstvím, ale rovněž sledující politické cíle, patřili tzv. asasíni. David Morgan je označuje za příslušníky "vražedné sekty, která vyvíjela činnost v oblasti Perského zálivu zhruba od 11. do 13. století." [6]

Velká francouzská revoluce přivedla v letech 1792-1794 k moci vůdce frakce jakobínů a propagátora tzv. régime de la terreur Maximiliena Robespierra. Robespierrův režim přinesl světu negativně vnímaný pojem "terorismus" spjatý se státním režimem, teprve později užívaný pro "revoluční nebo protivládní projevy vykonávané nestátními nebo subnárodními objekty." [6]

1.2.2 Terorismus v 19. a na počátku 20. století

Až v poslední třetině 19. století převzaly teroristické praktiky nejrůznější, převážně sekulární skupiny. V etapě tzv. sekulárního terorismu konce 20. století se objevovaly nové pohnutky teroristů, částečně navazující na francouzskou revoluci. Anarchistické hnutí v Rusku bylo opakem Karlu Marxovi, nejvíce v té době rozšířené v Rusku. Nahlíženo historickým členěním W. Laqueura je anarchistické, nacionalistické či nihilistické násilí konce 19. století tzv. druhým obdobím rozvoje terorismu. [6]

Pod vlivem radikálních myšlenek na změnu zřízení vznikaly nejrůznější anarchistické skupiny především v carském Rusku. Tak jako ve své době asasíni prostřednictvím veřejně páchaných vražd, také stoupenci ruských anarchistů o osm století později chápali, jak důležitá je publicita. Mezi nejvýznamnější organizaci patřila skupina Narodnaja volja, jejímž

nejvýraznějším činem bylo zavraždění ruského cara Alexandra II. roku 1881. Tato etapa anarchistického, nacionalistického a nihilistického násilí končí podle D. Rapoporta atentátem na Františka Ferdinanda d´Este, který byl spáchán v roce 1914 organizací Černá ruka. [6]

S teroristy se ve druhé polovině 19. století potýkala nejen Evropa, ale také Amerika, kde po americké občanské válce patřila mezi nejvýraznější organizace ultrapravicová teroristická skupina Ku-klux-klan (KKK). Podle D. Rapoporta byl rozdíl mezi KKK a například ruskými anarchisty v tom, že myšlenky ruských teroristů měly vliv i na další organizace v jiných státech, kdežto vliv KKK se omezil na USA. V době první světové války začala tzv. druhá éra klanu, který se nyní zaměřil proti katolíkům či Židům. Další rozmach klanu pokračoval v polovině 50. let jako reakce na snahy o zrušení rasové segregace. Vliv KKK však v té době již upadal a ztrácel podporu veřejnosti. [6]

Teroristé konce 19. a začátku 20. století podle D. Rapoporta nikdy zcela nedosáhli svých cílů. Ve své činnosti využili nové populární ideologie, jako byl marxismus, anarchismus a nacionalismus. Na průběh tzv. první vlny terorismu měl významný vliv také rozvoj technologií, které zrychlily komunikaci a teroristickým útokům dodaly větší publicity. [6]

1.2.3 Terorismus 60. a 70. let 20. století

Psychologické předpoklady pro vznik třetí vlny „nové levice“ vytvořila podle D. Rapoporta vietnamská válka.

Jednu z nejvýraznějších skupin subverzivního subrevolučního terorismu vycházející z ultralevicových pozic představují italské Rudé brigády, jejichž aktivita započala na podzim roku 1970. Do této skupiny, která staví na ideologii marxismu-leninismu, řadí H.Henderson také francouzskou Přímou akci (Action Directe) a německou frakci Rudé armády (Rote Armee Fraktion), rovněž nazývanou skupina Baader-Meinhofové, která se nevyhýbala ani čistě kriminálním činům, aby si zajistila finanční zdroje. [6]

1.2.4 Současný terorismus

Poslední etapu v historii terorismu D. Rapoport nazývá náboženskou vlnou. Novinkou ve čtvrté vlně jsou sebevražedné útoky. Právě takovým způsobem byl mimo jiné také zavražděn indický premiér Radžív Gándhí v roce 1991 teroristickou organizací Tygři za osvobození tamilského Ílamu ze Srí Lanky (Tamilští tygři). [6]

Nábožensky motivované skupiny se začaly objevovat v 80. letech i v rámci arabsko-izraelského konfliktu. Mezi ty patří například skupina Islámský džihád či Hamás, který vznikl

v roce 1987 a podílí se na politických i teroristických aktivitách. Další organizací je šíitská libanonská skupina Hizballáh (Strana Boží), která vznikla z iniciativy, ale podporu získávala i ze strany Sýrie. Hizballáh proslul zejména používáním atentátníků – sebevrahů. [6]

Do kategorie náboženského terorismu patří rovněž náboženská sekta Óm šinrikjó, která v roce 1995 provedla za použití nervového plynu sarin útok na tokijské metro.

V 90. letech začalo rovněž působit v současné době nejznámější teroristické organizace al-Káida, která stojí například za útok na Světové obchodní centrum v New Yorku v roce 1993. Na svědomí má rovněž zřejmě nejvýznamnější teroristický útok v dějinách na New York a Washington dne 11. září 2001.

Novou a zatím poslední etapu terorismu zaznamenává také J. Šedivý. Ve svém členění ji časově identifikuje s koncem studené války a nachází v ní tzv. nový typ terorismu. [6]

1.3 Ideologie terorismu

1) *Menšinové a národnostní skupiny*

   - podporují náboženské nebo národnostní menšiny v konfliktu s dominantní kulturou.

2) *Marxistické a krajně levicové skupiny*

   - založeny na ideologii myšlenkově vycházející z děl K. Marxe a B. Engelse s celou řadou odchylek.

3) *Anarchistické skupiny*

   - nemají pevnou ideologickou orientaci nebo cíl, jsou zaměřeny pouze na destrukci existujícího systému.

4) *Neonacistické a krajně pravicové skupiny*

   - útoky zaměřené proti cizincům a přistěhovalcům. Jejich motivem je rasová nesnášenlivost, zdůvodněná nacistickou ideologií.

5) *Psychopatické (patologické) skupiny*

   - činy psychopatů jsou převážně činem jednoho člověka.

6) *Skupiny s náboženskou motivací*

   - za těmito náboženskými cíli jsou většinou skryty naprosto chladně prokalkulované politické cíle. [21]

1.4 Typy terorismu a nejčastější typy teroristických útoků

1.4.1 Typy terorismu

Z hlediska základního stanovení hrozeb a jejich předcházení je třeba stanovit především motivaci teroristů. Podle motivace je možné vypracovat typologii terorismu, která zahrne i ”nepolitické formy” terorismu:

1) *Terorismus kriminální*

   - teroristické akce provedené primárně za účelem získání osobních materiálních výhod.

2) *Terorismus patologický*

   - teroristické akce provedené primárně kvůli psychickému sebeuspokojení.

3) *Terorismus politický, resp. ideologický*

   - akce provedené z kolektivních pohnutek bez hledání přímých materiálních výhod.

   Tuto kategorii lze dále dělit na:

- Ultralevicový terorismus
- Ultrapravicový terorismus
- Etnický terorismus
- Náboženský terorismus
- Environmentální terorismus
- Vigilantistický terorismus (kterému jde o ”právo a pořádek”, který údajně není stát s to zajistit, sem lze řadit například latinskoamerické ”černé brigády”, útočící proti bezdomovcům atd.)
- ”Single-issue” terorismus (”jednopoložkový” - proti potratům atd.)

Co do rozsahu působení terorismu existuje kategorie domácího terorismu a mezinárodního terorismu, související s počtem zemí, v nichž terorismus působí anebo získává prostředky a logistiku pro svoji činnost. Nepřehlédnutelná je vazba terorismu na jiné negativní jevy, jakými je například obchod s drogami (ze kterého jsou teroristické akce nezřídka financovány) nebo obchod se zbraněmi. Společně s organizovaným zločinem a šířením zbraní

hromadného ničení patří terorismus – zejména jeho mezinárodní forma – k nejzávažnějším rizikům ohrožujícím celou lidskou civilizaci. [16]

1.4.2 Nejčastější typy teroristických útoků

- bombový - proti osobám, symbolickým cílům, významným cílům, série útoků;
- hrozba použití výbušného zařízení;
- atrapa výbušného systému;
- zadržení rukojmí, únosy;
- zastrašování, hrozby;
- vydírání;
- sabotáže a rozvratné operace;
- dezinformace a propaganda;
- vraždy významných osob a další. [16]

1.5 Teroristické metody

1.5.1 Klasické teroristické metody

1) *Střelba, použití sečných a bodných zbraní, ubití*

Tato metoda zahrnuje akce namířené do davu anonymních osob, akce zaměřené na konkrétní osoby (např.: politiky, ekonomické špičky, umělci, novináři), akce zaměřené na konkrétní národy či jiné skupiny osob (např.: Izraelci, vojáci, policisté)

2) *Výbuchy pum samy o sobě*

Cílem je místo samo a jsou namířené na nijak nevybírané budovy, nebo na místa, kde se shromažďuje mnoho lidí (např.: náměstí, supermarkety, zábavní parky, nemocnice), dále mohou být namířeny na konkrétní instituce (např.: zastupitelské úřady, soudní budovy, sídla politických stran, státní úřady), dále místa hojně navštěvovaná turisty, místa pohybu konkrétních osob, místa či budovy, které obývají či navštěvují konkrétní národy či skupiny osob (ubytovny, restaurace), dále zahrnují výbuchy, které mají za cíl vyvolat zmatek v době voleb a referend, výbuchy, které poškozují komunikační tepny (mosty, železnice, metro, letiště, vodovody), útoky na samotné dopravní prostředky – letadla, vlaky, autobusy, lodě –

kde je cílem subjekt zničit, sabotáže, zamířené na ekonomické provozy (továrny, elektrárny, založené požáry lesů a polí).

3) *Výbuchy iniciující další ničivou činnost*

Zahrnují útok na chemické provozy, útok na jaderné provozy (jaderné elektrárny, školní reaktory, výzkumné závody – konvenční útok na tyto cíle je o mnoho snazší a levnější, než výroba či krádež atomové bomby, útok na vodní rezervoár (přehradu nebo protipovodňovou hráz) - riziko zaplavení velkých území, útok na místa koncentrace vysoce hořlavé hmoty, nesoucí s sebou znečištění životního prostředí, vyloučit nelze ani výbuch, který iniciuje lavinu či sesuvy půdy, zařadit sem lze snad i útoky na věznice, kdy uprchlí vězni mohou destabilizovat situaci v zemi.

4) *Únosy, braní rukojmí*

Únosy anonymních nebo konkrétních významných osob (spojené s dalšími požadavky - propuštění jiných teroristů), obsazení celé budovy a kladení požadavků.

5) *Různé formy násilí na turistech*

Útoky namířené na turisty, které mají za cíl poškodit zejména ty země, pro které je velkým přínosem cestovní ruch.

6) *Dopisní bomby*

7) *Další*

Útoky na umělecké památky v galeriích i jinde, poškozování provozuschopnosti vozidel, šíření zmatku, poplašné zprávy vedoucí k chaosu, při kterém dojde ke zranění či ušlapání lidí.

8) *Specifické cíle postmaterialistického a environmentálního (ekologického) teroru*

Ničení restaurací, útoky na lidi nosící kožichy, útoky na jatka, na laboratoře, v nichž provádějí pokusy na zvířatech, zatloukání hřebíků do kmenů stromů, aby nemohly být vytěženy dřevorubci. [16]

1.5.2 Moderní metody terorismu (užití zbraní hromadného ničení, kybernetický terorismus atd.)

Nové technologie, možnosti modelování na počítačích a další pronikavý rozvoj vědy a techniky vytváří podmínky pro urychlení výzkumu a vývoje. Zvláště na poli genového inženýrství, biologických a genových manipulací (tzv. klonování), ale i oblasti chemie a chemického průmyslu, jsou vytvořeny nebývalé předpoklady k tomu, že výsledky vědeckých

pokusů mohou být zneužity pro vojenství, respektive pro teroristické cíle. Zcela samostatnou rozsáhlou problémovou oblastí je kontrola používání a dopravy nebezpečných látek, včetně kontroly nebezpečných průmyslových odpadů. [16]

Některé zbraně hromadného ničení nebo jejich účinné součásti se tak mohou stát velmi účinným nátlakovým prostředkem při vydírání státních činitelů, státních institucí nebo i různých skupin obyvatelstva, průmyslových a zemědělských koncernů, i když by nedošlo k jejich přímému použití. Teroristé (či klasičtí zločinci) přitom počítají s využitím silně vypěstovaného strachu z použití zbraní hromadného ničení a jsou přesvědčeni, že držením takové síly donutí stát (či jiného protivníka) k přijetí svých požadavků. [16]

Pokud k útoku přesto dojde, mohou teroristé útočit, aniž by sami sebe museli vystavovat bezprostřednímu nebezpečí. Výsledné zamoření by pak přitom mohlo představovat i velmi dlouho trvající neobyvatelnost velkých rozloh území. Většina aktuálních dekontaminačních prostředků a praktik jakož i speciálního zařízení je konstruována koncepčně tak, že počítá s dekontaminací vojenské techniky a materiálu. To jsou zpravidla pevné povrchy z kovů, které jsou kryté speciálními nátěry proti korozi. Málo se však počítá s případy zasažení budov. [16]

Klasický terorismus je ve srovnání s užitím chemikálií, bakterií nebo počítačových virů více vidět. Moderní akcí se terorista tolik nezviditelní, i když při ní třeba zabije více lidí a zničí víc hodnot. Zatím se zdá pravděpodobnější, že drtivá většina teroristických skupin zůstane u klasických metod, které jsou hmatatelné, mohou zasáhnout přesně určený cíl a navíc okamžitě vyvolají pozornost sdělovacích prostředků. [16]

1) Jaderné technologie

Velké jaderné zbraně jsou technicky značným, ale nikoli nepřekonatelným problémem. Materiálně špatně zajištění atomoví vědci by se mohli k takovému výzkumu pro teroristy propůjčit. Jaderný materiál lze zakoupit na černém trhu, lze ho uloupit z úložišť vyhořelého odpadu či z likvidačních provozů raket. Riziko přináší možnosti krádeže munice obsahující ochuzený uran.

Zmínit je nutné i skutečnost, že výbuch malé atomové bomby asi 40 km nad povrchem Země může být zdrojem elektromagnetických vln, které by mohly zlikvidovat elektronické obvody družic, pozemních zařízení a veškerou elektrickou síť určitého regionu. Kapacitu pro vypuštění malé rakety do výšky 40 kilometrů má dnes už několik desítek států, z nichž některé jsou nepřáteli Západu. Žádný přírodní jev ani jakékoliv jiné atomové zbraně nemají na mikroelektroniku, na které je do velké míry založena moderní civilizace, tak dalekosáhlé

účinky. Odhady působení elektromagnetických vln se nedají předvídat. A proto je obtížné proti nim vytvářet ochranu celé infrastruktury. Elektromagnetické vlny jsou mimořádně intenzivní, ale působí krátce, a to v dohledu atomového výbuchu. Působením elektromagnetického záření by všechny kovové struktury, jako telefonní a elektrické dráty, rádiové a televizní antény i ploty mohly poškodit nebo zničit zařízení, která napájejí. Přitom novější a modernější systémy bývají zranitelnější než zařízení starší.

2) Biologické technologie

Biologickým terorismem rozumíme užití rozličných virů a mikrobů nebezpečných nemocí s úmyslem zasáhnout civilní populaci.

Biozbraň je pro teroristy i pro ”zločinné státy” levnější a "bezpečnější". Stačí vypěstovat bakterie a nenápadně je někde rozptýlit. Ve chvíli, kdy začnou účinkovat, jsou teroristé dávno v bezpečí. Některé nemoci mají dlouhou inkubační dobu, přenášejí se dále mezi lidmi a jejich výsledky mohou být strašlivé. Pro teroristy je spíše problémem, že při neoparné manipulaci mohou onemocnět sami.

Zdokumentovány jsou i případy kriminálních akcí, kdy zbraní byla injekční stříkačka, naplněná - podle pachatelů – krví infikovanou virem HIV. Vyloučit nelze ani záměrné zavlékání chorob, napadajících zvířata např.: BSE, slintavka, kulhavka atd.

3) Chemické technologie

Některé toxické látky, takové jako kyanovodík nebo nervově paralytické látky mohou způsobit smrt během několika minut po vypuštění a okamžitá lékařská pomoc je nezbytná.

Substance chemikálií jsou dostupné a levné, sloučeniny snadno vyrobitelné a přenosné, špatně detekovatelné a mají pro teroristy i jiné klady. Velmi nebezpečná – a pro teroristy lákavá – je tzv. binární chemická munice. V ní není obsažena otravná látka, ale pouze výchozí komponenty, které vytvoří vlastní otravnou látku až při dopravě munice na cíl nebo po explozi konvenční rozbušky.

Na pomezí chemických a biologických technologií se nacházejí – i realizované - případy, kdy teroristé (ale častěji zločinci, ekonomičtí konkurenti, vyšinuté osoby a sabotéři) otrávili některé potraviny v obchodech (jedy, průmyslovými chemikáliemi, bakteriemi).

Existuje obecně daleko vyšší pravděpodobnost použití biologických a ještě spíše chemických zbraní než zbraní jaderných. Dostupnost technologií těchto zbraní, relativně jednoduchá a levná výroba a možnost použití jednoduchých aplikačních metod vytvořily takovou situaci, že zneužití otravných látek, toxinů, virů a bakterií můžeme dnes očekávat

kdykoliv a kdekoliv na světě, a to z různých důvodů. Užití jaderných zbraní teroristy je podstatně méně pravděpodobné zejména proto, že:

- jaderná výbušnina je neobyčejně drahá;
- jaderná výbušnina je velmi obtížně dostupná;
- technologie výroby jaderných zbraní je stále relativně nejlépe utajovaná;
- rychlost detekce je velmi rozdílná: u radioaktivních látek je zjistitelnost okamžitá, u otravných látek je zjistitelnost od několika sekund do několika minut, a u biologických látek - dosud není uspokojivě vyřešena rychlá a spolehlivá detekce;
- výroba jaderných zbraní vyžaduje speciální materiály;
- existují zřejmě alespoň částečné morální zábrany pro užití jaderných zbraní;
- existují obavy, aby se manipulací s jadernými či biologickými zbraněmi teroristé nezabili sami respektive, aby nezamořili na dlouho prostor, kde se pohybují oni či jejich blízcí; u chemických zbraní je riziko smrti teroristy menší.

Chemické a biologické zbraně jsou v porovnání se zbraněmi jadernými podstatně levnější a jejich výroba není provázena technickými a technologickými potížemi, jako je to u jaderných zbraní. Navíc je možné celý proces přípravy a výroby chemických, biologických a toxinových zbraní podstatně lépe utajit, než je to u zbraní jaderných. Ani otázka dopravy těchto zbraní na cíl nečiní zvláštní potíže, neboť v nejjednodušším pojetí je možné předpokládat, že otravné látky, viry, bakterie, houby, plísně a toxiny mohou být do místa cíle dopraveny samotnými teroristy a zde použity tzv. diverzním způsobem - zamoření potravin, vody a vodních zdrojů, ventilačních šachet a ventilačního systému supermarketů a metra, vlakových a autobusových nádraží, apod.

Dále je třeba uvést, že značný rozsah produkce biologických látek může být proveden skrze fermentaci v relativně krátké době. Pouze malé množství biologické látky je potřeba k výrobě vhodného biologického zbraňového materiálu ve velkém množství. Užití práškovacích letadel nebo vrtulníků může sloužit jako velice efektivní dopravní systém pro použití chemických a biologických látek.

4) Zvukové zbraně

Málo prozkoumanou oblastí je nebezpečí, plynoucí z aplikace zbraní, které jsou založené na emitaci specifických zvukových (ultrazvukových, infrazvukových) frekvencí (vln). Tyto vlny mohou lidem způsobit fyziologické komplikace (bušení srdce, rezonanci tělních dutin a

tělních tekutin) a mohou mít i vliv na psychiku (uvedou lidi do apatie, nebo naopak vyvolají panické reakce). Výsledkem jejich užití může být i smrt velkého počtu osob. [16]

2 AKCIOVÉ TRHY

Akciové trhy jsou trhy, na kterých se obchoduje s cennými papíry, zejména s akciemi. Akcie jsou obchodovatelné cenné papíry, s nimiž jsou spojena práva akcionáře jako společníka podílet se na řízení společnosti (právo účasti a hlasování na valné hromadě akcionářů), na zisku společnosti (právo na dividendy) a na likvidačním zůstatku. [20]

Akcie fungují na rozdíl od dluhopisů jako dividendové cenné papíry, jejichž dividendový výnos není předem zaručen. Dokonce, i když je společnost zisková, management může navrhnout zadržení zisku za účelem tvorby fondů pro budoucí investice. [20]

2.1 Druhy akcií

Akcie je cenný papír představující podíl na vlastnictví akciové společnosti. Společnost vydává akcie za účelem získání peněz pro svůj vznik nebo rozvoj svých aktivit. [12]

Existují dva druhy akcií:

- Kmenové (běžné) akcie,
- Prioritní (preferenční) akcie.

Většina akcií je ve formě akcií kmenových. [12]

a) Kmenové akcie

Existují kmenové akcie obyčejné, ale kromě nich existují i jejich různé varianty:

- kmenové akcie „A“, které mají všechny znaky obyčejných kmenových akcií s tím rozdílem, že jsou spojeny s nižšími hlasovacími právy či jsou zcela bez hlasovacích práv, byly zavedeny z důvodu udržení hlasovacích práv ve společnosti v rukou určitých osob za současného vstupu jiných akcionářů (pro ně se emitují kmenové akcie „A“), jsou spojeny se stejnými dividendami jako obyčejné kmenové akcie, cena kmenových akcií „A“ je nižší než cena obyčejných kmenových akcií, což odráží jejich nižší status, a tudíž jejich výnosnost je vyšší.
- svolatelné akcie, které mají všechny znaky obyčejných kmenových akcií s tím rozdílem, že emitent je může za určitých okolností svolat, je možné je emitovat pouze v případě, že existují obyčejné kmenové akcie.
- akcie s oddálenou výplatou dividend, které mají všechny znaky obyčejných kmenových akcií s tím rozdílem, že nárok na výplatu dividend je oddálen až do

určitého okamžiku v budoucnosti, jsou levnější, v čemž se odráží jejich nižší status, a tudíž je jejich výnosnost vyšší.

- zakladatelské akcie, které se emitují pouze pro zakladatele společnosti. Někdy jsou s nimi spojena vyšší hlasovací práva než u obyčejných kmenových akcií. Kromě toho jejich vlastníci někdy mají nárok na minimální výši dividend. Emise zakladatelských akcií jsou výjimečné. [12]

b) Prioritní akcie

Prioritní akcie jsou hybridem mezi kmenovými akciemi a dluhem podniku. Při výplatě dividend, mají prioritní akcie přednost před akciemi kmenovými.

Kromě obyčejných (nekumulativních) prioritních akcií existují i jejich varianty:

- kumulativní prioritní akcie, které umožňují výplatu zadržených dividend z předchozích let, a to před výplatou dividend kmenovým akcionářům. Většina prioritních akcií je právě kumulativních.
- svolatelné prioritní akcie, které umožňují emitentovi jejich svolání.
- účastnické prioritní akcie, které poskytují držiteli možnost obdržet určitý podíl ze zisku společnosti po splacení stanovené částky jako dividendy kmenových akcií, při bankrotu společnosti akcionáři mohou mít také nárok na určitý procentní podíl z přebytku aktiv nad závazky.
- konvertibilní prioritní akcie, které jsou spojeny s právem majitele na konverzi na kmenové akci k určitému datu a za určitou cenu.
- hierarchické prioritní akcie jsou akcie, u nichž jedna emise prioritních akcií je při bankrotu nadřazena či podřízena jiným emisím prioritních akcií. [12]

V USA existují dva druhy prioritních akcií:

- přímé akcie – emitují se bez splatnosti, někdy a za určitých podmínek jsou svolatelné a spojené s pevnou dividendou.
- konvertibilní akcie – obsahují ustanovení, podle kterého je může vlastních za určitých podmínek konvertovat na akcie kmenové. [12]

c) Zaměstnanecké akcie

V některých zemích emitují společnosti zvláštní druh akcií pro své zaměstnance. Zaměstnanci je mohou obdržet formou odměny a prostředek motivace. Akcie se nazývají

zaměstnaneckými. Zaměstnanci je mohou získat, buď za zvýhodněných podmínek, nebo dokonce zcela zdarma. Při ukončení pracovního poměru (vyjma odchodu do penze) nebo při úmrtí zaměstnance musí být akcie vráceny společnosti. Majitelé zaměstnaneckých akcí mají stejná práva jako akcionáři, pokud není určeno jinak stanovami. [12]

Společnosti vlastněné zaměstnanci jsou společnosti, jejichž akcie plně či částečně vlastní zaměstnanci. V rámci těchto společností existují i společnosti zcela vlastněné zaměstnanci. Akcie jsou na trhu neprodejné a zisk společnosti si rozdělují výlučně zaměstnanci. U těchto společností běžně zaměstnanci volí výbor ředitelů. [12]

d) Podoba akcií

Podoba akcií může být dvojí:

- listinná – akcie skutečně existují jako cenné papíry, které drží akcionář u sebe;
- zaknihovaná – akcie jsou registrovány v některém registru cenných papírů (v ČR jsou registrovány ve Středisku cenných papírů). [12]

e) Forma listinných akcií

Listinné akcie mohou být:

- na jméno – jsou spojeny s konkrétním akcionářem, práva má pouze osoba, která je zapsána v seznamu akcionářů, který je veden emitentem či zprostředkovatelem;
- na doručitele – nejsou spojeny s konkrétním akcionářem, práva má osoba, která je jejich vlastníkem, převod akcií spočívá pouze v jejich předání. [12]

f) Klasifikace akcií

Akcie můžeme klasifikovat mnoha způsoby. Základem klasifikace je vztah mezi akciovým rizikem a výnosností. Platí, že čím vyšší je akciové riziko, tím vyšší je očekávaná výnosnost. [12]

Nejčastěji se používají tyto klasifikace:

- podle sektoru – tato klasifikace vychází z hypotézy, že akcie společností ze stejného sektoru podobně reagují na změnu vnějších podmínek.
- podle chování cen akcií – klasifikace je založena na různém chování akcií na trhu. V tomto směru se používají klasifikace růstových akcií, defenzivních akcií, cyklických akcií a spekulačních akcií.

Prvotřídní akcie jsou akcie prvotřídních společností. Prvotřídní akcie jsou relativně drahé a mají tudíž nízkou výnosnost. Prvotřídní společnosti jsou velké a důvěryhodné společnosti, které dlouhodobě vykazují růst, zisk a dividendy.

- podle objemu obchodování – je klasifikace založena na obratu jednotlivých akcií a odráží jejich likviditu a schopnost obchodování. [12]

2.2 Akcie v České republice

Akcie je cenným papírem, s nímž jsou spojena práva akcionáře jako společníka podílet se na jejím řízení, jejím zisku a na jejím likvidačním zůstatku při zániku společnosti. Osoba, která se podílí na základním kapitálu společnosti, je oprávněna vykonávat práva akcionáře jako společníka, i když společnost dosud nevydala akcie nebo zatímní listy, a to ode dne zápisu základní kapitálu, na němž se podílí, do obchodního rejstříku. [12]

Akcie mohou být vydány v souladu se zvláštním zákonem v listinné nebo zaknihované podobě.

Akcie musí obsahovat:

- firmu a sídlo společnosti,
- jmenovitou hodnotu,
- označení formy akcie, u akcie na jméno firmu, název nebo jméno akcionáře,
- výši základního kapitálu a počet akcií k datu emise akcie,
- datum emise.

Listinná akcie musí obsahovat i číselné označení a podpis člena nebo členů představenstva, kteří jsou oprávněni jménem společnosti jednat k datu emise. [12]

Akcie může znít:

- na jméno – společnost vede seznam akcionářů, v němž se zapisuje označení druhu a formy akcie, její jmenovitá hodnota, firma nebo název a sídlo právnické osoby nebo jméno a bydliště fyzické osoby, která je akcionářem, popřípadě číselné označení akcie a změny těchto údajů. Vydala-li společnost akcie zaknihované, mohou stanovy určit, že seznam akcionářů nahradí evidence zaknihovaných cenných papírů. Práva spojená s akcií na jméno je oprávněna vykonávat osoba uvedená v seznamu. Listinná akcie je převoditelná rubopisem nebo předáním.

- na majitele – akcie je neomezeně převoditelná. Práva spojená s akcií vzhledem ke společnosti může uplatňovat ten, kdo ji předloží, nebo ten, kdo prokáže písemným prohlášením osoby, která vykonává úschovu nebo uložení, že akcie je pro něho uložena. V prohlášení musí být uveden účel, pro který se prohlášení vydává, a den jeho vystavení. Práva spojená se zaknihovanou akcií na majitele vykonává osoba vedená v evidenci zaknihovaných cenných papírů. [12]

Stanovy mohou určit, že zaměstnanci společnosti mohou nabývat akcie společnosti za zvýhodněných podmínek. Dále stanovy nebo usnesení valné hromady o zvýšení základního kapitálu mohou určit, že zaměstnanci nemusí splatit celý emisní kurz akcií nebo celou cenu a rozdíl bude pokryt z vlastních zdrojů společnosti. Souhrn částí cen všech akcií, které nepodléhají splacení zaměstnanci, nesmí překračovat 5 % základního kapitálu v době, kdy se o upsání akcií zaměstnanci nebo jejich prodeji zaměstnancům rozhoduje. Zvláštní práva mohou uplatnit pouze zaměstnanci společnosti a zaměstnanci společnosti, kteří odešli do důchodu. [12]

Na českém akciovém trhu skutečně existují veřejně obchodovatelné akcie, které mají omezenou převoditelnost. Akcionář tyto akcie nemůže prodat bez souhlasu orgánů společnosti, nejčastěji představenstva. Kdo vydává souhlas a kdo, povoluje prodej akcií, musí být uvedeno ve stanovách společnosti. Omezení převoditelnosti je kvůli zamezení obavám, například z prodeje velkého množství akcií konkurenční společnosti, která by mohla společnost ovládnout. Většinový akcionář pak nemusí mít obavy, že přijde o své výsadní postavení. [12]

3 KYBERNETICKÝ TERORISMUS

Tato kapitola se zabývá kybernetickým terorismem, dále podstatným rozdílem mezi pojmy hacker a cracker, které jsou mezi sebou často zaměňovány. Dále se zde můžete dočíst o typech hackerů. Dozvíte se zde i o jejich potřebách, nástrojích a technikách.

3.1 Kybernetický terorismus

Pro technickou západní společnost jsou velmi devastující případné útoky na počítačovou síť. Již byly zdokumentovány případy, kdy byli tzv. „hackeři“ schopni pomocí počítače vyřadit rozvod elektrické energie a uvrhnout některé regiony západních zemí do tmy. Už v polovině osmdesátých let skupina hannoverských hackerů financovaných KGB pronikla do počítačů americké armády. Mnozí moderní bezskrupulózní hackeři se netají svou ochotou prodávat nalezené informace zločinným státům. [16]

Útoky prostřednictvím počítačových sítí představují hrozbu srovnatelnou s účinky zbraní hromadného ničení. Západ spoléhá víc a víc na počítačové sítě. To posiluje závislost – a ze závislosti se rodí zranitelnost. Zpoza počítačového terminálu lze totiž teoreticky zablokovat automatizované rozvody vody, elektřiny, plynu i ropy. Nebo naopak otevřít přehrady a zatopit přilehlé oblasti. Chaos se dá snadno vyvolat i v letecké dopravě a v plně elektronizovaných finančních operacích. Kolaps hrozí i vládním komunikačním systémům včetně vojenských. Při jednom cvičení se dokonce povedlo vybranému specialistovi ovládnout přes počítač několik moderních válečných lodí. Miliony obyvatel vyspělého světa pak mohou náhle zjistit, že jim doma nesvítí světlo, neteče voda, nefunguje telefon, rádio mlčí a nakupovat lze jen za hotové. Řada zemí pochopila, že při klasickém vojenském konfliktu s USA nemohou získat navrch, a tak ubírá své aktivity tímto směrem – směrem kybernetické sabotáže. [16]

Říká se, že stovka specialistů za třicet milionů dolarů poškodí americkou infrastrukturu tak, že si její plná obnova může vyžádat roky. V této souvislosti je poukazováno na ruské a čínské aktivity. Také Íránci mají prý vlastní rozsáhlý program. Čínští stratégové jsou podle jedné studie Pentagonu například přesvědčeni, že tok informací uvnitř americké armády je již dnes z 90 % závislý na satelitech. A jejich vyřazení tak představuje nejlevnější cestu, jak dostat dočasně ze hry armádu světové supervelmoci. Protivník však může být i mnohem menší než nejlidnatější země světa. Pentagon nechce podceňovat ani menší země a právě teroristy. Naštěstí zdaleka ne všichni potenciální zájemci o podobnou sabotáž disponují potřebnými vědomostmi a současně technickým vybavením. S rostoucí mírou závislosti mnoha západních institucí a firem na výpočetní technice spolu se stále širším využitím

Internetu však útok na počítačové sítě vypadá z pohledu „zvenčí“ stále lákavěji. [16]

Sekundární nebezpečí Internetu

Sekundární nebezpeční Internetu spočívá v tom, že je doménou řady podrobných návodů pro přípravu nebezpečných zbraní. Dříve bylo šíření podobných návodů technicky náročné - bylo nutné zaplatit tiskárnu a zařídit distribuci. Teď si napíšete na počítači pár stránek, dáte je na Internet a je to dostupné všude. Technologie je prostě rychlejší než lidské myšlení. Nejenom rychlejší, ale i všudypřítomná, neboť do stejného dokumentu se můžeme dostat prostřednictvím několika různých serverů. Adresa takového dokumentu se může velmi operativně měnit. Na Internetu najdeme širokou škálu návodů na výrobu Molotovových koktejlů, střelné bavlny, dynamitu, nitroglycerinu i tritolu (TNT). Rozvedena je i výroba bomb, roznětek, časovačů i samotné konstrukce pum. Významnou roli v plánování teroristických útoků hrají, především v posledních letech, i všechny druhy médií, neboť věnují těmto zprávám značnou pozornost. Tím vlastně jistým způsobem teroristické požadavky nebo dokonce i program popularizují. [16]

Bez ohledu na mimořádné úsilí bezpečnostních složek všech demokratických států mezinárodní terorismus eliminovat se s jeho aktivitami každoročně setkává kolem padesáti až šedesáti zemí. Téměř nic neřeší zpřísnění trestů. Mezinárodní teroristé – k jejichž požadavkům patří změna vnitřní a zahraniční politiky, změna právního systému, propuštění vězněných teroristů či zaplacení výkupného a umožnění bezpečného úniku – jsou odhodláni ke všemu, nedají se zastrašit, často jsou připraveni zemřít při sebevražedném útoku. Zastavení připravené akce je proto nesmírně obtížné a stejně obtížná je i jakákoliv prevence. O to větší a zcela nezastupitelnou roli hrají v celé této oblasti zpravodajské služby, které získávají a analyzují informace o záměrech a pohybech teroristických organizací, skupin i jednotlivců. [16]

3.2 Hacker versus cracker

Média často zaměňují pojmy "hacker" a "cracker". Hacker v původním významu rozhodně neznamená nějakého člověka, který chce ničit, škodit, krást, atd. Tato činnost je typická právě pro crackery. Cílem hackera je dostat se do cizího systému, stroje apod., ale nikoli s úmyslem někoho anebo něco či nějakou instituci poškodit natož tak cokoli zničit, ale upozornit na bezpečnostní chyby, nedostatky a rizika, jenž objevil právě při průniku do cizího systému. Eric Raymond k tomu píše: „*Existuje ještě jiná skupina lidí, kteří si hlasitě říkají hackeři, ale hackery nejsou. Jsou to lidé (převážně adolescentní muži), které vzrušuje nabourávání do počítačů a telefonního systému. Skuteční hackeři říkají takovým lidem "crackeři" a nechtějí s*

nimi mít nic společného. Opravdoví hackeři považují většinou crackery za líné, nezodpovědné a nepříliš bystré a namítají, že schopnost nabourat ochranný systém nedělá z člověka hackera víc, než schopnost ukrást auto dělá z člověka automechanika. Bohužel mnozí novináři a spisovatelé se nechali zmást a používají slovo "hacker" pro popis crackera, což hackerům velice vadí.“ Možná je to málo známé, ale hackeři mají svou etiku- základním rozdílem je, že hackeři věci vytvářejí a crackeři je ničí. [14]

Zajímavá je také tzv. kultura darů, kterou hackeři pěstují - „*Své postavení a pověst v ní získáváte ne nadvládou nad jinými, ne svou krásou, ani tím, že máte věci, které ostatní chtějí, ale tím, že něco dáváte. V tomto případě tím, že věnujete svůj čas, kreativitu a výsledky svých schopností*,“ říká Eric Raymond. [14]

3.2.1 Hacking a hackeři

Hacking a průniky do systémů a aplikací s cílem ovládnout cíl útoku nebo zneužít či alespoň negativně ovlivnit jeho funkčnost. Jeho historie sahá k počátkům prvních počítačů. Motivace hackerů bývá různá, je to například osobní prospěch, prezentace osobních postojů hackera, dále zviditelnění se v rámci komunity, nebo zábava na různé etické úrovni. [15]

Politické rozdělení hackerské scény

White Hats – někdy též hackeři etičtí, nezávislé experti a konzultanti, individuality, komerční bezpečnostní laboratoře.

Existují i Grey Hats a vztahy mezi White Hats a Black Hats jsou často velmi napjaté.

Co potřebuje správný hacker

- *Nástroje*
  - škála používaných nástrojů je obrovská, řada z nich je volně dostupná na Internetu.
  - řada nástrojů je vlastní výroby – hacker » programátor.
- *Znalosti*

  - hacker (s výjimkou script kiddies) obvykle disponuje poměrně detailní technikou znalostí, kterou si musí průběžně udržovat – tj. potřebuje i dostatek času.
- *Informace*
  - hacker potřebuje přístup k informacím (některé jsou veřejně dostupné jiné jen v uzavřené komunitě). [15]

Nejčastěji používané techniky hackerů

- *Zneužití Buffer Overflow (BOF*) – poměrně velký okruh slabin, jejichž příčinou je programátorská chyba.
- *Zneužití chyb ve WWW aplikacích* – nejčastěji SQL injection či podobné variace.
- *Síťové techniky*
  - Sniffing – odposlech síťové komunikace
  - IP Spoofing – předstírání cizí IP adresy
- *Denial of Service (DoS) útoky*
  - flooding (zahlcení linky, zahlcení systému požadavky, …)
  - distribuované DDoS (při současných technologiích prakticky není obrany)
- *Červi, trojské koně* („social hacking" – sociální inženýrství) …→
- *Útoky na heslo* – hádání/lámání hesel, základem jsou slovníkové útoky versus hrubá síla, dnes existují již i sofistikovanější heuristické metody. Výkonnost běžně dostupné výpočetní síly roste a kvalita hesel přirozeně stagnuje, u slabších hashovacích funkcí není problém v historicky krátké době projít celý prostor hesel. Kvalita hesel je tradičním bezpečnostním problémem.[15]

Hacking v praxi - bezpečnostní slabiny nevznikají, existují již léta jen se o nich neví - v horším případě je znají jen někteří (blackhats). Zranitelný systém neochrání IDS ani správce u konzole, dále zabezpečení dodávaných systémů není ani u renomovaných dodavatelů samozřejmostí (často garantují funkčnost jen na své konfiguraci). U systémů přístupných z internetu musíme počítat s tím, že budou nebo mohou být napadeny. [15]

Skutečné hrozby hackingu- napadení nemusí být na první pohled viditelné, největší hrozbou je lidský faktor – zejména vlastní uživatelé a dále neodborné zásahy případně backdoory administrátorů. Z hlediska odhalení jsou nejproblematičtější zcela specifické chyby v aplikacích na míru. Červi mohou přijít novější a mnohem horší a stále není dostatečné obrany proti útokům DDoS. [15]

Technická protiopatření proti Hackingu

- *Firewall* – v současnosti je prakticky nutností

– v současnosti prakticky nutnost, technologicky „usazená" oblast.

- *IDS*

– hlavně monitorovací nástroj, představuje možnost předcházení útokům, je omezené a často přeceňované – efektivní provoz vyžaduje nastavení patřičných interních procesů. Díky dynamickému vývoji technologie se předpokládá, že v budoucnu stoupne význam této technologie.

- *Content security* (ochrana před „zlovolným" SW). [15]

Penetrační test jako kontrolní nástroj – je zhodnocením bezpečnosti hodnoceného systému (sítě) neboli je pokusem o průnik – metodami i použitými nástroji je blízký reálnému útoky, je prováděn vzdáleně – po síti (z internetu - „externí", z vnitřní sítě - „interní"), ve „skryté" variantě prověří také monitorovací a reakční mechanismy. Předmětem kontroly jsou jednotlivá zařízení případně část sítě, jedním z hlavních přínosů je využití kombinačních schopností odborníků. [15]

Průběh penetračního testu

• Varianty testů

– externí (simulace hackera z Internetu),

– interní (simulace útočníka uvnitř),

– speciální varianty (testy WWW aplikací, Wi-Fi sítí apod.)

• Základní kroky penetračního testu

– rekognoskace - sběr informací o testovaném prostředí,

– automatizované testy bezpečnostních slabin,

– detailní manuální testy na základě výsledků testů,

– praktická demonstrace zneužití slabin (provedení útoku).

Výsledek penetračního testu - poskytne obrázek o tom, čeho by při současné úrovni znalostí mohl dosáhnout útočník při reálném útoku. Výstupem je nejen nález, ale i doporučení, ale ani negativní výsledek testu nám nedává jistotu. Existují stále agresivnější nástroje a metody a reálný útočník není časově omezen. Neustále se vyvíjí znalost bezpečnostních slabin a řada slabin existujících nebyla doposud odhalena či zveřejněna. [15]

3.2.2 Crack, cracking a crackeři

Crack je malý program, sloužící k odstranění, či omezení funkčnosti ochranných prvků jiného programu či softwarového balíku. Obvykle přepíše údaj o originálním sériovém či registračním čísle, aby bylo možno spustit program s jiným, veřejně dostupným, číslem či heslem.

Cracking (z anglického crack – lámat) je metoda odstraňování ochranných prvků softwaru. Osoba odstraňující tyto ochrany se nazývá cracker. [19]

Prolamování softwarových ochran je ve většině zemí nezákonné, protože je software opatřen autorským právem (copyrightem). Programátoři se obvykle snaží maximálně zamezit crackování svého softwaru a používají nejrůznější techniky (šifrování, automodifikační kód, apod.), aby tomu zamezili.

Black Hats – uzavřená společnost crackerů, jejichž cílem je nalezení bezpečnostních slabin a jejich využití pro vlastní potřebu, často je odhalí dříve než White Hats.

Cracker je člověk, který zneužívá své vědomosti o počítačové bezpečnosti ke svému prospěchu při průnicích do softwarů. Cracker musí mít dobré znalosti o principech fungování informačních technologií, dále o programování a počítačové bezpečnosti apod. Nevhodným vzorem programů a existencí programátorských chyb vznikají v softwarech zranitelnosti, které lze využít. [19]

3.2.3 Boj proti kybernetickým hrozbám

ČR nepatří mezi země, kterým by se vyhýbaly bezpečnostní incidenty v oblasti kybernetického prostoru. Ačkoli se zatím jednalo zejména o pokusy o zneužití internetového bankovnictví, nelze do budoucna vyloučit daleko závažnější a politicky motivované útoky, které by mohly zapříčinit velké škody a rovněž například oslavit důvěru veřejnosti v koncept e-governmentu. „Miliony osob mohou náhle zjistit, že jim doma nesvítí světlo, neteče voda, nefunguje telefon, televize ani neblikne, rádio mlčí a nakupovat lze jen za hotové.“ [18]

Policejní kapacity věnující se boji proti kybernetickým hrozbám jsou plně vytíženy běžnou agendou (boj proti nedovolené pornografii, extremistické propagandě, porušování práv k duševnímu vlastnictví atd.) a postrádají lidské a technické rezervy, které by jim umožnily sledovat aktuální trendy, provádět výzkum nebo aktivní operace v kybernetickém prostředí.

Není bez zajímavosti, že boj proti kybernetickým hrozbám byl jednou ze stěžejních třetipilířových priorit ČR během jejího předsedání orgánům EU v první polovině roku 2009. [18]

Dlouho se nedařilo jednoznačně stanovit, který subjekt (resort) je střechovým gestorem odpovědným za otázky informační (kybernetické) bezpečnosti, bezpečnosti kritické informační infrastruktury. Po zániku ministerstva informatiky vzniklo vakuum, které bylo zaplněno až jednáním Bezpečnostní rady státu ze dne 5. ledna 2010. To rozhodlo, že koordinací dalšího úsilí bude pověřeno Ministerstvo vnitra. Zároveň není zřejmé, zda v ČR bude vybudováno národní pracoviště typu CSIRT/CERT (hlásné pracoviště, které by ve spolupráci s obdobnými pracovišti v zahraničí mohlo potírat kybernetické incidenty v samém zárodku). [18]

4 KYBERNETICKÉ ÚTOKY A JEJICH PŮSOBENÍ NA TRŽNÍ HODNOTY AKCIÍ SPOLEČNOSTÍ V ČESKÉ REPUBLICE

4.1 Kybernetický útok na banky ze středy 6. března 2013

V této kapitole se zabýváme kybernetickým útokem ze dne 6. března 2013. S problémy se potýkala trojice největších českých bank, ČSOB, Komerční banka a Česká spořitelna. Mimo to útoky mířily také na Českou národní banku a Pražskou burzu cenných papírů. Vyřazeny z provozu byly i některé menší banky. Útoky byly jednodenní, většinou portály postižených bankovních a finančních institucí fungovaly již po poledni. [17]

4.1.1 ČESKÁ SPOŘITELNA

„Dočasně jsme měli nefunkční webové stránky, internetové bankovnictví a aplikace běžící přes internet, jako je Servis 24, e-commerce nebo platby kartou u obchodníků. Příčinou výpadku byl vnější útok," informoval Marek Pšeničný z tiskového centra České spořitelny.

Vnitřní systémy banky nebyly narušeny, data klientů a jejich vklady nebyly ohroženy, bankomaty fungovaly. [17]

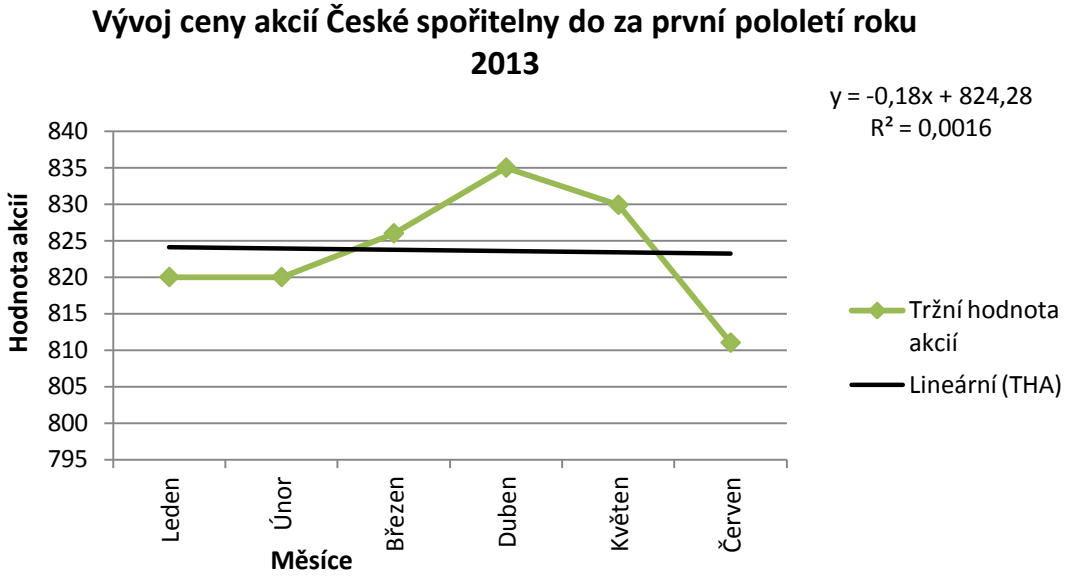
V tabulce č. 1 jsou uvedeny tržní ceny akcií České spořitelny od začátku roku 2013 do konce června roku 2013. Tržní ceny akcií jsou uvedeny ke dni, který je zhruba ve středu daného měsíce, ale není sobotou či nedělí.

Tabulka 1: Tržní ceny akcií České spořitelny od 01/2013 do 06/2013

Období (1. pololetí roku 2013)	Leden	Únor	Březen	Duben	Květen	Červen
Tržní hodnota akcie (v Kč)	820	820	826	835	829,9	811

Zdroj: upraveno dle [2]

Graf 1: Vývoj ceny akcií České spořitelny za první pololetí roku 2013



Zdroj: vlastní úprava dle [2]

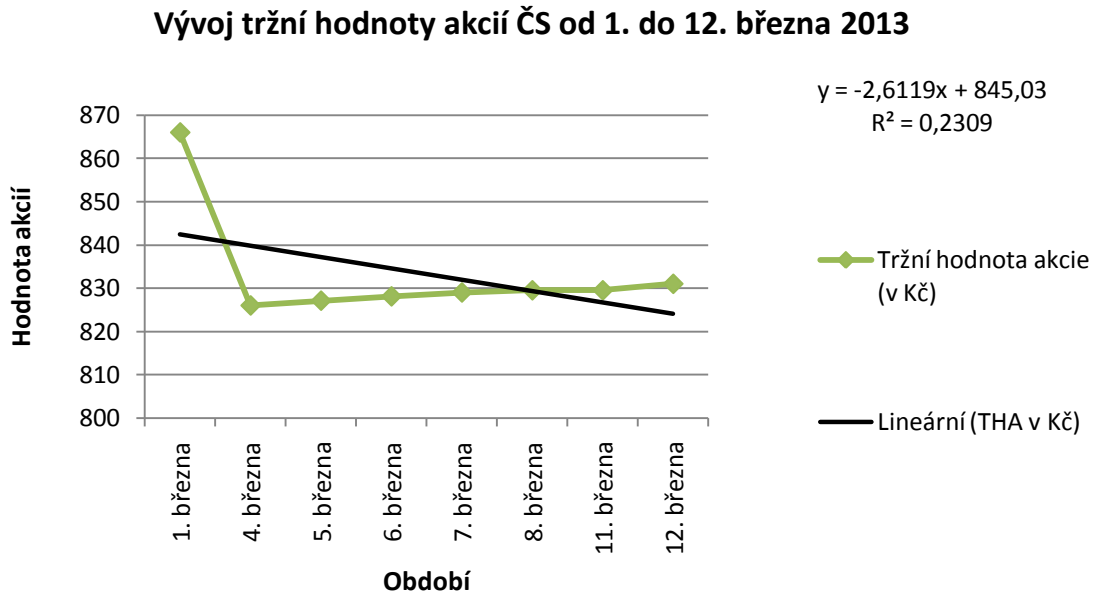
Tržní hodnoty akcií České spořitelny uvedené v tabulce č. 2 jsou za období od 1. do 12. března 2013, za všechny všední dny, neboli dny, ve kterých se obchoduje na české burze. Tržní hodnoty jsou uvedeny vždy ke konci obchodování daného dne.

Tabulka 2: Tržní ceny akcií České spořitelny od 1. do 12. března roku 2013

Období	1. března	4. března	5. března	6. března	7. března	8. března	11. března	12. března
THA (v Kč)	866	826	827,1	828,1	829	829,5	829,5	831

Zdroj: vlastní úprava dle [2]

Graf 2: Vývoj tržní hodnoty akcií ČS od 1. do 12. března 2013



Zdroj: vlastní úprava dle [2]

Tržní hodnoty akcií ČS se vlivem DDoS elektronického útoku podle jejich vývoje uvedeného v grafu nesnížily. Podle mého očekávání by se vlivem elektronického útoky ceny akcií měly snižovat, ale u ČS nastal pravý opak. A ani v krátkodobém horizontu, čili v období od 1. do 12. března 2013, se kybernetický útok na tržní hodnotě akcií neprojevil žádným významným poklesem. Naopak ceny akcií ode dne útoku, tedy od 6. března 2013, začaly nepatrně růst.

Tato banka není na trhu akcií v pořádku. Banky by se měly snažit systematicky zhodnocovat své ceny akcií a vést je tak k růstu. Česká spořitelna je na tom ale úplně opačně.

4.1.2 KOMERČNÍ BANKA

Mluvčí Komerční banky Monika Klucová sdělila: „Komerční banka dnes zaznamenala DDoS útok na své portály www.kb.cz a www.mojebanka.cz. V žádném případě nedošlo k úniku žádných klientských dat.“ [17]

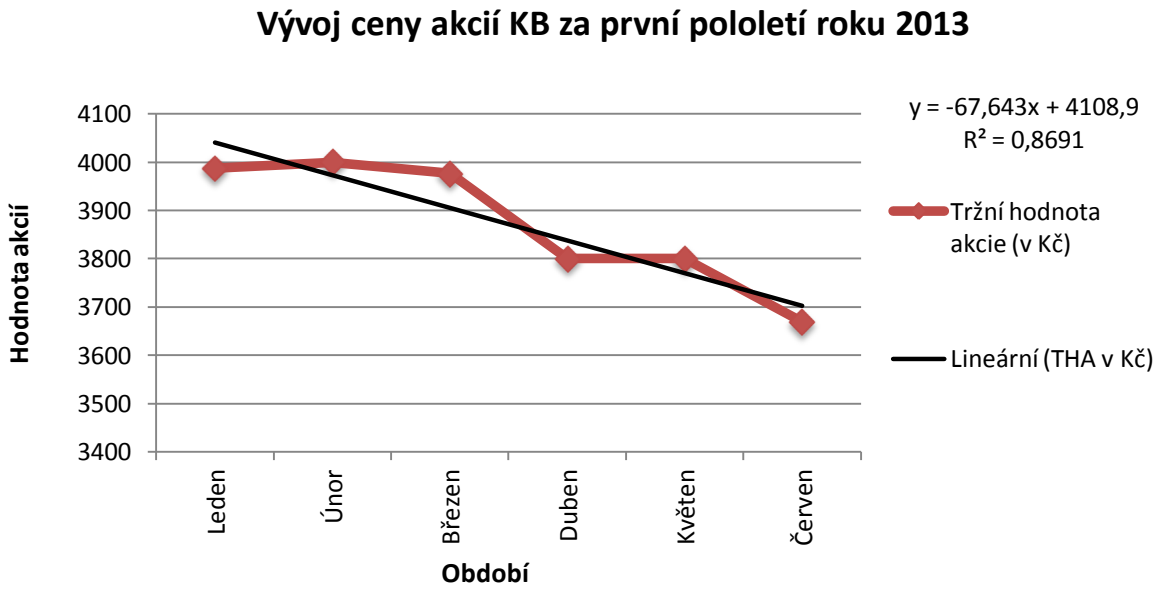
V tabulce č. 3 jsou uvedeny tržní ceny akcií Komerční banky od začátku roku 2013 do konce června roku 2013. Tržní ceny akcií jsou uvedeny ke dni, který je zhruba ve středu daného měsíce, ale není sobotou či nedělí.

Tabulka 3: Tržní ceny akcií Komerční banky od 01/2013 do 06/2013

Období (1. pololetí roku 2013)	Leden	Únor	Březen	Duben	Květen	Červen
Tržní hodnota akcie (v Kč)	3 987,30	4 000	3 976,50	3 800	3 800	3 669,10

Zdroj: vlastní úprava dle [1]

Graf 3: Vývoj ceny akcií Komerční banky za první pololetí roku 2013



Zdroj: vlastní úprava dle [1]

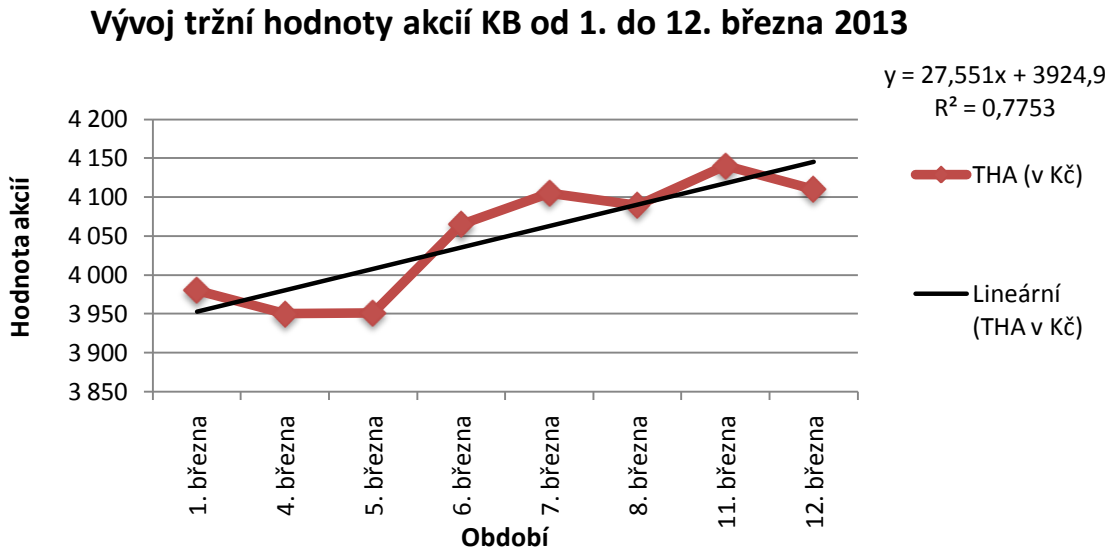
Tržní hodnoty akcií Komerční banky uvedené v tabulce č. 4 jsou za období od 1. do 12. března 2013, za všechny všední dny, neboli dny, ve kterých se obchoduje na české burze. Tržní hodnoty jsou uvedeny vždy ke konci obchodování daného dne.

Tabulka 4: Tržní ceny akcií KB od 1. do 12. března roku 2013

Období	1. března	4. března	5. března	6. března	7. března	8. března	11. března	12. března
THA (v Kč)	3 980	3 950	3 951,40	4 065	4 105	4 089,50	4 140	4 110

Zdroj: vlastní úprava dle [1]

Graf 4: Vývoj tržní hodnoty akcií KB od 1. do 12. března 2013



Zdroj: vlastní úprava dle [1]

Tržní hodnoty akcií KB se vlivem elektronické útoky také příliš nezměnily. Tržní hodnoty v delším časovém období, tedy v prvním pololetí roku 2013, rostly i klesaly, ale to je u akciových společností přirozené. Od ledna do února se ceny akcií pohybovaly nepatrně směrem nahoru a od března do konce června ceny akcií postupně klesaly. Tento pokles od března do června 2013 mohl být způsoben i tímto teroristickým útokem, ale nemůžeme tvrdit, že pokles je způsoben jen tímto. V grafu č. 3 je velmi dobře viditelná statisticky prokazatelná závislost poklesu tržních hodnot akcií.

V kratším časovém intervalu však hodnoty akcií rostou i klesají, ale vzhledem k 1. březnu 2013 se hodnoty akcií pohybují spíše směrem nahoru. Tedy v kratším časovém období hodnoty spíše pozvolna rostou namísto poklesu, který by měl být způsoben kybernetickým útokem.

Stejně jako Česká spořitelna je na tom i Komerční banka. Tedy není na trhu akcií v pořádku. Její akcie také klesají, oproti tomu, aby rostly. Kybernetický útok tyto dvě banky neohrozil, ale ani jim nepomohl. A zároveň neměl žádný vliv na funkčnost ani jedné z nich.

4.1.3 ČSOB

Mluvčí ČSOB Pavla Hávová řekla: „Během středečního dopoledne jsme zaznamenali kybernetický útok na dostupnost našich elektronických služeb. Cílem útoku bylo omezení dostupnosti webových stránek ČSOB a Ery/Poštovní spořitelny,“

„Podle námi zjištěných informací byl útok veden ze zahraničí. Bezpečnost prostředků klientů či jejich dat nebyla incidentem nijak ohrožena,“ doplnila Hávová. [17]

Podle informací, které poskytla Česká televize, akcie ČSOB na burze nejsou a nebudou prodejné, protože belgická skupina KBC se rozhodla, že je na burzu neuvede z důvodu změny strategického plánu. Se změnou plánu souhlasila i Evropská komise. Uvedení na trh, však původně plánovala. Banka tak například prodá polské bankovní a pojišťovací společnosti KBC Kredyt Bank a Warta, menšinový podíl akcií ČSOB na burzu naopak neuvede. KBC plánovala na pražskou burzu uvést 30 až 40 procent akcií ČSOB již v dubnu či květnu 2010. Pak, ale termín postupně odkládala. Mezitím se objevily spekulace o možném přímém prodeji ČSOB nebo její části, které ale skupina popřela. [9]

Z tohoto vyplývá, že akcie nejsou na burze prodejné a tudíž nelze srovnávat ceny akcií v časovém období, ve kterém proběhl teroristický útok, který neměl vliv na funkčnost této banky.

5 KYBERNETICKÉ ÚTOKY A JEJICH PŮSOBENÍ NA TRŽNÍ HODNOTY AKCIÍ SPOLEČNOSTÍ V ZAHRANIČÍ

V této kapitole se budeme zabývat kybernetickými útoky z prosince 2010 na společnosti Visa a MasterCard a dále dvěma kybernetickými útoky na společnost Google.

5.1 Kybernetický útok na společnost Visa a MasterCard, prosinec 2010

Na začátku prosince roku 2010 skupina Anonymous, což je skupina, která se netají elektronickými útoky na různé servery, rozjela akci zvanou „Operation PayBack“ neboli operace odplata. Dne 8. prosince 2010 tato skupina zaútočila na velmi významné společnosti a hlavně na jejich servery. Těmito společnostmi byly MasterCard, Visa a PayPal.

Skupina Anonymous k útokům využívá typy útoku DDoS. Což znamená, že tyto stránky chtějí ochromit přetížením, ale nezanechávají na serverech žádné trvalé následky. [11]

Nyní budeme srovnávat pohyby tržních hodnot akcií společnosti Visa a MasterCard.

5.1.1 VISA

Anonymous zaútočili na servery této významné společnosti v rámci operace Payback, neboli „operace odplata.“ Dále si uvedeme tržní hodnoty akcií této společnosti v určitém časovém rozpětí a budeme je analyzovat.

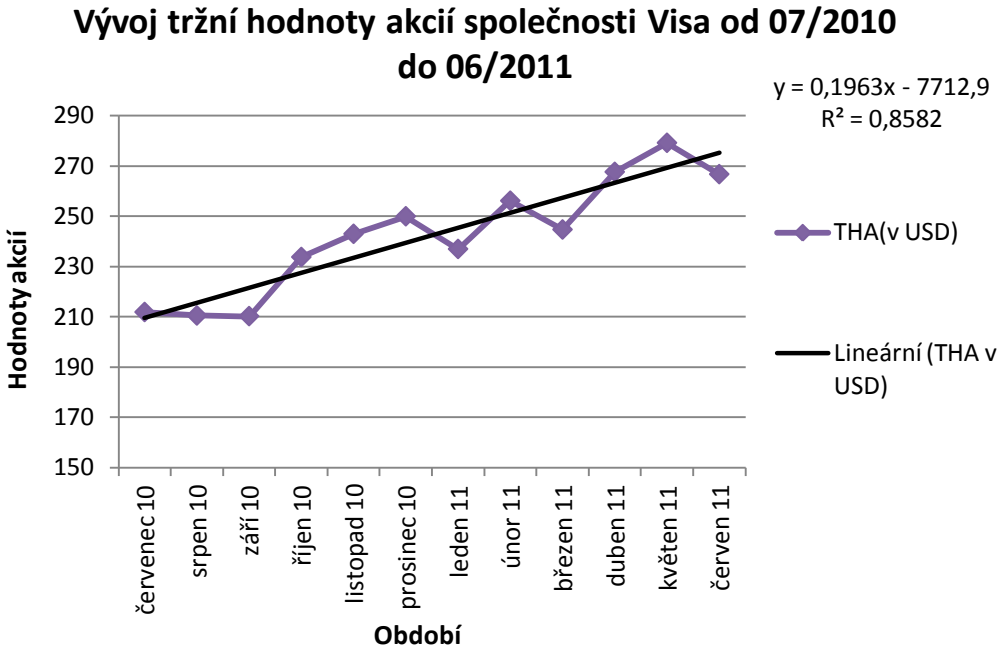
Prvním časovým úsekem je období od července 2010 do června 2011, tedy jeden kalendářní rok. Hodnoty jsou brány vždy zhruba k datu, které je ve středu měsíce, pokud není sobotou či nedělí. Hodnoty tržních hodnot akcií jsou uvedeny v amerických dolarech (USD).

Tabulka 5: Tržní hodnota akcií společnosti Visa od 07/2010 do 06/2011

Období	07/10	08/10	09/10	10/10	11/10	12/10	01/11	02/11	03/11	04/11	05/11	06/11
THA(v USD)	75,28	73,36	68,93	77,6	75,73	76,94	71,12	75,61	71,2	76,47	80,6	75,93

Zdroj: vlastní úprava dle [3]

Graf 5: Vývoj tržní hodnoty akcií společnosti Visa od 07/2010 do 06/2011



Zdroj: vlastní úprava dle [3]

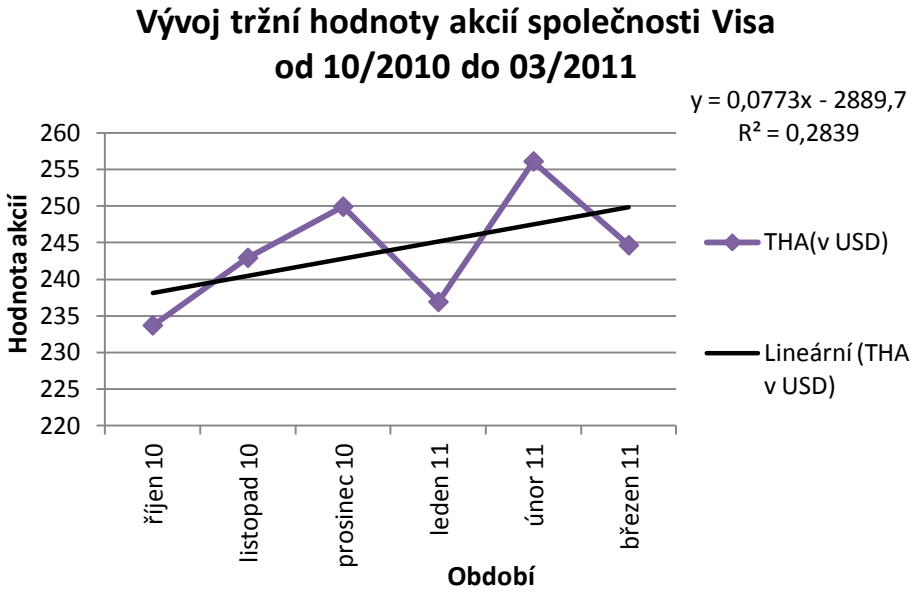
V další tabulce jsou uvedeny hodnoty za kratší časové období, přesněji od října 2010 do března 2011.

Tabulka 6: Tržní hodnota akcií společnosti Visa od 10/2010 do 03/2011

Období	10/10	11/10	12/10	01/11	02/11	03/11
THA(v USD)	77,6	75,73	76,94	71,12	75,61	71,2

Zdroj: vlastní úprava dle [3]

Graf 6: Vývoj tržní hodnoty akcií společnosti Visa od 10/2010 do 03/2011



Zdroj: vlastní úprava dle [3]

Tržní hodnota akcií společnosti Visa svědčí o dobrém hospodaření společnosti. Za dvanáct měsíců, přesněji tedy od července 2010 do června 2011, pohybovala velmi různorodě. V prosinci roku 2010 došlo k útoku ze strany skupiny Anonymous. Od poloviny prosince do poloviny ledna zaznamenala tržní hodnota akcií této společnosti značný pokles, ale od ledna do února akcie zase stouply zpět na téměř původní prosincovou hodnotu. Od února do března hodnota opět poklesla, ale poté stoupala až do poloviny května 2011. Z poklesu, který nastal v období z prosince na leden, ale nelze říci, že byl způsoben, kybernetickým útokem zařazeným do „operace odplata." Tento útok tržní hodnoty akcií nijak neovlivnil a je způsoben běžnými výkyvy ceny akcií.

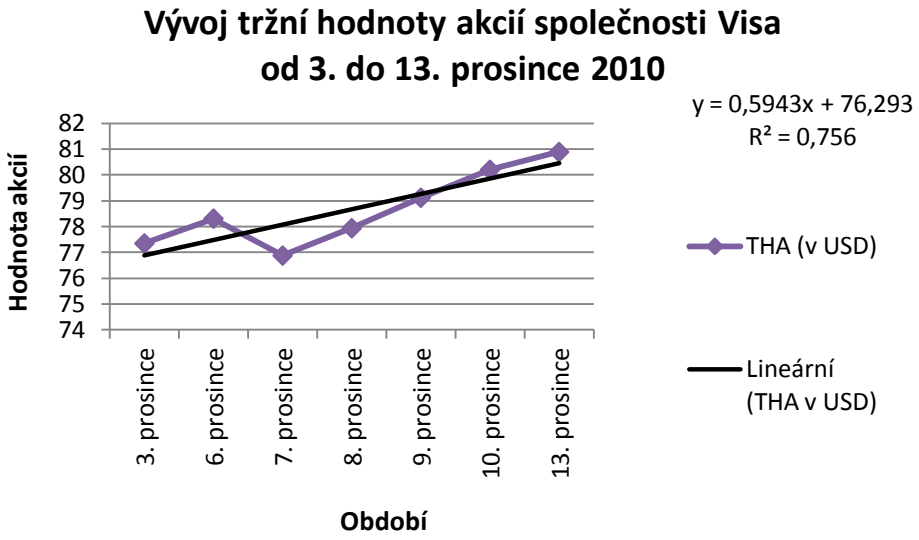
V následující tabulce a grafu je uvedeno ještě kratší období než v předchozích tabulkách a grafech, tj. období od 3. prosince do 13. prosince 2010. Tedy období bezprostředně před útokem a bezprostředně po něm.

Tabulka 7: Tržní hodnota akcií společnosti Visa od 3. prosince do 13. prosince 2010

Období	3. prosince	6. prosince	7. prosince	8. prosince	9. prosince	10. prosince	13. prosince
THA (v USD)	77,35	78,31	76,88	77,94	79,12	80,2	80,89

Zdroj: vlastní úprava dle [3]

Graf 7: Vývoj tržní hodnoty akcií společnosti Visa od 3. prosince do 13. prosince 2010



Zdroj: vlastní úprava dle [3]

Z grafu č. 7, ve kterém je vyjádřeno bezprostřední období před a po útoku, není zřejmý žádný pokles tržní hodnoty akcií, který jsem očekávala. Naopak tržní hodnota akcií společnosti Visa těsně po elektronickém útoku stále stoupá. Z toho vyplývá, že tato společnost je na tom velmi dobře na akciovém trhu a že nebyla ovlivněna elektronickým útokem a zároveň můžeme říci, že nebyla nijak ohrožena či narušena její funkčnost.

5.1.2 MASTERCARD

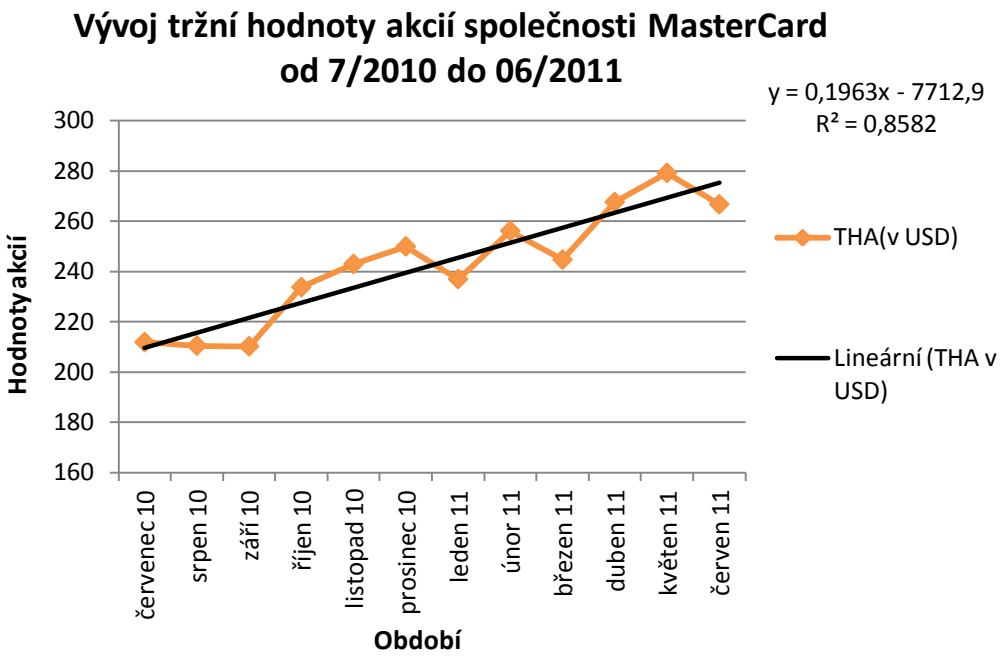
Při „operaci odplata“ skupiny Anonymous byl proveden i útok typu DDoS na servery společnosti MasterCard. Tento útok byl taktéž proveden dne 8. prosince 2010.

Tabulka 8: Tržní hodnoty akcií společnosti MasterCard od 07/2010 do 06/2011

Období	07/10	08/10	09/10	10/10	11/10	12/10	01/11	02/11	03/11	04/11	05/11	06/11
THA(v USD)	211,81	210,44	210,18	233,7	242,93	249,92	236,91	256,1	244,65	267,58	279,15	266,68

Zdroj: vlastní úprava dle [4]

Graf 8: Vývoj tržní hodnoty akcií společnosti MasterCard od 07/2010 do 06/2011



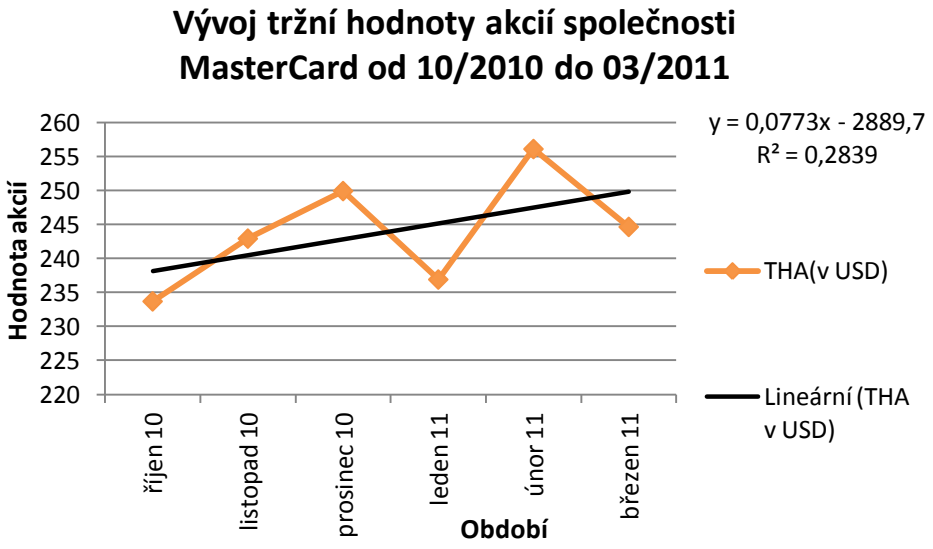
Zdroj: vlastní úprava dle [4]

Tabulka 9: Tržní hodnoty akcií společnosti MasterCard od 10/2010 do 03/2011

Období	10/10	11/10	12/10	01/11	02/11	03/11
THA(v USD)	233,7	242,93	249,92	236,91	256,1	244,65

Zdroj: vlastní úprava dle [4]

Graf 9: Vývoj tržní hodnoty akcií společnosti MasterCard od 10/2010 do 03/2011



Zdroj: vlastní úprava dle [4]

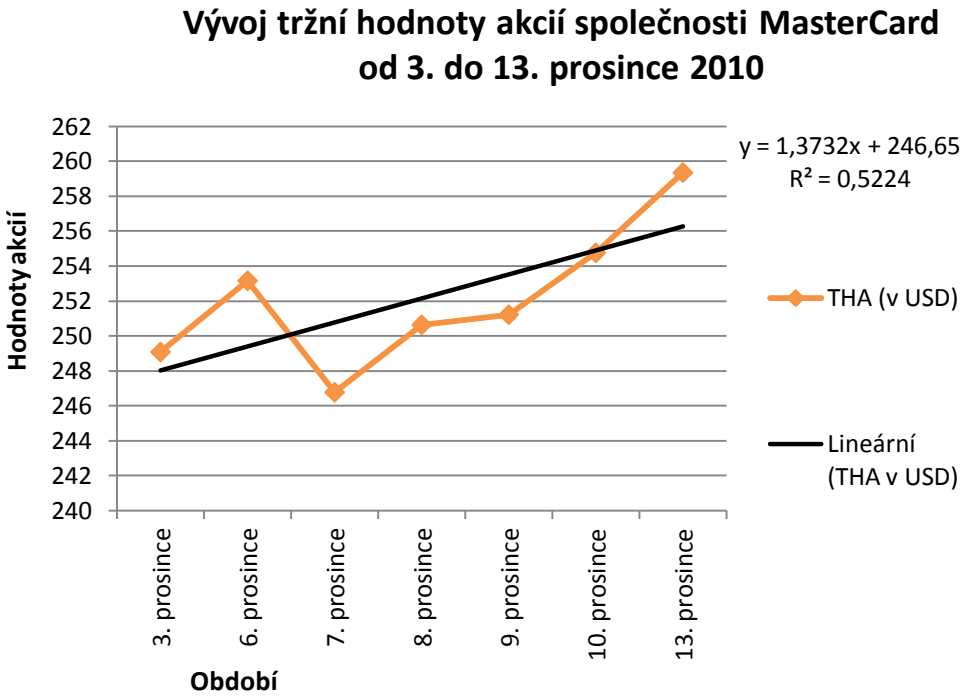
Tržní hodnota akcií společnosti MasterCard v delším (ročním) časovém horizontu klesala i stoupala, například od července do září roku 2010 tržní hodnoty akcií pozvolna klesaly, ale od října do prosince tržní hodnoty těchto akcií zaznamenaly velmi výrazný vzrůst a to téměř o 40 amerických dolarů. Ovšem v lednu tržní hodnoty klesly a do února opět stouply, ale vzhledem k tomu, že po tomto období akcie klesaly i rostly téměř pravidelně, nemůžeme říct, že tento pokles byl způsoben elektronickým útokem skupiny Anonymous. Jedná se spíše o běžné výkyvy na burze cenných papírů, které jsou takřka na denním pořádku. Naopak můžeme říci, že společnost hospodaří dobře, což je dobře vidět z grafu č. 8, ze kterého vyplývá, že se společnost snaží systematicky zvyšovat tržní hodnotu akcií společnosti.

Tabulka 10: Tržní hodnoty akcií společnosti MasterCard od 3. do 13. prosince 2010

Období	3. prosince	6. prosince	7. prosince	8. prosince	9. prosince	10. prosince	13. prosince
THA (v USD)	249,08	253,16	246,78	250,64	251,22	254,76	259,35

Zdroj: vlastní úprava dle [4]

Graf 10: Vývoj tržní hodnoty akcií společnosti MasterCard od 3. do 13. prosince 2010



Zdroj: vlastní úprava dle [4]

V krátkém časovém intervalu tedy od 3. do 13. prosince tržní hodnoty těchto akcií klesly pouze jednou a to z 6. na 7. března 2010. Je možné, že tento pokles byl způsoben elektronickým útokem, ale dle dalšího vývoje tržních hodnot akcií této společnosti, které od 7.

až do 13. března již jen rostly, to není pravděpodobné. Spíše můžeme tvrdit, že výkyvy jsou způsobeny běžnými pohyby na akciových trzích.

5.2 Kybernetické útoky na společnost Google

NAPROSTO NAHODILÉ

5.2.1 LEDEN 2010

Společnost Google 13. ledna 2010 oznámila, že se stala terčem čínského kybernetického útoku zaměřeného na e-mailové účty služby Gmail. Podle zjištění společnosti byly primárním terčem útoku účty čínských lidsko-právních aktivistů.

Společnosti Google uživatelům radí používat spolehlivé antivirové a antispywarové program, aktualizovat prohlížeče, dále nedoporučuje klikat na hypertextové odkazy v e-mailech a nesdílet online osobní informace. [7]

V návaznosti na tento incident to firma využila jako záminku k tomu, že nebude s čínskými úřady nadále spolupracovat na cenzuře internetového obsahu, což je nutná podmínka pro všechny internetové firmy, které v Číně působí. Na jaře roku 2010 se Google z čínského trhu stáhnul.

S tímto i následujícím útokem na společnost Google je spojován jeden ze šesti klíčových úřadů lidové osvobozenecké armády a rovněž technická univerzita v čínském Ťi-nanu. [7]

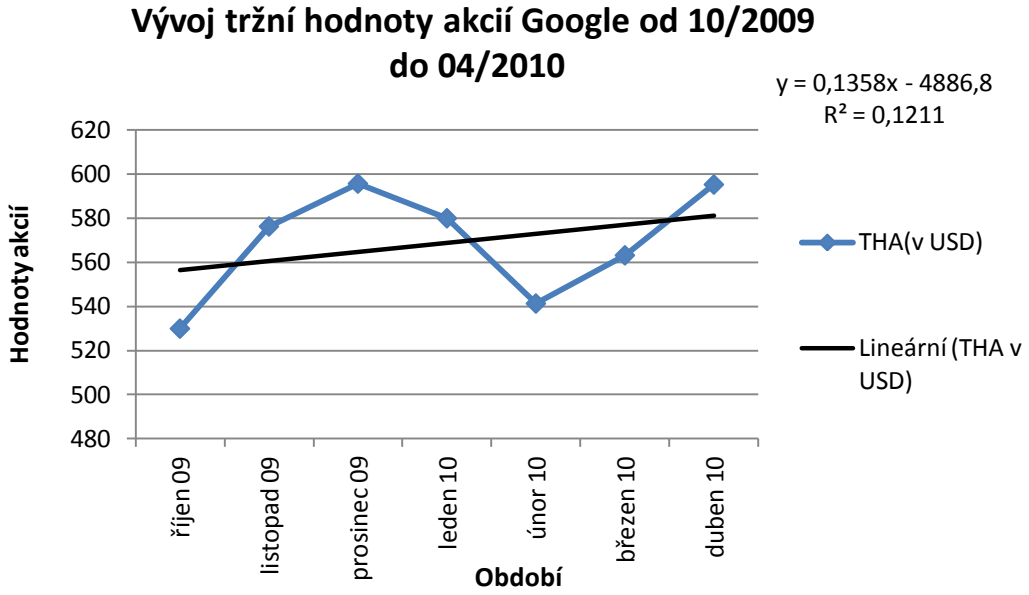
V následující tabulce a grafu vidíme hodnoty tržních hodnot akcií společnosti od října 2009 do dubna 2010 včetně. Tržní hodnoty akcií jsou vždy uváděny přibližně k datu, které je uprostřed měsíce, není-li sobotou či nedělí.

Tabulka 11: Tržní hodnoty akcií společnosti Google od 10/2009 do 04/2010

Období	říjen 09	listopad 09	prosinec 09	leden 10	únor 10	březen 10	duben 10
THA(v USD)	529,91	576,28	595,73	580	541,3	563,18	595,3

Zdroj: vlastní úprava dle [5]

Graf 11: Vývoj tržní hodnoty akcií Google od 10/2009 do 04/2010



Zdroj: vlastní úprava dle [5]

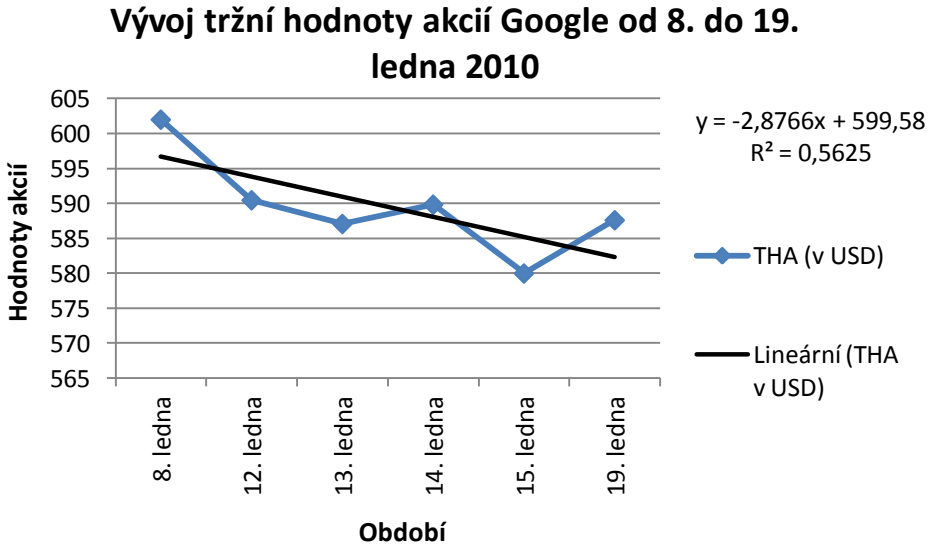
Následující tabulka a graf vyjadřují období bezprostředně před útokem a bezprostředně po něm, tedy období od 9. do19. ledna 2010.

Tabulka 12: Tržní hodnoty akcií společnosti Google od 8. do 19. ledna 2010

Období	8. ledna	12. ledna	13. ledna	14. ledna	15. ledna	19. ledna
THA (v USD)	602,02	590,48	587,09	589,85	580	587,62

Zdroj: vlastní úprava dle [5]

Graf 12: Vývoj tržní hodnoty akcií Google od 8. do 19. ledna 2010



Zdroj: vlastní úprava dle [5]

Z grafu č. 11 je viditelné, že mezi lednem a únorem nastal velmi znatelný pokles tržní hodnoty akcií společnosti. Nemůžeme ale tvrdit, že tento pokles byl způsoben elektronickým útokem, protože se tváří spíše jako zcela nahodilý. Můžeme ho tedy považovat za běžný výkyv. Dále z grafu č. 12, který se dotýká bezprostředního období před, a po útoku již není znatelný žádný výrazný pokles, který by mohl být způsoben elektronickým útokem.

5.2.2 ČERVEN 2011

Americká internetová firma Google dne 2. června 2011 odhalila útok neznámých hackerů, kteří se pokusili ukrást hesla ke stovkám e-mailových účtů freemailu Gmail.

Podle informací, které poskytla firma Google má útok patrně kořeny v Číně a byl zřejmě veden i proti účtům vysokých představitelů americké administrativy, čínských aktivistů i novinářů. [10]

Hackeři se k e-mailům uživatelů dostali tak, že jim ukradli hesla - pravděpodobně s pomocí spywaru nasazeného do jejich počítačů. V účtech pak změnili nastavení umožňující automatické přeposílání pošty na jiný e-mail. [10]

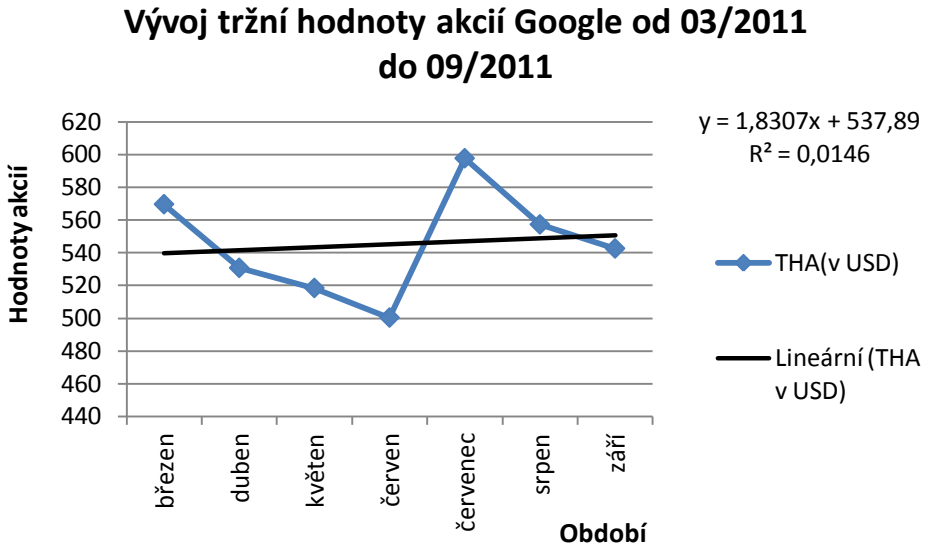
V následující tabulce a grafu vidíme hodnoty tržních hodnot akcií společnosti od března 2011 do září 2011 včetně. Tržní hodnoty akcií jsou vždy uváděny přibližně k datu, které je uprostřed měsíce, není-li sobotou či nedělí.

Tabulka 13: Tržní hodnoty akcií Google od 03/2011 do 09/2011

Období	Březen	duben	květen	červen	Červenec	srpen	září
THA(v USD)	569,56	530,7	518,42	500,37	597,62	557,23	542,56

Zdroj: vlastní úprava dle [5]

Graf 13: Vývoj tržní hodnoty akcií Google od 03/2011 do 09/2011



Zdroj: vlastní úprava dle [5]

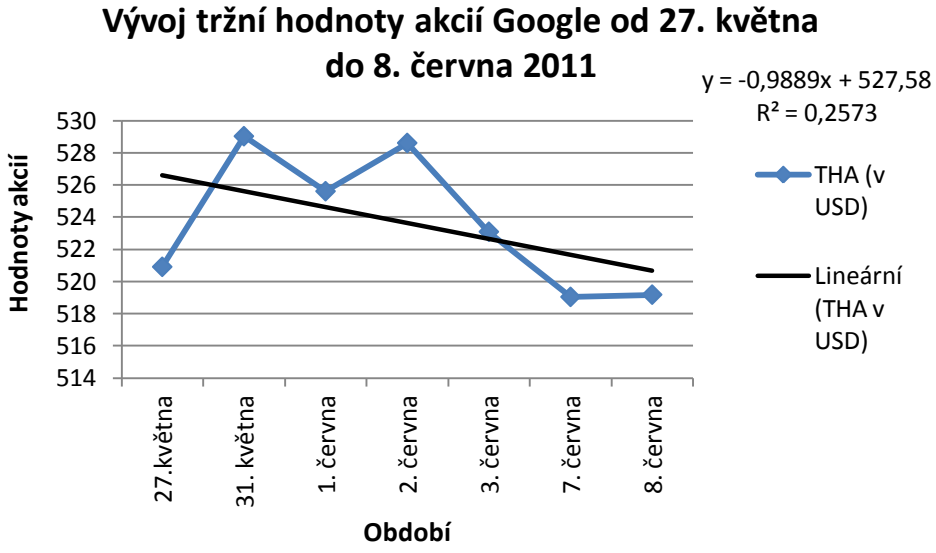
Následující tabulka a graf vyjadřují období bezprostředně před útokem a bezprostředně po něm, tedy období od 27. května do 8. června 2011.

Tabulka 14: Tržní hodnoty akcií Google od 27. května do 8. června 2011

Období	27.května	31. května	1. června	2. června	3. června	7. června	8. června
THA (v USD)	520,9	529,02	525,6	528,6	523,08	519,03	519,17

Zdroj: vlastní úprava dle [5]

Graf 14: Vývoj tržní hodnoty akcií Google od 27. května do 8. června 2011



Zdroj: vlastní úprava dle [5]

Z grafů č. 13 a 14 je viditelné, že tento teroristický kybernetický útok tržní hodnoty akcií nijak neovlivnil. Naopak je zde viditelné dobré hospodaření společnosti. Můžeme tak soudit z viditelného systematického zvyšování tržní hodnoty akcií společnosti.

5.2.3 Vyhodnocení obou útoků na společnost Google

V následující tabulce a grafu vidíme hodnoty tržních hodnot akcií společnosti od prosince 2009 do července 2011. Tržní hodnoty akcií jsou vždy uváděny přibližně k datu, které je uprostřed měsíce, není-li sobotou či nedělí.

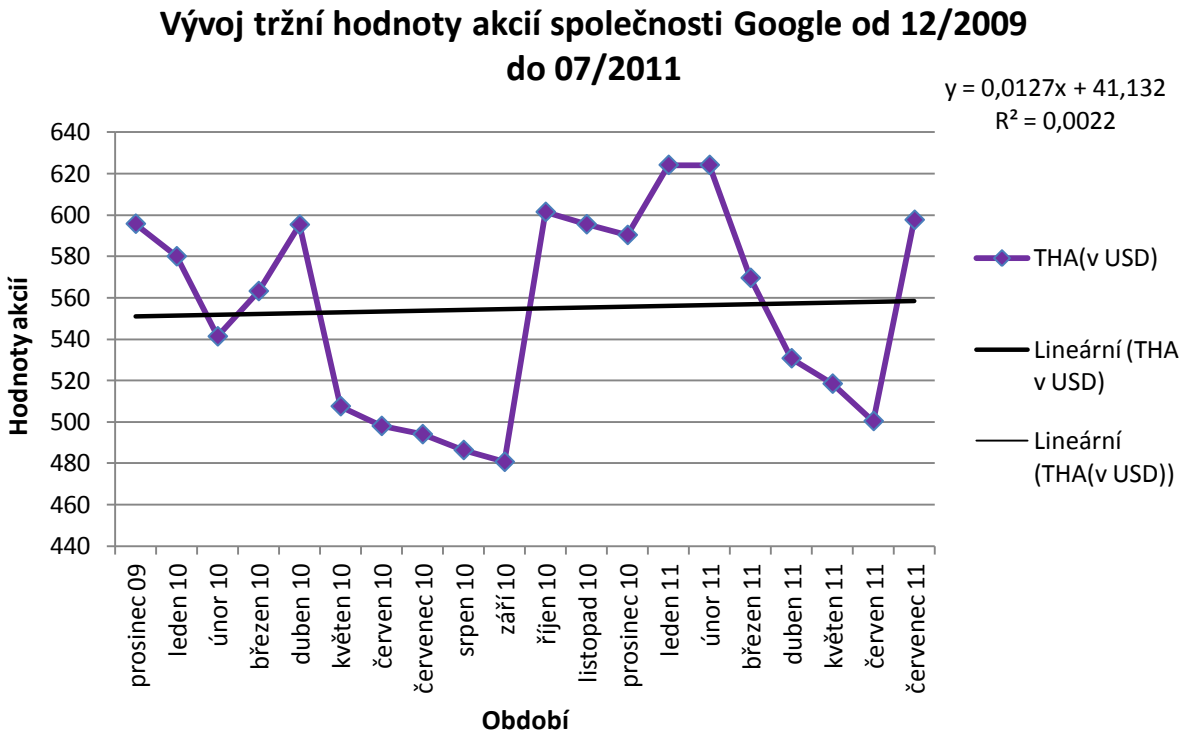
Tabulka 15: Tržní hodnoty akcií společnosti Google od 12/2009 do 07/2011

Období	prosinec 09	leden 10	únor 10	březen 10	duben 10	květen 10	červen 10	červenec 10	srpen 10	září 10
THA(v USD)	595,73	580	541,3	563,18	595,3	507,53	497,99	494,02	486,35	480,64

Období	říjen 10	listopad 10	prosinec 10	leden 11	únor 11	březen 11	duben 11	květen 11	červen 11	červenec 11
THA(v USD)	595,73	580	541,3	563,18	595,3	507,53	497,99	494,02	486,35	480,64

Zdroj: vlastní úprava dle [5]

Graf 15: Vývoj tržní hodnoty akcií společnosti Google od 12/2009 do 07/2011



Zdroj: vlastní úprava dle [5]

V grafu č. 15 můžeme vidět dlouhodobý vývoj tržních hodnot akcií od prosince roku 2009 do července roku 2011. V grafu je velice dobře viditelný účinek obou teroristických kybernetických útoků. Po útoku v lednu roku 2010 je vidět pokles tržní hodnoty, ale jen do měsíce února, což není způsobeno útokem, ale výkyvem, který je na burze cenných papírů naprosto běžný. Ale další kybernetický útok, který proběhl v červnu roku 2011, se očekávaným snížením tržní hodnoty akcií nepodepsal. Z toho vyplývá, že nemůžeme říci, že kybernetický terorismus ovlivňuje tržní hodnoty akcií na burzách.

6 HLAVNÍ POZNATKY

Hlavním poznatkem mé bakalářské práce je to, že vybrané kybernetické útoky na akciové společnosti jak v České republice, tak v zahraničí nijak neovlivňují tržní hodnoty akcií společností.

Na tuto skutečnost se můžeme dívat ze dvou úhlů pohledu. Prvním úhlem pohledu je ten, že řekneme, že kybernetické útoky nebyly dostatečně silné, nebo měly být jen výstrahou pro napadené společnosti. Pokud byly jen výstrahou, pak by společnosti měly začít pracovat na silnějším obranném systému, které by v případě dalších útoků, které mohou být buď stejně silné, nebo ještě silnější, odolaly. Druhým úhlem pohledu je situace, kdy můžeme tvrdit, že obranný systém, jak českých tak i zahraničních společností je dostatečně silný. Tento úhel pohledu je, ale dle mého názoru ten horší. Protože pokud se společnosti nebudou zdokonalovat v obraně před hrozbou kybernetického terorismu, tak toho teroristické skupiny využijí a budou nadále páchat útoky, které budou postupně nabývat na intenzitě.

ZÁVĚR

Práce je složena ze šesti hlavních kapitol, kde první tři kapitoly, lze považovat za teoretické. V těchto teoretických kapitolách je přiblížen terorismus obecně, dále zde nalezneme jednoduchý popis trhu s akciemi a ve třetí je kapitole je podrobně popsán terorismus kybernetický.

Ze zjištěných a zanalyzovaných údajů nemůžeme tvrdit, že se kybernetický terorismus podílí na změnách, tedy hlavně na poklesech, tržních hodnot akcií akciových společností. Očekávala jsem relativně velkou spojitost mezi kybernetickými útoky a tržními hodnotami akcií společností, ale spojitost není žádná.

Závěrem tedy můžu říci jen to, že kybernetický terorismus žádným způsobem neovlivňuje tržní hodnoty akcií na burzách cenných papírů a že akciové společnosti, které byly analyzovány v této práci by měly zapracovat na obranných systémech proti kybernetickému terorismu.

První cíl, tedy popis terorismu a zejména terorismu kybernetického byl splněn v kapitole 1 a 3. Dalším cílem, kterým byl stručný popis trhu s akciemi je obsažen v kapitole 2. Posledním cílem této práce bylo zjistit, jak a zda vůbec kybernetické útoky ovlivňují hodnoty akcií vybraných institucí a tento cíl byl splněn v kapitole 4 a 5.

POUŽITÁ LITERATURA

[1] Akcie.cz. *Akcie online: informace pro Vaše úspěšné investice* [online]. 2010 [cit. 2013-07-26]. Dostupné z: http://www.akcie.cz/kurzy-cz/graf/akcie-717-komercni-banka/

[2] Akcie.cz. *Akcie online: informace pro Vaše úspěšné investice* [online]. 2010 [cit. 2013-07-26]. Dostupné z: http://www.akcie.cz/kurzy-cz/akcie-302-ceska-sporitelna/

[3] Akcie.cz. *Akcie online: informace pro Vaše úspěšné investice* [online]. 2010 [cit. 2013-07-26]. Dostupné z: http://www.akcie.cz/kurzy-svet/akcie-69905-visa-inc-visa-inc/

[4] Akcie.cz. *Akcie online: informace pro Vaše úspěšné investice* [online]. 2010 [cit. 2013-07-26]. Dostupné z: http://www.akcie.cz/kurzy-svet/akcie-65390-mastercard-inc/

[5] Akcie.cz. *Akcie online: informace pro Vaše úspěšné investice* [online]. 2010 [cit. 2013-07-26]. Dostupné z: http://www.akcie.cz/kurzy-svet/akcie-61911-google-inc-class-a/

[6] BELFER, Mitchell A. *Terorismus: pokus o porozumění*. Vyd. 1. Editor Emil Souleimanov. Praha: Sociologické nakladatelství (SLON), 2010, 345 s. Knižnice Sociologické aktuality, 20. sv. ISBN 978-807-4190-384.

[7] Britské listy. *Společnost Google po útoku pohrozila, že ukončí spolupráci s Čínou* [online]. 2010-01-13 [cit. 2013-07-26]. Dostupné z: http://blisty.cz/art/50769.html

[8] Clarke, R.A.Strategie války proti terorismu. Praha: Alfa Publishing, s.r.o., 2005. ISBN:80-8651-14-1

[9] ČT 24. *Akcie ČSOB na tuzemské burze budou chybět* [online]. Praha, 2011-07-27 [cit. 2013-07-26]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/131322-akcie-csob-na-tuzemske-burze-budou-chybet/

[10] DATARAMA: Aktuálně.cz. *Google hlásí phishingový útok na Gmail, přišel z Číny* [online]. 2011-06-02 [cit. 2013-07-26]. Dostupné z: http://datarama.aktualne.centrum.cz/clanek.phtml?id=702365

[11] Idnes.cz: Zprávy. Operace odplata: fanoušci WikiLeaks zahájili kybernetickou pomstu[online]. 2010 [cit. 2013-07-26]. Dostupné z: http://zpravy.idnes.cz/operace-odplata-fanousci-wikileaks-zahajili-kybernetickou-pomstu-10b-/zahranicni.aspx?c=A101209_1496218_zahranicni_btw

[12] JÍLEK, Josef. *Akciové trhy a investování*. 1. vyd. Praha: Grada, 2009, 656 s. Finance (Grada). ISBN 978-80-247-2963-3.

[13] Kolektiv autorů, Terorismus a my ochrana před hrozbou moderní doby. Praha: Computer Press, 2001. ISBN 80-7226-584-9

[14] LinuxEXPRES. *Hacker vs. cracker: Kdo jsou hackeři a čím se liší od crackerů* [online]. 2008 [cit. 2013-07-26]. Dostupné z: http://www.linuxexpres.cz/blog/hacker-vs-cracker

[15] MIKO, Karel. DCIT a.s. [online]. 2009 [cit. 2011-05-19]. Hacking – Jak reálná je tato hrozba? Jak se jí bránit?. Dostupné z: http://www.dcit.cz/cs/system/files/eTime_Miko.pdf.

[16] Ministerstvo vnitra ČR: Typologie terorismu. ODBOR BEZPEČNOSTNÍ POLITIKY. [online]. 2009 [cit. 2013-06-06]. Dostupné z: http://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d

[17] Novinky.cz. *Internetové bankovnictví zkolabovalo, další kybernetický útok mířil na banky*[online]. Praha, 2013-03-06, 2013-03-06 [cit. 2013-07-26]. Dostupné z: http://www.novinky.cz/internet-a-pc/295187-internetove-bankovnictvi-zkolabovalo-dalsi-kyberneticky-utok-miril-na-banky.html

[18] SOULEIMANOV, Emil. *Terorismus: válka proti státu*. Vyd. 1. Praha: Eurolex Bohemia, 2006, 394 s. ISBN 80-868-6176-7.

[19] The Jargon File. *Cracker* [online]. 2013, 2013-03-10 [cit. 2013-07-26]. Dostupné z: http://catb.org/~esr/jargon/html/C/cracker.html

[20] Trhy.měšec.cz: Průvodce-České akciové trhy. [online]. [cit. 2013-06-06]. Dostupné z: http://trhy.mesec.cz/pruvodci/ceske-akciove-trhy/

[21] Typ a zdroje terorismu. [online]. [cit. 2013-06-06]. Dostupné z: http://www.mestovsetin.cz/bezpeci/brevir/static/dokumenty/prestupky_a_trestne_ciny/terorismus/terorismus.htm

[22] Zeman, J. Terorismus historicko-psychologická studie. Praha: Nakladatelství TRITON, s.r.o., 2002. ISBN 80-7254-305-9