UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2015 – 2016

BAKALÁŘSKÁ PRÁCE

Lubomír Černý

Kyberterorismus a kybernetická kriminalita

Praha 2016

Vedoucí bakalářské práce: PhDr. Aleš Zoubek, Ph.D.

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED STUDIES

2015 - 2016

BACHELOR THESIS

Lubomír Černý

Cyber terrorism and cyber crime

Prague 2016

The Bachelor Thesis Work Supervisor: PhDr. Aleš Zoubek, Ph.D.

Prohlášení

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

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne …… Lubomír Černý

Poděkování

Na tomto místě bych rád poděkoval panu PhDr. Alešovi Zoubkovi, Ph.D. za odborné vedení a pomoc při zpracování bakalářské práce.

Anotace

Bakalářská práce popisuje problematiku kybernetických útoků a kyberterorismu. Práce je rozdělena na část teoretickou a praktickou. V teoretické části vysvětlím pojmy související s kybernetickým prostorem a popíši různé hackerské činnosti související s možnými útoky. V praktické části se budu věnovat konkrétním kybernetickým útokům, které byly označeny jako kybernetická válka, a které směřovaly na objekty kritické infrastruktury. Vzhledem k nejednotnému přístupu počítačových expertů a nejednotné terminologii pouze nastíním tuto problematiku. Pravdou ale je, že kyberterorismus patří mezi největší nebezpečí 21. století.

Klíčová slova

Hacker, kritická infrastruktura, kyberkriminalita, kybernetická bezpečnost, kybernetický útok, terorismus.

Annotation

Bachelor's thesis describes the problem of cyber attacks and cyber terrorism. The work is divided into theoretical and practical. The theoretical part will explain concepts related to cyberspace and the description of the various hacking activities related to possible attacks. In the practical part I will deal with specific cyber attacks, which were labeled as cyber war, and which were directed at critical infrastructure facilities. Due to the inconsistent approach of computer experts and inconsistent terminology just outline this issue. The truth is, that cyber terrorism are among the greatest dangers of the 21st century.

Keywords

Hacker, critical infrastructure, cybercrime, cyber security, cyber attack, terrorism.

OBSAH

ÚVOD

V dnešní době vzrůstá závislost jednotlivců, veřejných a státních institucí i jednotlivých států na komunikačních a informačních technologiích. Přímo úměrně tím vzrůstá i nebezpečí s nimi spojené. Celosvětové propojení počítačovou sítí, příkladem je internet, umožňuje každému připojenému účastníku ovlivnit de facto každý systém, který je do této sítě zapojený. Každý účastník tím získá vysoký potenciál ovlivnit významné až strategické cíle v rámci mezinárodní bezpečnosti.

V posledních letech se kromě destruktivních útoků čím dál více objevují kybernetické útoky[1] zaměřené na přerušení komunikačních schopností a omezení fungování protivníka. Velmi rozšířené jsou krádeže strategických dat a informací na vnitrostátní a mezinárodní úrovni.

Téma bakalářské práce jsem si vybral pro jeho aktuálnost. Počítač se stal součástí téměř každé domácnosti a většina lidí ho využívá i v práci. Spoléháme se na to, že spolehlivě a bezchybně vykoná práci, která mu je zadána. S naší závislostí na informačních a komunikačních technologiích stoupá i riziko jejich zneužití. Proto je nutné zabývat se kyberbezpečností. Rád bych ve své práci demonstroval, jak je tato bezpečnost důležitá.

Cílem teoretické části práce je popsat historický i současný pohled na kybernetický prostor a na nebezpečí s ním spojené.

Cílem praktické části je analyzovat kybernetické útoky na modelových případech. Tyto případy budou analyzovány s důrazem na kontext. Kontext je prvek, který umožní alespoň částečně zúžit okruh možných aktérů a motivací k útokům. Úkolem práce je analyzovat okolnosti vzniku útoku a popsat dopady na společnost.

[1]Využívání kybernetického prostoru pro vedení konfliktů není tak novodobou záležitostí, jak bývá někdy prezentováno. Děje se tak de facto od doby, kdy začaly být informační a komunikační systémy implementovány a používány pro činnosti, jejichž narušení může způsobit nějakou reálnou škodu či negativní reálný zásah. Například již v roce 1986 východoněmečtí hackeři sbírali informace z tisíců počítačů Spojených států, které následně prodávali KGB.

Vzhledem k nejednotnému přístupu počítačových expertů a nejednotné terminologii je záměrem práce diskutovat a pokusit se vymezit význam kybernetického útoku a s ním souvisejících pojmů jako kybernetický prostor, kybernetická kriminalita, hacktivismus, kybernetický terorismus. Kybernetický útok může mít různé charakteristiky, aktéry, cíle a může být proveden v různých kontextech, proto i vymezení tohoto pojmu může být rozmanité.

V teoretické části využívám metody popisu, v praktické části byla použita metoda deskriptivně analytická. V rámci celé práce pak budou řešeny výzkumné otázky:

1. Jakým způsobem je v současné době chápán pojem kybernetického prostoru? Jaké je obecné chápání kybernetického útoku a kyberterorismu v bezpečnostních studiích?
2. Za jakých okolností a s jakými následky proběhly popsané kybernetické útoky?

Teoretická část práce vychází ze současné odborné literatury a odborných textů. Analytická část čerpá informace ze sekundárních zdrojů - články z odborných a novinových periodik a komentářů odborné veřejnosti.

Praktickým záměrem práce je popsat nebezpečí kybernetického prostoru a zdůraznit nutnost správného používání informačních a počítačových technologií jednotlivci.

I. TEORETICKÁ ČÁST

TERORISMUS

Slovo terorismus vzniklo z latinského slova „*terrere*“[2], což znamená šíření strachu a hrůzy. Toto slovo se rozšířilo v Evropě ve čtrnáctém století a jako první bylo ve spojení s násilím použito ve Francii za vlády Ludvíka XIV. Při velké francouzské revoluci, kdy se král snažil, aby neztratil svou moc a použil proti lidu vojáky a násilí. Později slovo přijala i angličtina „terrorism“ a odtud i český jazyk. Terorismus má mnoho definic, existuje více než sto různých vysvětlení. Dá se říci, že co stát to jiný výklad. Definice se různě upravovala zvláště podle toho, jak se samotný terorismus vyvíjel.

Terorismus je charakterizován jako systematické páchání násilí k vyvolání strachu proti vládám, skupinám obyvatel či jednotlivcům. Je brán jako nástroj k prosazování politických cílů, které mohou využívat vlády, pravicové i levicové strany, různé organizace, národnostní a etnické skupiny, revolucionáři a jiní. V článku číslo jedna Rámcového rozhodnutí Rady Evropské unie ze dne 13. června 2002 o boji proti terorismu se definuje terorismus jako „úmyslné jednání, které může vzhledem ke své povaze nebo souvislostech závažně poškodit zemi nebo mezinárodní organizace, bylo-li spácháno s cílem, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo mezinárodní organizace, aby jednala způsobem, nebo aby se jednání zdržela, nebo závažným způsobem destabilizovala či zničila základní, politické, ústavní, hospodářské či sociální struktury země nebo mezinárodní organizace“.[3]

Je mnoho způsobů, jakými se terorismus může projevit. Patří sem úmyslné jednání, například poškození jedné organizace nebo rozsáhlé poškození vládních nebo veřejných zařízení, včetně informačního systému nebo narušení či přerušení dodávek elektřiny či vody, jehož důsledkem je ohrožení životů a zdraví lidí. Pokud dojde k napadení prostřednictvím počítače na dálku, budeme hovořit o kyberterorismu.

[2]*Halonoviny.* [Online] 2014. [cit:: 2015-12-22]. Dostupné z: http://www.halonoviny.cz/articles/view/16724657.

[3]Rámcové rozhodnutí Rady Evropské unie 2002/475/SVV o boji proti terorismu

1.1 KYBERNETICKÝ PROSTOR

Kyberprostor, anglicky *cyberspace*, byl poprvé jako termín použit na počátku osmdesátých let v povídce Vypálit chrom od Wiliama Gibsona. Slovo kyberprostor použil ještě v roce 1984 ve svém sci-fi románu Neuromancer, kde jej definuje jako „*Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům…grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Jako světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. Jako světla velkoměsta vzdalující se.“*[4] Je to imaginární prostor, který je tvořen a zpracováván počítačovými daty a je přístupný pouze našemu vědomí. Fyzicky neexistuje, ale má jasně daný začátek a konec, například zapnutím a vypnutím počítače. První, kdo použil termín kyberprostor v souvislosti s počítačovými a telekomunikačními sítěmi, byl spoluzakladatel mezinárodní neziskové společnosti Electronic Frontier Foundation John Perry Barlow.

Kyberprostor neboli virtuální realitu nebo také metaforicky internetovou síť nelze jednoduše definovat. Existuje až 28 různých definic kyberprostoru, ale vědci a odborníci z celého světa nejsou schopni jej přesně definovat. V současné době se popisuje jako „globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra“, je to nehmotný prostor či svět, který je vzájemně propojen s ostatními počítači v síti. Navzájem si vyměňují data a informace v komunikačním systému. Do kyberprostoru je přístup omezen různými faktory především technickým a obsahovým. Lze říci, že v tomto prostoru je možno vytvářet, uchovávat, mazat a navzájem si vyměňovat informace. Uživatelské rozhraní je zlomem mezi světem reálným a světem virtuálním, který se zjevuje skrze monitor počítače, televize, tabletu, notebooku a dnes tak rozšířených a oblíbených chytrých mobilních telefonů.[5]

[4]GIBSON, W., překlad NEFF, O. *Neuromancer*. Praha : Laser, 2010. ISBN: 80-85601-27-3

[5]*Revue pro média.* [Online] 2001. [cit: 2015-12-22]. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm.

1.2 KYBERTERORISMUS

Hovořit o kyberterorismu můžeme v případě, když cílem teroristů je útok na informační, elektronické či telekomunikační systémy. V současné době neexistuje obecná definice kyberterorismu. Jeho podstata ale zní „počítačový útok může být definován jako kyberterorismus, pokud jsou jeho následky narušující nebo dostatečně zničující a vyvolávají strach srovnatelný s teroristickým útokem“.

Podle Evropské unie má v dnešní době informační technologie velkou roli. Především k šíření ideologií, které jsou pro teroristy živnou půdou pro výcvik a výuku teroristických postupů. „ *Moderní informační a telekomunikační technologie hrají důležitou roli při šíření hrozby terorismu. Zejména internet je levný, rychlý, snadno přístupný a má prakticky celosvětový dosah. Všechny tyto výhody vysoce oceňované občany dodržujícími zákon, kteří využívají internet ve svém každodenním životě, jsou bohužel zneužívány teroristy. Ti používají internet jako prostředek šíření propagandy zaměřené na mobilizaci, nábor a dále na šíření pokynů a on-line příruček určených k výcviku nebo plánování útoků. Obojí je určeno současným a potencionálním sympatizantům. Tímto způsobem internet slouží jako jeden z hlavních urychlujících faktorů procesů radikalizace a náboru; také slouží jako zdroj informací o teroristických prostředcích a metodách, čímž funguje jako „virtuální výcvikový tábor“. Šíření teroristické propagandy a teroristických znalostí pomocí internetu doplňuje a rozšiřuje indoktrinaci a výcvik prováděné jinak než pomocí internetu a přispívá k rozvoji silnější a širší platformy teroristických aktivit a sympatizantů. “*[6] Evropská Rada Úmluvy požaduje, aby státy zajistily, aby podněcování k páchání teroristického trestného činu nebo nábor a výcvik terorismu bylo trestné. Tyto trestné činy patří do oblasti tzv. informační trestné činnosti.

Asymetrické hrozby, je pojem, který se objevil počátkem devadesátých let. Důvodem tohoto pojmu byl fakt, že vyspělé státy, které jsou na vysoké technologické a ekonomické úrovni, se nemohou dostatečně bránit útokům ze zemí třetího světa. Vyspělé státy nejčastěji napadají rozvojové země nebo útočníci organizovaní v malých skupinách, ale i jednotlivci sympatizující s teroristy nebo člověkem duševně nemocným. Dnes, kdy je trh

[6]SMEJKAL, V., *Kybernetická kriminalita*, Plzeň: Aleš Čeněk, 2015. 84 s. ISBN 978-80-7380-501-2

takřka přesycen elektronikou, mohou útočníci zaútočit na citlivá místa, data a systémy technologicky vyspělejších protivníků. Pokud dojde k napadení energetického, dopravního, bankovního systému technologicky vyspělejšího státu nebo k jeho počítačové paralýze, mluvíme o tzv. kybernetické válce. Celosvětově klesají ozbrojené konflikty mezi státy, alespoň podle statistik, a zvyšují se bezpečnostní hrozby a rizika nekonvenční povahy. Asymetrické hrozby jsou v současnosti jedním s nejžhavějších celosvětových témat, jde o napadení technologicky vyspělejšího cíle, kdy útočník využívá a překonává slabých bezpečnostních míst sytému za použití různých metod lišících se od běžných konvenčních metod vedení operací. Kybernetická válka není jen novým fenoménem působení teroristů, ale i států s důvěryhodnou pověstí. Jednotlivé státy se snaží chránit proti útokům vedených v kyberprostoru, které ohrožují ať už světovou nebo národní bezpečnost.

V polovině sedmdesátých let se poprvé objevil termín informační válka, který použil Thomas Rona ve studii „ Weapons System and Information War“, k označení boje rozhodovacích systémů. Informační válka je pojem, který je různými autory chápán a vysvětlován rozdílně. A.Rathmell ve své práci " Information Warfare: Implication for Arms Control" obecně definuje informační válku jako boj o kontrolu nad informačními aktivitami. Velkým důrazem ukazuje na rozvoj a rostoucí závislost lidstva na získávání a konzumaci informací, růst a rozvoj informačních sítí. Podle Rathmella lze informační válku rozdělit minimálně do tří rovin.

1) Jde o boj při použití psychologických, mediálních, diplomatických a vojenských technik a nástrojů pro ovlivňování mysli protivníka.

2) Jde o koncept RMA - koncept informační války za využití vojenských sil ovládnout informační spektrum.

3) Jde o moderní boj války za pomocí elektronických úderů, jako je hacking, nebo psychologických operací, které vedou k fyzickému zničení.

Proto lze informační válku rozdělit do dvou kategorií

1) Útoky na informační a komunikační infrastrukturu

- Jsou to útoky na vojenskou infrastrukturu, kdy hlavním cílem je oslabení, narušení, odříznutí jednotek od velení.

2) Útoky na obsah
   - Zde je veden psychologický boj o změnu názorů a postoje lidí. Účelem je zamezit shromažďování a zpracovávání informací.

Útoky, které by narušily či vyřadily informační a komunikační síť se mohou provést dvěma způsoby:

1) Útok za pomocí systémů a bomb EMP/T a HERT, které se shazují na území nepřítele za účelem zničení veškeré elektroniky, následkem je pak zničení procesorů, pamětí, smazání veškerých dat a programů.
2) Útoky vedené v kybernetickém prostoru za pomocí programů, příkazů, kde hlavním cílem jsou elektronická data. O tomto způsobu mluvíme jako o kybernetické válce.

Existují tři možné útoky:

a) DoS útok (Denial of Service) - odepření služeb
b) DoC útok (Denial of Capability) - odepření schopností
c) TC útok (Taking Control) - převzetí kontroly

Kyberterorismus nerozdělujeme podle účelu či podle útočníků, ale podle použitých prostředků. Jak jsem již psal, kyberterorismus je protiprávní útok proti počítačům a počítačovým sítím za účelem zastrašit, přinutit ať už vládu nebo lid k prosazování politických a sociálních cílů.

Kyberterorismus, aby mohl být kvalifikován jako útok, musí mít za následek násilí proti osobám nebo poškození majetku. Útok vede k oslabení ekonomiky a infrastruktury nebo k lidským ztrátám.

Rozdělení znaků kyberterorismu podle typologie

1) Primární znaky
   - Psychologické útoky jsou vedeny na civilní cíle a lid v širším kruhu
   - Vnesení zmatku a vytvoření nejistoty
   - Široká publicita prostřednictvím medií
2) Sekundární znaky
   - Použití prostředků informační a komunikační techniky
   - Cílení na informační a komunikační systémy
   - Opakovatelnost a možnost opakovaného útoku
3) Terciální znaky
   - Útoky na hardware
   - Politické motivy
   - Velký dopad i za participace malé skupiny
   - Snadná finanční dostupnost
   - Snadná distribuce útoku
   - Státem sponzorované skupiny

Kromě kyberterorismu a informační války existuje ještě tzv. elektronický boj (Elektronic Warfare), zkráceně EW, a informační operace (Information Operation) zkráceně IO. EW a IO jsou způsoby vedení informační války, které jsou zaměřeny na kryptografii, stenografii, radarové rušení výškového leteckého průzkumu, elektronické zaměřování a získávání zpravodajských informací. EW a IO použila například americká armáda v roce 1991 při operaci „Pouštní bouře“. Během války v Iráku zavedla viry do počítačů a řídících center Irácké republikánské gardy, což mělo za následek ochromení startů a zaměřování spojeneckých cílů raketami SCUT.

Je tudíž otázkou, zda kyberterorismus není součástí kybernetické kriminality, protože zavedení a napadení počítače virem či škodlivým červem patří do této oblasti. K tomu se přiklání řada autorů této problematiky. Chybí zde vydírání, podvod nebo krádež identity, ale zato ovlivňuje celou společnost. V současné době převládají bombové útoky, jejichž cílem je násilí na nevinných civilistech, nad kyberterorismem.

1.2.1 PACHATEL KYBERNETICKÉHO ÚTOKU

Pachatelem trestného činu je podle trestního zákona osoba, která svým jednáním naplnila znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, jeli trestná. Pachatel je i ten, kdo k provedení činu zneužil takové osoby, která není trestně odpovědná pro svůj věk, nepříčetnost nebo proto, že jednala v nutné obraně, v krajní nouzi nebo za jiných okolností vylučující protiprávnost.

Pachatele lze rozdělit:

1) Individuální útočník
2) Ideologicky motivovaný útočník
3) Útočník v oblasti státního terorismus

Individuální útočník

Do této kategorie patří útočníci, kteří především chtějí uspokojit svoje ego, chtějí zažít pocit moci nebo se mstít a poškodit svého zaměstnavatele či jinou osobu. Tyto útoky lze kvalifikovat jako počítačovou kriminalitu. Pokud ovšem hacker provádí útok, který je politicky nebo jiným způsobem motivován, můžeme ho označit jako teroristický.

Ideologicky motivovaný útočník

Ideologicky motivovaní útočníci provádí své útoky různými způsoby. Nejčastějším způsobem útoku je napadení webových stránek. Jejich útoky mohou vést k narušení komunikační a informační infrastruktury.

Hacker

Hacker je člověk, který žije ve virtuálním světě. Hacker propaguje především svobodu, sílu jednotlivce, nesnáší omezování a autoritu. Je to osoba s hlubokými znalostmi počítačových systémů, výpočetní techniky, programování, přenosových protokolů. Opravdivý hacker nezneužívá své schopnosti k ničení, svým jednáním pouze zkoumá a učí se, tzn. nemění obsah internetových stránek. Existují i tací, kteří zneužívají svých znalostí ke svému obohacení a k negativnímu ovlivnění svého cíle. Nedá se proto

říci, že jde o skutečný hacking, ale jen o jeho okraj. Tyto lidi označujeme jako phiseři, crackeři nebo prostě počítačoví kriminálníci[7].

Pro hackera je nejdůležitější detailní znalost v oblasti počítačových systémů a především znalosti UNIXu[8]. Celý internet a veškeré důležité části v IT běží a točí se kolem UNIXu. UNIX je programové jádro všeho virtuálního v počítačové síti a v technických prostředcích. Tím, jak se vyvíjí svět počítačů, zvyšují se i znalosti a dovednosti hackerů. Hackerským jazykem se tak stává programovací jazyk a dalo by se říci, kolik programovacích jazyků znáš, tolikrát jsi hackerem. Existuje mnoho programovacích jazyků, základem je programovací jazyk C a C++. Hacker ke své práci využívá znalosti i dalších jazyků, například PHP, Java, SQL databáze.

Cracker

Cracker je osoba, která jedná vždy s úmyslem zaútočit. Zabývá se prolamováním hesel, databází, nabouráváním do licenčního mechanismu, ničením či pozměňováním dat nebo jejich odcizením, snaží se získat licenční kódy. Do napadnutého sytému zavádí viry a snaží se získat co nejvíce osobních dat.

Phreaker

Slovo pheaker vzniklo spojenín dvou slov „phone“ a „cracker“. Jde o osobu, která provádí trestnou činnost pomocí nezákonného využívání telefonní sítě. Tyto osoby se vyskytovaly ještě dříve než hackeři nebo crackeři. Dokázali za pomocí frekvenčních tonů v pásmu 2 600 Hz ovlivnit nebo ovládat telefonní ústřednu. Mohli tak zdarma volat, získat kredit pro volání, dokázali odposlouchávat hovory nebo využívat síť k odběru proudu bez placení.

Státní terorismus

Do této kategorie patří útoky státních hackerů, crackerů.

---

[7]HARIS, S., HARPER, A. a EAGLE, CH. *Hacking - Manuál hackera.* Praha : Grada Publishing a.s., 2008. 5 s. ISBN 978-80-247-1346-5.

[8]*Revue pro média.* [Online] 2001. [cit: 2015-12-22]. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm.

2. POČÍTAČOVÁ KRIMINALITA,KYBERKRIMINALITA

Kriminalita

Kriminalitu lze obecně chápat jako protiprávní jednání osob páchající přestupek nebo jiný trestný čin. Co není zakázáno, je dovoleno. Tato věta říká, že, co není napsáno v zákoně z hlediska přestupků, v tzv. Přestupkovém zákoně č. 200/1990 Sb. a Trestním zákoníku č.40/2009 Sb., můžeme udělat cokoliv. Kriminalitou se zabývá celá řada oborů.

Počítačová kriminalita

Je trestná činnost, jejíž útok je veden pomocí počítače. Útok je veden na hardware, software či jiná data, která jsou uložena v počítači nebo v počítačové síti. Může dojít k útoku i na data přenášená pomocí kabelového připojení nebo bezdrátového spojení pomocí přenosných disků a USB disků.

Historie

Na začátku rozvoje počítačů byla počítačová kriminalita, jak po technické, tak po uživatelské stránce téměř nemožná. Počítače nebyly na takové úrovni, jak je známe dnes a internet neexistoval. Počítače byly tak velké, že se nevešly do větší místnosti a jejich provoz byl omezen jen na několik minut z důvodu přehřívání. Počítače se nejprve využívaly především ve velkých firmách pro složité výpočty nebo pro vědecké výzkumy. Mezi první trestné činy spojované s počítačovou kriminalitou patří takzvané *sabotáže*. Sabotáže se prováděly z různých důvodů, jednalo se též o zaměstnanecké msty. V České republice je jako první trestný čin spojovaný s touto problematikou případ, který se stal v 70. letech, kdy na Úřadu důchodového zabezpečení jeden z úředníků poškozoval záměrně záznamy na magnetických páskách, na které se v té době ukládaly veškeré záznamy a data. Úředník byl odsouzen za sabotáž podle tehdejšího trestního zákona.[9] Na základě těchto skutečností se začaly provádět různá bezpečností opatření, například přímý dohled nad těmito pracovníky.

[9]Trestný čin proti základům socialistické republiky – tyto trestné činy se projednávaly především pro postih odpůrců tehdejšího režimu.

Dalším závažným trestným činem, který se v té době nejčastěji objevoval, byl takzvaný dokladový delikt. Pomocí počítače se falšovaly údaje na dokladech, které pak pomohly zločincům pří manipulaci s penězi. Tento trestný čin byl před rokem 1989 kvalifikován podle tehdejšího trestního zákona § 132 jako „*Rozkrádání majetku v socialistickém vlastnictví*“.[10] Tyto trestné činy jsou dnes podle trestního zákona § 209 a § 230 kvalifikovány jako neoprávněný přístup k počítačovému systému a nosičům informací.[11] Pro zločince to znamenalo pokusit se měnit údaje přímo v počítačovém systému, což obvykle vyžadovalo mít přímý a neustálý přístup do počítače. Tato počítačová kriminalita patřila mezi latentní kriminalitu. Důvodem byl takzvaný počítačový čas, nebylo totiž možné žádným způsobem dokázat, že bylo něco ukradeno.

Zlom v oblasti počítačové kriminality a bezpečnosti přišel v době příchodu osobních počítačů do domácností a připojením do počítačových sítí. Tyto nové technologie vytvořily a umožnily přístup zločincům páchat trestnou činnost.

Objevují se další způsoby páchání trestných činů podvodů, mezi něž patří například phishing, pharming. Dochází k takzvaným DoS útokům, které mají ovlivnit funkčnost a činnost počítačových systémů. Používáním spyweru a malweru se útočníci snaží získat informace, data nebo zprávy, které se posílají skrze počítačovou sít. Trestní zákon takový čin označuje za porušení tajemství dopravovaných zpráv dle § 182 trestního zákona.

Porušování autorských práv je další počítačová trestná činnost. Je též označována jako počítačové pirátství nebo také softwarové pirátství. Do této kriminality patří nelegální kopírování, šíření, plagiátorství programů za účelem vlastního obohacování. Tuto trestnou činnost popisuje náš trestní zákoník přesněji zákon O porušení autorských práv a práv souvisejících s právem autorským a práv k databázi § 270. Dále se můžeme zmínit o § 180 o neoprávněném nakládání s osobními údaji, nebo také § 232 o poškozování záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

[10]Kdo majetek, který je v socialistickém vlastnictví, rozkrádá tak, že a) přivlastní věc z takového majetku tím, že se jí zmocní, b) přivlastnil si věc z takového majetku, která mu byla svěřena, nebo c) ke škodě takového majetku sebe nebo jiného obohatí tím, že někoho uvede v omyl nebo jeho omylu využije, bude potrestán odnětí svobody na šest měsíců až pět let, nebo nápravným opatřením nebo zákazem činnosti nebo peněžitým trestem.

[11]Viz usnesení Nejvyššího soudu ČR, sp. zn. 7 TDO 808/2010 ze dne 25.10 2010

Kyberkriminalita

Kyberkriminalita se liší od počítačové kriminality pácháním trestné činnosti v kybernetickém prostoru. Kyberkriminalitu lze dělit do dvou kategorií:

1) Činy, které nejsou mířené přímo proti samotnému kyberprostoru, například neoprávněný přístup do systému, kdy se útočník snaží získat přístupové heslo a dostat se tak neoprávněně k datům.
2) Trestné činy pevně spojené s kyberprostorem, například tzv. emailový phishingový útok využívající důvěřivosti uživatelů.

Sabotáž

Jak jsem již zmínil, první trestná činnost spojována s počítačovou kriminalitou byla sabotáž. Jde o trestný čin, který spočívá v omezení nebo ve zničení funkčnosti počítače nebo jeho části fyzickým napadením. První taková sabotáž byla provedena ve Francii roku 1801, kdy došlo ke zničení textilních tkacích strojů, které byly programovány pomocí děrných štítků. Při této trestné činnosti se také poprvé objevilo slovo „sabotage“, které je odvozeno od slova „sabot“, dřevák či kopyto.

Původ této trestné činnosti pochází z Anglie z počátku 19. století, kde existovalo hnutí textilních řemeslníků, zvaných Luddistů. Hnutí bojovalo proti automatizaci ve výrobě. Na protest byly ničeny tkalcovské stavy, údajní původci nezaměstnanosti. Trestní zákon definuje počítačovou sabotáž jako čin, který omezuje či znemožňuje funkčnost počítače nebo jeho části nebo jiného zařízení formou fyzického nebo logického útoku. Úmyslem pachatele je poškodit ústavní zařízení nebo obranyschopnost státu nebo jemu na úroveň postaveného subjektu.

3. POČÍTAČE

Počítače

Jako první počítač na světě je uváděné takzvané kuličkové počítadlo. S dnešním počítačem nemělo nic společného, šlo spíše o pomůcku, která měla usnadnit počítání. První opravdový počítač byl analytický stroj, který byl schopen pomocí děrných štítků analyzovat seznam instrukcí. Byl vyvinut kolem 19. století dvojicí panem Charles Babgagem a kněžnou Augustou Adou. Jako počítač můžeme označit každý stroj, kterým lze naprogramovat seznam instrukcí. Dnešní počítač se skládá z určitých jednotek, hardwaru a softwaru. Slouží k uchovávání, zpracovávání, přenosu dat nebo ke komunikaci s uživatelem. Je to stroj, který dokáže přijímat strukturovaný vstup, zpracovává jej podle předepsaných pravidel a jeho výsledkem je výstup.

Počítače lze užít ve všech odvětvích lidské společnosti (kancelářské či databázové aplikace, grafické a řídicí systémy, systémová ochrana dat, programování, hry, zábava, sociální komunikace, …).[12]

3.1 HARDWARE

Každý počítač se skládá z různých komponentů. Liší se podle účelu a výkonnosti. Jiný výkon má osobní počítač (PC) a jiný výkon server, sálový (mainframe) nebo počítač pro řízení procesů. Všechny mají společné výstupní a vstupní zařízení, mezi které patří monitor, klávesnice, myš, kamera, scanner, mikrofon, sluchátka, tiskárna. Každý z nich se dále skládá ze základní desky, speciálních karet (zvuková, sítová, grafická), operační paměti, sběrnice, disků (HDD), napájecích zdrojů. Definice hardwaru zní, že jde o „ *fyzické součásti systému pro zpracování informací nebo jejich část“.*[13]

[12] *Vlastik Chytrák.* [Online] 2001. [cit: 2015-12-22]. Dostupné z: http://www.vlastik.chytrak.cz/definice_pocitace.htm.

[13] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň : Aleš Čeněk, 2015. 24 s. ISBN 978-80-7380-501-2.

3.2 SOFTWARE

Jedná se o nezbytnou součást počítače, bez které nemůže fungovat. Jde o naprogramované instrukce, které způsobují, že hardware pracuje. Definice softwaru zní, jedná *se o sekvenci instrukcí, která je prováděna prostřednictvím počítače.* Tento termín se vztahuje na originální zdrojový kód nebo na proveditelnou verzi strojového jazyka. Termín program vyměřuje stupeň kompletnosti. To znamená, že program ve zdrojovém kódu obsahuje všechny příkazy a soubory nezbytné pro kompletní interpretaci nebo kompilaci. Tento proveditelný program lze vložit do daného prostředí a umožnit mu nezávisle fungovat na ostatních programech.[14] Další definice říká, že jde o „*programy, procedury a pravidla pro zpracování konkrétních úloh na počítači nebo pokyny, jak má počítač danou úlohu řešit“.*[15]

3.3 DATA A DATABÁZE

Data

Slovo data vzniklo z latinského názvu datum, bylo odvozeno od slova *dare*, což znamená dát. Data v počítačovém světě znamenají čísla, zvuk, obraz nebo text. Je to soubor čísel, kterým vyjadřujeme naše myšlení s potenciálem vytvořit z nich informace pro pozdější vyvolání. Proto můžeme data považovat za nositele nejen informací. Data lze ukládat na různé nosiče jako je USB, HDD, DISC. Data lze rozdělit do dvou kategorií podle přístupu k nim, na sekvenční a přímé. Sekvenční přístup k datům znamená takzvané souborové uspořádání, anglicky data file structure a v druhém případě jde o databázový přístup, anglicky direct access.

Definice slova data je vymezená jako „*opakovaně interpretovaná formalizovaná podoba informace vhodná pro komunikaci, vyhodnocování nebo zpracování“.*[16]

[14]MICROSOFT. *Microsoft Press slovník výpočetní technik.* Praha : Plus, 1993 . 301 s. ISBN 80-85297-48-5.

[15]HINDLS, R., HOLMAN, R., HRONOVÁ, S a kolektiv. *Ekonomický slovník.* Praha : A plus, 2003. ISBN: 978-80-903804-5-5.

[16] KUNEŠOVÁ-SKÁLOVÁ, J., SKÁLA, M. *Vymezení pojmu nehmotný majetek.* Praha : Tributum, 1998.

Počítačová data jsou formulovány jako „*jakékoli vyjádření faktů, informací nebo pojmů ve formě pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem*“.[17] Soubor „*obsahuje data ve formě odlišné od souboru programu, obsahujícího proveditelné instrukce*“.[18] Banka dat je definována jako archiv dat nebo jakýkoliv soubor dat.

Databáze

Databáze je soubor informací se společnou vlastností, tzn. pomáhají vyhledávat data podle zadaných kritérií a jejich uspořádání. Lze je rozlišit podle charakteru, autorského zákona nebo zda se nacházejí mimo ochranný režim. Směrnice Evropského parlamentu a Rady 96/9/ES o právní ochraně databází vysvětluje databázi, jako soubor nezávislých děl, údajů nebo jiných prvků, které jsou systematicky nebo metodicky uspořádány, a které jsou jednotlivě přístupné elektronickými nebo jinými prostředky. Slovník výpočetní techniky definuje databázi, jako souhrn dat obsahující určitý počet záznamů. Každá je složena z polí daného typu a ty společně s množinou operací umožnují hledání, třídění, spojování a jiné aktivity. Jako první databáze jsou označovány kartotéky.

3.4 INFORMACE A INFORMAČNÍ SYSTÉMY

Počítač zpracovává informace uložené v databázích, které jsou prezentovány jako data.

Informace

Slovo informace pochází z latiny od slova *informatio*, představa, poučení a podle slova *informare,* tvořit nebo také formovat, upravovat. Dnešní slovníky vyjadřují informaci jako zprávu, sdělení, poučení. Pomocí těchto zpráv někoho informujeme o nějaké situaci nebo věci, vyjadřujeme zmenšení neurčitosti sdělení nebo vyjadřujeme odrazy rozlišností mezi objekty a procesy. „*Informace je jakýkoli energetický či hmotný*

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

[18]MICROSOFT. *Microsoft Press slovník výpočetní technik.* Praha : Plus, 1993. 101 s. ISBN 80-85297-48-5.

projev, který může mít smysl buď pro toho, kdo sděluje, nebo pro toho, kdo sdělované přijímá".[19] Informace jsou data v kontextu, jsou použitelná a srozumitelná. Hodnota informace je součástí procesu transformace dat na informace, proto má subjektivní charakter. Hodnota informace nemá přímou souvislost s případnou cenou dat. Data lze proto kupovat, prodávat a mají různou hodnotu. Pro někoho jsou informace cenné ihned, pro někoho jsou cenné až v době použitelnosti a někdy se můžou ukázat jako bezcenné. Informace proto vnímáme jako data a zpracováním dat získáváme data nová a tedy i nové informace. Informace se mohou předávat na přenosném médiu, papíru, z historie známe i obrazové informace nakreslené na kamenech, stěnách jeskyň, magnetickém pásku nebo přenosu pomocí radiových vln, světla, zvuku, ústně. Za nosiče informací můžeme považovat i jiná zařízení – tablety, GPS, iPody, smartfony a další, tedy všechna zařízení, která dokáží uchovávat nejen digitální informace.

Informační systémy

Informační systémy jsou systémy, které zpracovávají a distribuují informace. Podle definice jde o „*identifikovatelný funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňovaní informací uložených na nosiči v údajových základnách a reprodukovatelných technickými prostředky. Informační systém integruje informační základnu, technické a programové prostředky, technologie, finanční prostředky a procedury a pracovníky".*[20] V České republice jsou známé i pod jinými názvy, například evidence, rejstřík, seznam, registr. Tato označení nemusí být vždy vhodná, protože tyto informační systémy nemusí být vedeny automatizovaně. Jde o systémy, jejichž úkolem je sbírání dat, jejich zpracování, ukládání, vyhledávání a šíření. Zahrnují informační dokumenty, procesy, tvůrce a uživatele. Cílem informačních systémů je lepší podpora informačních a rozhodovacích procesů, které mohou pomoci k řízení podniků a organizací.

[19]MATES, P., MATOUŠOVÁ, M. *Evidence, Informace, systémy – právní úprava.* Praha : Codex Bohemia, 1997 27 s.

[20]Standarty státního informačního systému ČR, ÚSIS, Praha, 1996, 1. díl, 63 s.

3.5 POČÍTAČOVÁ SÍŤ, INTERNET, PŘENOS DAT, UKLÁDÁNÍ DAT, DÁLKOVÝ PŘÍSTUP

Počítačovou sítí neboli sítí vzájemně propojených uzlů označujeme technické a programové prostředky, které mají za úkol spojení a výměnu dat a informací mezi jednotlivými počítači.

Počítačovou síť lze rozdělit do dvou kategorií:

a) Lokální síť, LAN
b) Vzdálená síť, WAN

Pro úplnost se uvádí další komunikační sít tzv. PAN, Personal Area Network, komunikace probíhá mezi zařízeními, které nosíme při sobě – komunikace mezi mobilním telefonem - tabletem – chytrými hodinkami - palubním počítačem.

Lan – Local Arena Network

Je lokální síť, která je v určité vymezené oblasti např. firma, domácnost, uživatel je většinou shodný s provozovatelem sítě. Jde o lokální propojení nezávislé na vnějším připojení, které ovšem komunikuje s jakýmkoliv jiným zařízením v síti. Komunikace uvnitř sítě nepodléhá předpisům o komunikaci, komunikace mimo tuto sít již předpisům podléhá.

WAN – Wide Area Network

Jde o vzdálenou komunikační síť, která spojuje počítače a počítačové sítě na delší vzdálenost. Propojuje geograficky oddělené oblasti. Patří sem internet.

Internet

Lze definovat jako celosvětový systém, který propojuje počítačové sítě, kde dochází ke komunikaci mezi počítači a počítačovými sítěmi pomocí protokolů TCP/IP. Jde o soustavu sítí a podsítí, serverů a dalších různých datových komunikací. Pro současnou dobu je charakteristické vzájemné propojování komunikační a výpočetní techniky – přes Bluetooth a WiFi, přes sítě LAN a WAN a internet. K internetu se lze připojit přes počítač, mobil, tablet i jiné domácí zařízení.

K internetu se lze připojit různými způsoby:

1) Pomocí dnes již už moc nepožívaného analogového připojení dial-up modemu, ISDN – Integrated Services Digital Network, xDSL – Digital Subsriber Line (ADSL, SDSL,HDSL,VDSL)
2) Kabelovou přípojkou – jde o připojení kabelové televize
3) Pomocí optických kabelů FTTx
4) Přenos pomocí elektrické sítě
5) Komunikace pomocí satelitních družic
6) Bezdrátové sítě
7) Mobilní širokopásmové sítě typu GSM, EDGE, UMTS,CDMA, LTE

Internet má široké možnosti a pomocí něj můžeme například číst tiskoviny, sledovat televizi nebo film, poslouchat hudbu, nahlížet do různých slovníků, máme přístup do škol, sociálních sítí, můžeme nakupovat, hrát on-line hry, provádět peněžní transakce, podepisovat smlouvy, vstupovat do státních databází, komunikovat se státní správou, získat návod na výrobu bomb nebo návod na páchání trestné činnosti nebo teroristický útok. Internet může být také nástrojem pro dezinformaci a dezorientaci lidí nepravdivými informacemi.

Přenos dat

Pro komunikaci mezi počítači byl definován tzv. model ISO/OSI. Tento doporučovaný model byl definován v roce 1983 organizací ISO. Komunikace mezi počítači je rozdělena do 7 souvisejících vrstev. Nižší vrstva poskytuje vyšší vrstvě služby bez nedůležitých informací. Data se před přenosem rozdělí do paketů, k těm se pak přidají doplňkové informace nezbytné pro přenos.

Přehled vrstev:

1) Fyzická vrstva
2) Linková vrstva
3) Síťová vrstva
4) Transportní vrstva
5) Relační vrstva
6) Prezentační vrstva
7) Aplikační vrstva

Fyzická vrstva

Umožnuje přenos dat v bitech. Jde o komunikaci, mezi přenosným médiem a technickými prostředky. Definuje fyzické, mechanické, funkční parametry, které se týkají propojení jednotlivých zařízení. Je to hardwarová vrstva.

Linková vrstva

Úkolem je bezchybně přenést data z jednoho počítačového uzlu na druhý, tak aby nedošlo k porušení integrity přenosu. Je to hardwarová vrstva.

Síťová vrstva

Síťová vrstva nám zajištuje přenos dat do síťového uzlu pomocí protokolů pro směrování dat. Je hardwarová, ale když se propojí 2 PC je softwarová.

Transportní vrstva

Přijímá data, která rozkládá na nejmenší jednotky přenášených dat, tedy na pakety, kterým zajištuje přenos. Jejím cílem je, aby se přenášená data přenesla k cíli správně a opakovat zprávu při náhlé chybě nebo porušení. Je to softwarová vrstva.

Relační vrstva

Koordinuje udržení spojení mezi počítači či stanicemi a zajištuje jejich komunikaci. Má funkci zabezpečovací, přihlašovací a správní. Je to softwarová vrstva.

Prezentační vrstva

Definuje, jak mají být data formátována, prezentována, kódována, transformována. Úkolem je správné uspořádání a formát dat tak, aby byla čitelná a přístupná po celé síti. Zajišťuje šifrování a komprimaci dat a kódování znaků. Je to softwarová vrstva.

Aplikační vrstva

Je to nejvyšší vrstva. Tato vrstva definuje, jakým způsobem budou komunikovat programy a aplikace v síti. Je to softwarová vrstva a tvoří rozhraní k vlastnímu programu.

Ukládání dat

Data lze ukládat, jak na HDD neboli Hard Drive Disk, tak na takzvané cloud computing a webová úložiště. Tyto data můžeme sdílet po síti s ostatními uživateli anebo můžeme povolit přístup jen některým uživatelům. Sdílíme soubory či složky pomocí úložišť například Google Drive, Microsoft One Drive, Uložto.cz, Uschovna.cz, Rapidshare, Fastshare. Některé tyto služby jsou dostupné zdarma a některé jsou přístupné za poplatek. Tato úložiště se nejvíce, podle statistik, využívají k šíření pornografie či rasistického nebo jiného trestného obsahu.

Cloud computing

Cloud computing je služba, která nám pomáhá využívat programy a jiné služby na internetu prostřednictvím počítačových serverů, ke kterým můžeme přistupovat odkudkoliv za pomocí webového prohlížeče. Uživatel využívá službu podle typu, definovanou nebo zaplacenou. Existují tři základní služby. První je technologická infrastruktura, kde zákazníka zajímá především výkon, velikost datového úložiště a rychlost sítě. Tato služba dále umožnuje nainstalovat libovolný operační systém a programy. Druhou službou je platforma jako služba, jejímž cílem je možnost využít prostor pro běh vlastních dodaných aplikací a programů, kde poskytovatel zajišťuje prostředí a funkčnost těchto programů. Ve třetí službě jde především o to, že si zákazník pronajímá prostor, aby využil nějaký předem nahraný program, například pro analýzu.

Nevýhody externího ukládání dat

- Data jsou uložená někde na serveru, tudíž nemáme nad těmito soubory kontrolu.
- Data jsou uložená mimo území, kde se nacházíme, mohou tak nastat právní problémy, např. v oblasti zpracování osobních dat.
- Jsme závislí na poskytovateli služby.
- Poskytovatel rozhoduje o tom, co se na cloud computingu děje.

Web hosting

Web hosting je služba, kdy si pronajímáme webový prostor, datový prostor nebo výpočetní výkon serveru.

Servery jsou:

1) Servery virtuální
2) Servery, které poskytovatel provozuje a technicky podporuje.
3) Server, který si sám zákazník spravuje.
4) Vlastní server zákazníka je umístěn do prostoru poskytovatele služeb.

Dálkový přístup

Příchodem osobních počítačů, rozšířením internetu a počítačových sítí, můžeme k těmto systémům přistupovat vzdáleně.

Existuje řada způsobů a programů, které nám to umožnují, například komerční programy TeamViewer, VNC.

4. NÁSTROJE KYBERNETICKÝCH ÚTOKŮ

Je nutné rozlišit co je a co není kyberterorismus. Ne každý, kdo používá výpočetní techniku pro svůj užitek nebo šíří svůj program internetem je kyberterorista.

Existuje mnoho nástrojů, které mohou používat kyberteroristé k dosažení svého cíle například backdoors, scanery, sniffery, rootkity, debugerry, trojské koně atd.

4.1 HACKERSKÉ NÁSTROJE

Backdoors

Každý programátor si při tvoření programu nechává takzvaná zadní vrátka, která umožnují vzdálený přístup k zařízení. Tato zadní vrátka jsou oblíbená u hackerů, kteří tyto vstupy vyhledávají a objevují tak bezpečnostní díry. Každý hacker má většinou více počítačů, na kterých má nainstalovaný speciální software pro vzdálené připojení. Může tak napadnuté počítače užívat k dalším útokům. Hacker využívá počítače i pro svoji bezpečnost, proti odhalení, aby nebyl vystopován a případně dopaden. Kvalitní backdoors nelze snadno odhalit či zjistit, pokud není často užíván. Většinou umožnují úplnou kontrolu nad počítačem. Backdoors fungují na principu spuštěné služby, například webového přístupu portu 80. nebo terminálového přístupu portu 23. Tyto služby bývají většinou nechráněné a jsou odfiltrované firewally, což jsou bezpečnostní prvky pro počítačovou sít. Backdoors využívají právě těchto chyb protokolů, které se využívají ke komunikaci různých messengerů, jako je například ICQ, IRC, Facebook.

Scanery

Scanery se využívají pro skenování portů v počítači. Je to program, který běží na cílovém počítači. Odhalí tak pro útočníka základní informace o počítači a jeho systému. Zjistí, který z portů je špatně zabezpečen. Odhaluje chyby síťových protokolů a identifikaci služby běžící na daném portu.

Zjistíme-li, že je na počítači nainstalován takový program, můžeme si být jisti, že je to předzvěst potenciálního útoku. Jediná ochrana, která existuje je mít na počítači

nainstalovaný takzvaný podscan, který dokáže tento program odhalit a přerušit spojení s útočníkem nebo provést jiná bezpečnostní opatření.

Sniffery

Umožnují odposlouchávat síťový provoz. Nejde tedy přímo o nástroj pro útok, ale o prostředek, jehož úkolem je shromažďování informací, které jsou potřebné pro pozdější útok. Cílem snifferu je přepnutí síťového rozhraní tak, aby přijímal všechny pakety, které se na síti pohybují. Všechny pakety se zaznamenávají, analyzují, vyhodnocují, například o jaký protokol jde, IP adresy, MAC adresy a další. Lze tak odposlouchávat komunikaci v síti, zachytit přístupová hesla nebo jiná citlivá data.

Rootkity

Je to soubor skrytých činností probíhající v operačním systému. Jde o podobný program jako backdoors. Rootkit pochází z Unixového operačního systému. V unixovém prostředí by byl backdoor stoprocentně odhalen, ale roottkit zůstane v utajení na účtu superuživatele, tedy administrátora. Opět tento program využívají hackeři, aby získali neomezený přístup k počítači.

Unixové systémy využívají především operační systémy Linuxu, od kterého je Unixové jádro odvozeno. Příkladem můžeme uvést operační systémy REDHAT, SLACKWARE, UBUNTU.

Debuggery

Tyto programy jsou velice důležitou pomůckou pro hackery. Když hacker odhalí slabinu nebo bezpečnostní mezeru, provede analýzu kódování a ověří funkci exploitu, jenž má za úkol tuto bezpečnostní mezeru využít. Debuggery provedou ověření správné funkce kódu a najdou nejlepší místo pro napadení útočníkem. Využívají se zejména pro odhalování kódu pro kontrolu platných licencí softwaru. Útočník se snaží najít v programu podprogram, který kontroluje správnost licenčního čísla přidělené uživateli nebo ho následně po odhalení odstraní, čímž zbaví tento program, software jeho ochranných prvků.

Trojské koně

Trojské koně patří k nejoblíbenějšímu hackerskému nástroji. Převážně se jedná o malé programy, které jsou komprimované do samospustitelného programu, a které se tváří jako utilita pro vylepšení programového vybavení počítače nebo mohou být poskytovány jako bezplatné hry. Jejich možnosti jsou různé, mohou napadený počítač jen monitorovat „Data Mining“, nebo mohou monitorovat činnost uživatele až po útok DoS.

Viry

Počítačové viry mají jeden hlavní úkol, a ten je infikovat program nebo systém na cílovém počítači, který chtějí zločinci napadnout. Úkolem viru je napadnout a provést kopii, která se dál bude šířit prostřednictvím sítě či internetu.

Viry dělíme do několika skupin:

a) boot viry – napadají systémové oblasti disku
b) souborové viry – napadají pouze soubory uložené v PC
c) multipartitní viry – napadají systémové i souborové oblasti
d) makro viry – napadají datové soubory
e) stealth viry – ochraňují jiné viry před detekcí antivirovými programy
f) polymorfní viry – provádí změnu vlastního kódu pro znesnadnění detekce
g) rezidentní viry – ukládají se do paměti, kde zůstávají nadále přítomny

Nejčastěji se viry šíří pomocí přílohy v e-mailu, webových stránek, distribučním CD nebo USB.

Prolamování hesel

Prolamovač (Password Cracker) hesel patří k základnímu nástroji používaný hackery. Jak už název napovídá, jedná se o program, jehož funkcí je zjištění přístupového hesla, překonání ochrany, zjištění autorizace prováděné zadáváním hesla. Principem programu

je dosazování kombinací znaků. Pokud dojde ke zjištění hesla, program automaticky odešle přístupové heslo hackerovi, který může provést dva způsoby útoku.

1) Dictionary attak – slovníkový útok používá vlastní databázi slov
2) Brute-force attak – útok hrubou silou – generuje možné kombinace slov a znaků

Prolamovače hesel obsahují slovníky tzv. wordlisty, jejichž součástí jsou různé kombinace slov a znaků, z kterých se skládají hesla. To umožnuje rychlejší nalezení hesel. Ke zjištění hesla prolamovačem je zapotřebí rychlého procesoru, znalost typu hesla a zda jde o přístup k datům, souborům na síti, disku či internetu.

Spyware

Jde o program, který si většinou nahraje sám uživatel nevědomě do svého PC. Nejčastěji jako podružný program jiného programu. Úkolem spywaru je sbírání dat, informací o uživateli, ty pak zasílá k analýze. Mapuje a sbírá data o navštívených stránkách na internetu, o nainstalovaném softwaru. Tento spyware se dá považovat spíše za ten méně nebezpečný. Existuje ale i nebezpečná varianta spywaru, jehož cílem je získávat citlivá data, ovlivnit funkci počítače, stabilitu systému, umožnit vzdálený přístup.

4.2 SÍŤOVÉ ÚTOKY

Jde o útoky, kdy cílem útočníka je odposlech provozu na síti, za účelem zjištění informací a dat, ke kterým by neměl mít za normálních okolností nikdo přístup. Dokáží tak vyřadit počítače ze sítě či servery z provozu.

Sniffing

Sniffing je technika sledování sítě, při které dochází k ukládání (a opětovnému čtení) TCP paketů. Využívá se při „odposlouchávání“ datové komunikace. Některé síťové protokoly využívají jistou formu „čenichání“ k ověřování funkčnosti jednotlivých síťových prvků. Pátrají po špatně odhlášených uživatelích a tím uvolňují výkon sítě pro jiné operace.

Man In the Middle

Je to určitý druh sniffingu s cílem přerušit komunikaci síťového provozu a jejího opětovného připojení přes počítač útočníka. Tento způsob však vyžaduje fyzický přístup k síti.

Spoofing DNS

DNS má za úkol přeložit adresu webové stránky na IP adresu a opačně. Jde o lepší orientaci a zapamatování adres počítačů pro uživatele.

Obdrží-li systém sítě podvržený DNS, může se jednat o útok Man In the Middle, který směřuje podvrženou službu na server.

Jak probíhá takový útok?

1) Uživatel pošle požadavek na server DNS s žádostí o jeho přeložení na jméno domény, tedy IP adresu.
2) Útočník, který odposlouchává síťový provoz získá ID transakci a jiné informace.
3) Útočník zašle cíli špatnou odpověď, může dojít kromě zaslání i k zmanipulování DNS serveru.
4) Cíl získá nastrčený překlad domény IP a dochází ke komunikaci s falešným serverem, tedy útočníkem.
5) Útočník tak získal komunikaci s cílovým počítačem.

DHCP spoofing

DHCP Discover paket slouží ke zjištění, o jaký DHCP server se jedná. Paket je odeslán jako broadcast pro všechny počítače. DHCP server na tento paket odpovídá DHCP Offer paketem, kde jsou informace a další parametry k připojení. A jestliže jsou v síti zapojeny i další servery, vybírá si ten nejrychlejší. Server odpoví DHCP Request paketem, kde je uložena žádost o připojení a následně odpovídá DHCP ACK a provede připojení. Pokud chce útočník dosáhnout cíle a provést útok, musí být jeho server nejrychlejší, který odpoví na DHCP Discover paket. Tím se cíl napojí na útočníkův server, přes který lze směrovat provoz útočníka.

Dos Denial of service

Denial of service je tzv. odepření služby. Jde o útok, jímž se útočník snaží znemožnit přístup uživatelům k webovým stránkám nebo službám. Tento způsob se provádí po útoku k zahlazení stop. Lze ho dělit podle jeho realizace, a to buď hrubou silou útokem ICMP floods, Peer-to-peer, Distributed Denial of Service, Unintentional attack, nebo chybou v aplikaci Teardrop attack, Nuke, Land attack, Slowloirs.

ICMP floods

Jde o smurf útok, jedná se o všeobecné adresování. Útočník se snaží o zaslání většího množství ping paketů s broadcast adresou. Pakety se tak šíří do všech počítačů připojených k síti. Pokud by se jednalo o velkou sít s větším počtem připojených počítačů, došlo by tak k jejímu zahlcení.

Peer-to-peer

Peer-to-peer je server, kde uživatelé mezi sebou sdílejí data a informace. To probíhá prostřednictvím nějakého klienta. V tomto případě se využívá chyby právě u daného klienta k odpojení od tohoto serveru a připojení k jinému.

Distributed attack

Jde o verzi DoS útoku, cílem je zahlcení serveru s co největším množstvím počítačů v síti. Může jít o počítače, které jsou nakaženy škodlivým softwarem, nebo o počítače napadané trojským koněm. Útočník tak může předem naplánovat čas spuštění nebo může rozeslat spouštěcí signál k provedení útoku.

Unintentional attack

Zde dochází k neúmyslnému napadení webových serverů, které jsou málo navštěvované. Na webové stránky, které jsou často navštěvovány, se umístí odkaz pro připojení na tyto stránky, z kterých se stanou náhle hojně navštěvované, a tím dojde k zahlcení serveru.

Teardrop attack

Tento útok se provádí zasíláním IP fragmentu s množstvím velkých dat na cílový počítač uživatele, kde způsobí na starších verzích operačních systémů jeho pád.

Nuke

Cílový počítač je napaden tak, že přijímá větší množství ICMP paketů, které způsobují špatný CRC součet. Počítač, který se snaží tyto pakety zpracovat, se zahltí a přestane odpovídat. Dochází tak k jeho pádu.

Land attack

Provádí zasílání zprávy, tím dojde ke zmatení operačního systému cílového počítače, který má stejnou adresu. Stane se, že počítač začne odpovídat sám sobě, a tím dojde k jeho pádu.

Slowris

Útok způsobuje zasíláním požadavků ve velmi pomalém toku, a tím způsobuje udržování spojení mezi útočníkem a obětí na několik hodin.

Útoky na webové aplikace

Jsou jedním z nejčastějších a nejoblíbenějších útoků. Útoky poškozují nejen aplikace, ale především návštěvníky těchto webových stránek. Mohou získat přístupy na servery, a tím získat cenné informace pro útočníky.

Cross-Site Scripting

Je to metoda pro útok, který narušuje webové stránky. Je to jednou z nejpoužívanějších metod, nazýváme ji také jako XXS. Cílem je najít ve skriptech bezpečnostní chyby, které se nejčastěji nacházejí ve webových formulářích nebo v URL. Útočník do nich vloží svůj upravený HTML kód, čímž může získat citlivá data, aniž by někdo něco poznal. I když se o této hrozbě ví, stále je to nejčastější chyba současných webových stránek.

SQL Injection

Stejně jako u XXS se snaží útočník najít bezpečnostní chybu a vložit svůj upravený program do aplikace. Zde nejde jenom o aplikace, ale především o manipulaci s daty v databázi, které se mohou upravovat i mazat.

HTTP Response Spliting

Útočník se snaží do webové aplikace vložit kód neboli řetězec, jímž může manipulovat s odpovědí uživatele. Získává tak kontrolu a vstup od uživatele, může ovlivnit obsah zprávy nebo naopak získat více informací tím, že vloží do aplikace jiné otázky, na které má uživatel odpovědět.

4.3 SOCIOTECHNIKA

Jde o netechnický způsob útoku, využívá jeden z nejslabších článků v systému, člověka. Z bezpečnostního informačního hlediska jde v sociotechnice o ovlivnění člověka nebo jeho přesvědčení s cílem, aby uvěřil, že útočník zde figuruje jako někdo jiný. Ten pak může získat další informace nebo heslo od uživatele k provedení dalších úkonů. Vystupuje například jako správce sítě.

Phishing

Tak se označuje získávání informací s cílem tyto data zneužít (např. hesla, osobní certifikáty, rodná čísla, čísla kreditních karet…). Využívá se důvěřivosti oběti. Phishingové útoky se provádí SMS zprávami, telefonickými rozhovory a nejčastěji e-maily. Prvním případem pokusu o phishing v České republice byl březnu 2006 útok v Citybank. Existuje organizace Anti-Phishing Working Group (APWG)[21]. Tato organizace se zabývá řešením problémů, které jsou spojené s phishingovými útoky.

[21] *APWG.* [Online] 2016. [cit: 2016-1-8]. Dostupné z: http://www.antiphishing.org/

Pharming

Jedná se o podvodný útok. Je sofistikovanější než phishing. Útočník neútočí přímo na uživatele, protože nevytváří falešné webové stránky, ale ovládne skutečné webové stránky společnosti. Ochranu je potřeba zajistit na straně provozovatele webu.

5. NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI V ČR (NCKB)

NCKB se rozděluje do dvou sekcí. Tyto sekce řídí a spravují náměstci ministra vnitra.[22]

NCKB se rozdělujeme na vládní CERT a národní CERT. Vládní CERT řeší bezpečnost v počítačových sítích státní správy, kritické informační infrastruktury podle zákona o kybernetické bezpečnosti. Národní CERT je bezpečnostní tým, který řeší ostatní bezpečnostní incidenty v počítačových sítích v ČR.

Úkolem NCKB je dále zajišťovat vzdělávání v oblasti kybernetické bezpečnosti, účastnit se cvičení kybernetické bezpečnosti s národní a mezinárodní účastí, zastupovat ČR v mezinárodních orgánech zabývajících se kybernetickou problematikou.

Dne 1. ledna 2015 nabyl účinnosti zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a jeho prováděcí právní předpisy – vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Tento zákon má za cíl stanovit spolupráci mezi veřejným a soukromým sektorem a správou, jejímž účelem je zefektivnit řešení bezpečnostních a kybernetických útoků. Cílem zákona je zakotvit oprávnění a povinnosti z dané oblasti.

Dále bylo novelizováno nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury (tato novela je zveřejněna ve Sbírce zákonů pod číslem 315/2014 Sb.).[23]

[22] *Národní centrum kybernetické bezpečnosti.* [Online] 2011. [cit: 2015-12-22]. Dostupné z: http://www.govcert.cz.

[23] *Národní bezpečnostní úřad.* [Online] 2014. [cit: 2015-12-27]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/.

6. OCHRANA A BEZPEČNOST PROTI ÚTOKŮM

Ochrana a bezpečnost nejen pracovních, ale i osobních počítačů, je velké téma budoucnosti. Jedná se především o infrastrukturu, kterou lze chápat jako různá zařízení zapojená do sítí. Jedná se o počítače, servery, směrovače, přepínače nebo zabezpečení definovaná správci sítě, administrátory, supervizory, které slouží pro přístup do systému či sítě nebo ke zdrojovým stanicím.

Jak zvýšit naší ochranu a bezpečnost:

1) Pravidelně provádět zálohy dat, které nám umožnují návrat dat v případě napadení.
2) Single point of failure – jde o zabezpečovací způsob, kdy se v jednom zařízení nenachází všechny služby, například v jednom počítači pracuje firewall a na druhém mail server. V případě napadnutí musí útočník prolomit více systémů.
3) Pravidelné nahrávání bezpečnostních aktualizací.
4) Zadávat zásadně složitá hesla pro přístup.
5) Používat firewall –zabezpečuje přístup k jednotlivým službám v systému a pomocí něj můžeme ovlivňovat, kdo má a kdo nemá, přístup.
6) VPN – Virtual Private Network – jde o komunikaci a šifrování mezi systémy připojenými do internetové sítě.
7) Používání kvalitních antivirových programů.
8) Neinstalovat neověřené nebo nelegálně stažené programy.

Síťová bezpečnost patří mezi složitou problematiku. Nejhorší následky kyberterorismu mohou vzniknout po napadení počítačů a počítačových sítí v elektrárnách, na letištích, v dopravních podnicích, na finančních burzách, v bankách aj. Následky by výrazně ovlivnily chod celé společnosti nebo státu.

7. KYBERNETICKÝ ÚTOK, KYBERNETICKÁ VÁLKA

Podle Tallinského manuálu je kybernetický útok definován: „*Kybernetický útok je operace v kyberprostoru, ať už ofenzivní či defenzivní, v jejímž důsledku je důvodné očekávat způsobení zranění či smrt osobám, nebo poškození či zničení věci*“[24]

V současné době neexistuje společnost nebo stát bez závislosti na připojení v kyberprostoru, a proto pokud se hackerům podaří zorganizovat rozsáhlý útok, mohou být následky katastrofické. Za útoky mohou stát i jednotlivé státy (např. rusko – gruzinský konflikt v roce 2008).

Kyberprostor využívají armády i pro vedení konvenčních válek - bezpilotní letouny a drony jsou ovládány na dálku, bomby jsou naváděny GPS systémem, letadlové lodě jsou centry pro zpracovávání informací.

Typologie kyberútoků

Útoky lze podle cpt. Pascala Brangetta rozdělit[25]:

1. kategorie – narušení, cílem je objekt útoku poškodit
2. kategorie – útoky s cílem zničit objekt útoku, např. počítačový červ STUXNET (udává se, že byl vytvořen v Izraeli k sabotáži jaderné elektrárny Búšehr a závodu pro zpracování uranu v Iránu 2009)
3. kategorie – špionáž, nejčastější útoky, státy i velké společnosti vynakládají velké finanční prostředky na zjišťování informací od jiných státu nebo společností (případ Edwarda Snowdena, který zveřejnil rozsah odposlouchávání evropských politiků americkou tajnou službou NSA)

[24]SCHMITT, M. *Tallinnský manuál a mezinárodní právo pro kybernetickou válku.* Cambridge : Cambridge University Press, 2013. 106 s.ISBN 978-1-107-61377-5.

[25]*Právní prostor.* [Online] 2015. [cit: 2015-12-27]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/kratky-nahled-na-soucasnou-problematiku-kybernetickych-utoku.

Problematikou kyberútoků se zabývá například tallinské kybernetické centrum NATO CCDOE (Cooperative Cyber Defense Centre of Excellence. Cílem centra je interpretace mezinárodních smluv a úmluv v kontextu kybernetické bezpečnosti. V roce 2013 byl vydán tallinský manuál, Tallin on the International Law Applicable to Cyber Warfare, o mezinárodním právu aplikovatelném na válku v kyberprostoru. Je to dokument vypracován 20 nezávislými odborníky pro NATO v čele s prof. Michaelem N. Schmittem. Skládá se z 95 pravidel pro vedení kybernetického boje. Není závazný pro členy NATO. Každý stát pohlíží na problematiku kyberprostoru jinak (Rusko žádá nové mezinárodní dohody, USA uznává principy mezinárodního práva i v kyberprostoru). Tallinský manuál uznává stávající mezinárodní úmluvy a obecné zásady práva i v kyberprostoru.

Existuje tzv. šedá zóna kyberbezpečnosti. Patří sem tzv. honeypots – webové stránky, které lákají útočníky a poté se zjišťuje, o co se zajímají, a honeytoken – soubor se skrytou funkcí, která se aktivuje na počítači hackera, a tím ho pomůže lokalizovat. Užití honeypots a honeytoken je diskutabilní a vlastně i protiprávní, např. případ tzv. SONY Hack. Společnost SONY natočila film o atentátu na Kim-čong Una. Severní Korea označila tento film jako podporu terorismu a válečný čin. 24. 11. 2014 byl proveden hackerský útok na studio SONY, bylo odcizeno velké množství citlivých dat. 17. 12. 2014 FBI vydalo prohlášení, že propojilo hackery se Severní Koreou. Prezident Obama toto prohlášení podpořil a přislíbil, že USA bude na útok reagovat. Došlo tak k přímému obvinění jednoho státu druhého z kybernetického útoku. Pokud by USA skutečně reagovalo tzv. odezvovou kyberobranou (Responsive cyber defence), např. hack-backem, což znamená nabourání se do útočníkova systému s cílem získat ukradená data zpátky, jednalo by se též o kyberútok. Došlo by k narušení svrchovanosti cizího státu a porušení mezinárodního práva.

Kybernetická válka, tak se mohou označit útoky na informační a komunikační infrastrukturu, probíhají v kybernetickém prostoru prostřednictvím elektronických dat a elektronická data jsou též terčem operací. V tallinském manuálu jsou upřesněny principy „dotknutelnosti“ civilistů, kteří jsou součástí kybernetických útoků. Použít sílu proti kyberútoku lze, pokud došlo ke ztrátám na životech nebo k zásadnímu poškození fyzických objektů nebo infrastruktury.

II. PRAKTICKÁ ČÁST

V praktické části se budu zabývat konkrétními případy kybernetických útoků a kyberterorismu. Jako cíle kyberterorismu bývají uváděny tzv. objekty kritické infrastruktury. Kritickou infrastrukturou jsou označovány výrobní a nevýrobní systémy a služby. Vyřazení těchto objektů by mělo vážný dopad na zabezpečení životních potřeb obyvatelstva, ekonomiku, bezpečnost státu a veřejnou správu.

Ve dvou kazuistikách popíši napadení kritických infrastruktur ve státech Estonsko a Litva, ve třetí kazuistice pak kybernetický útok na jadernou elektrárnu v Íránu a v poslední kazuistice analyzuji útok na webový portál zabývající se bezpečností.

8. KYBERNETICKÝ ÚTOK NA ESTONSKO 2007

8.1 KONTEXT

Estonsko je evropský stát, který sousedí s Lotyšskem a Ruskou federací. Samostatným státem se stalo roku 1991, kdy byla jeho nezávislost uznaná i Ruskem (dříve bylo jednou ze sovětských republik). 2004 vstoupilo Estonsko do NATO a EU. V zemi se nachází početná ruská menšina, odhad tvrdí ¼ populace. Většina etnických Rusů žije v Tallinnu. Mezi Estonskem a Ruskem stále panuje řada sporů, zejména ideologických.

Informační infrastruktura je na vysoké úrovni. 2007 byly informační systémy a databáze propojené do jednotného systému s vlastní specifikou. 2005 se stalo Estonsko prvním státem, kde byli voleni veřejní zástupci přes internet.

V lednu 2007 rozhodla estonská vláda o přesunu bronzové sochy představující pomník neznámého sovětského vojáka jako osvoboditele Tallinnu z centra Tallinnu na vojenský hřbitov. Proti přesunu se ohradila Ruská Federace i etničtí Rusové. 26. 4. 2007, den před přesunem, propukla v centru Tallinnu násilná demonstrace.[26] V Moskvě byli velvyslanci Estonska napadeni členy skupiny Naši. Proti přesunu se vyjádřil i prezident Putin a pohrozil přerušením diplomatických styků s Estonskem.

[26] K první vlně protestů uvádí zdroje na 1500 protestujících (Spiegel Online 2007).

8.2 ÚTOKY

Kybernetické útoky začaly souběžně s demonstracemi. První útoky začaly 27. 4. 2007, směřovaly proti webovým stránkám vlády, prezidenta, parlamentu, premiéra, zpravodajským portálům a on-line mediím. Další útoky vedly do sektoru bankovnictví, 2 největší banky musely pozastavit své služby. To vedlo k omezení chodu společnosti a ekonomické aktivity Estonců vzhledem k tomu, že jsou peněžní služby poskytovány téměř výlučně elektronicky. Zpravodajské subjekty nemohly řádně informovat o vzniklé situaci ani Estonce ani zbytek světa.

Jednalo se o více druhů útoků – formu DoS útoků (zahlcení napadených serverů) i DDos útoků (zaměření na omezení funkce serverů). Pro útoky byly použity tzv. botnety (napadené počítače jsou ovládány někým jiným než vlastníkem či uživatelem a mohou být využity pro další kybernetické útoky bez vědomí vlastníka).

8.3 AKTÉŘI

Nejviditelnější skupinou při útocích bylo hnutí Naši.[27] Z útoků byl obviněn pouze student (etnický Rus) informačních technologií z Tallinnu. Existuje ale důvodné podezření, že za útoky nestáli jednotlivci, ale silná a bohatá skupina nebo stát, která mohla tyto útoky financovat a koordinovat. Do boje proti útokům se zapojil vládní i soukromý bezpečnostní sektor a pomoc přišla i z NATO. Estonsko z útoků oficiálně obvinilo Rusko. Důkazem měly být IP adresy některých ruských státních institucí. Rusko toto důrazně odmítlo. Estonsko poté od obvinění ustoupilo, ale poukazovalo na neochotu Ruska při spolupráci útoky zastavit a vyšetřit.

8.4 DOPADY

Odsouzen byl jeden člověk. Socha byla přesunuta z centra na periferii na vojenský hřbitov. Estonsko se začalo orientovat na problematiku kyberprostoru.

V Tallinnu sídlí CCDOE (Cooperative Cyber Defense Centre of Excellence), centrum kybernetické obrany NATO. Je vycvičen speciální kybernetický tým – RRT (Rapid

[27]Hnutí Naši je politické hnutí pro mladé Rusy. Samo je označováno jako demokratické, antifašistické, nicméně je velmi silně napojeno na vládní struktury. V době útoků na Estonsko bylo jednotným hnutím s více než 100 tisíci členy. V současné době se rozpadlo na několik odnoží.

Reaction Team) tzv. „Muži v černém“. Tým disponuje nejmodernější komunikační a počítačovou technikou pro zjišťování, analýzu kyberútoků a zabezpečení sítí.

V listopadu 2015 proběhlo v Estonsku již třetí cvičení NATO zaměřené na obranu před kybernetickými útoky. „Cyber Coalition“ se zúčastnilo na 600 vojenských a civilních expertů zemí Aliance. Cílem bylo ověřit koordinaci a schopnosti jednotlivých zemí při obraně proti kyberútokům v síti NATO. Ve virtuálním prostředí specialisté bojovali i s jinými hrozbami, jako jsou např. mobilní telefony s upraveným softwarem pro sledování a špionáž.[28]

[28] *iDNES*. [Online] 2015. [cit: 2015-12-28]. Dostupné z: http://zpravy.idnes.cz/nato-proveruje-svou-kyberobranu-d4o-/zpr_nato.aspx?c=A151120_130834_zpr_nato_inc.

9. W32.STUXNET V BÚŠEHRU

9.1 KONTEXT

Búšehr je město ve stejnojmenné provincii v Íránu. Nedaleko stojí první íránská jaderná elektrárna. S její stavbou začala německá společnost Kraftwerk Union AG v roce 1975, v roce 1979 po islámské revoluci stavbu ukončila. Od roku 1995 je do stavby a provozu zapojeno Rusko.

V dubnu 2008 se sešly světové velmoce v Šanghaji, cílem jednání byl íránský jaderný program. Západ se obával, že obohacený uran bude sloužit k výrobě jaderné zbraně. Rusko nabídlo, že by se obohacený uran, který by sloužil jako palivo pro elektrárnu, připravoval a po použití zpracovával v Rusku. A tak by mohla MAAE[29] (mezinárodní agentura pro atomovou energii) kontrolovat íránský jaderný program.

V dubnu 2010 Americká administrativa žádala světové velmoce o podporu pro uvalení sankcí na Írán. Rusko se distancovalo vzhledem k jeho spolupráci při stavbě jaderné elektrárny v Búšehru. Šéf ruské agentury pro atomovou energii Sergej Kirijenko prohlásil, že ruský projekt Íránu žádným způsobem k získání jaderné zbraně nepomůže. Termín spuštění elektrárny byl stanoven na září 2010 po skončení ramadánu.

9.2 ÚTOK

V dubnu 2010 se začal šířit počítačový vir s názvem W32.Stuxnet[30]. Hlavní postižené země byly – Írán (58 % počítačů), Indonésie (18%), Indie (8%).

Úkolem viru je zničit něco fyzického, nenapadá počítač s cílem získat informace nebo data. Má vlastnost rootkit, tzn. že, přepíše standartní systémové ovladače tak, aby byl pro ně nezjistitelný, využívá k tomu ukradené certifikáty. V napadeném počítači hledá vir pouze určitý software, a to software firmy Siemens, který v reálném čase řídí a kontroluje určitý proces. Pokud není v počítači tento software nalezen, vir se skryje a napadá další počítače. Tento vir se dostane i do počítačů odpojených od internetu, protože se nešíří

[29] *Eretz*. [Online] 2011. [cit:: 2015-12-29]. Dostupné z: http://eretz.cz/2011/11/maae-iran-usiluje-jaderne-zbrane/.

[30] *Pbweb*. [Online] 2001. [cit: 2015-12-29]. Dostupné z: http://pbweb.cz/Pocitacovy%20utok/Kryptograficke/stuxnet.html.

přes internet. Přenáší se přes USB a disky. V jaderné elektrárně v Búšehru Stuxnet fyzicky poškodil řadu odstředivek nezbytných pro obohacování Uranu.

9.3 AKTÉŘI

Podle prohlášení počítačových odborníků ze Západu je vir natolik účinný a vyspělý, že nemohl být vytvořen pouze jednotlivci. Útočník musel mít přístup k unikátním a tajným informacím o provozu jaderné elektrárny a musel disponovat perfektními hardwarovými a softwarovými znalostmi. Bylo potřeba několik špičkových týmů s perfektní koordinací a velkou finanční podporou. Irák tuto sabotáž nebo špionáž považoval za skrytou kybernetickou válku vedenou Izraelí nebo USA.
V listopadu 2010 Sergej Kirijenko zahájil provoz první íránské jaderné elektrárny.

9.4 DOPADY

V roce 2013 se objevila zpráva, že je vyšetřován generál James Cartwright[31]. Čelil obvinění, že umožnil zveřejnění informací o vytvoření viru Stuxnet. Informace udávaly spolupráci Izraele a USA – Izraelci zajistili informace o centrifugách v íránském zařízení a propašovali vir do počítačů, vir vytvořili programátoři v USA pomocí zdrojových kódů zapůjčených společností Microsoft.

MAAE od počátku vyjadřuje pochybnosti o civilním charakteru iránského jaderného programu. Obává se, že tamní resort slouží jako zástěrka pro vývoj jaderné zbraně. Žádá přístup svých inspektorů ke kontrole jaderných zařízení v Íránu.

V letech 2013 – 2015 proběhla jednání mezi Íránem a světovými velmocemi – USA, Velkou Británií, Francií, Německem, Ruskem a Čínou o íránském jaderném programu. 14. 7. 2015 byla uzavřena dohoda o omezení jaderného programu[32] výměnou za zrušení sankcí. Írán přislíbil inspektorům agentury MAAE větší přístup ke kontrole svých jaderných zařízení. Tuto dohodu ostře kritizuje Izrael, zakládá svůj Národní kybernetický úřad (National Cyber Authority).[33]

[31] *Press Report.* [Online] 2013. [cit: 2015-12-29]. Dostupné z: http://www.press-report.cz/clanek-3158877-informace-o-viru-stuxnet-prozradil-ctyrhvezdickovy-general-celi-vysetrovani.

[32] *Novinky.cz.* [Online] 2015. [cit: 2015-12-26]. Dostupné z: http://www.novinky.cz/zahranicni/amerika/383774-usa-a-eu-ucinily-kroky-ke-zruseni-sankci-proti-iranu.html.

[33] *Echo24.cz.* [Online] 2016. [cit: 2016-1-8]. Dostupné z: http://echo24.cz/a/wQUSF/zapad-privital-dohodu-s-iranem-usa-ale-oznamily-nove-sankce.

10. KYBERNETICKÝ ÚTOK V LITVĚ 2008

10.1 KONTEXT

Litva je další země, která byla více či méně pod kontrolou Ruska. V roce 1990 se Litva pokusila získat nezávislost. Reakcí Ruska bylo zavedení sankcí a ozbrojený útok na televizní věž ve Vilniusu. Žije zde 6% etnických Rusů.

Litva nemá vyspělé informační a komunikační technologie, a proto je z hlediska kybernetické bezpečnosti na nízké úrovni. Je zde nedostatečná spolupráce mezi veřejným a soukromým sektorem, bezpečnost v oblasti dat a informací je také nevyhovující.

V roce 2008 byl v Litvě přijat pozměňovací návrh k zákonu o sdružování, na tomto základě bylo zakázáno používat sovětské a nacistické insignie[34] na veřejnosti. Ruská Federace okamžitě reagovala vydáním stanovisek, které tento zákon kritizovaly. Rusko dále odmítalo záměr Litvy nabídnout umístění americké protiraketové obrany na svém území.

10.2 ÚTOKY

28. 6. 2008 se objevily kybernetické útoky jako reakce na zákon o sdružování. Útoky napadaly litevské weby, svým charakterem připomínaly ty v Estonsku roku 2007. Byly napadeny portály ze soukromého i vládního sektoru. Na portály byly umístěny sovětské symboly a ruskojazyčné proti-litevské slogany. Dalším útokem bylo rozesílání e-mailového spamu, který obsahoval manifest: „Hackeři spojeni proti externím hrozbám Ruska“.

10.3 AKTÉŘI

Původci nejsou dosud známí. Litevská vláda uvedla, že útoky byly vedeny ze zahraničí. Podle některých zdrojů jsou za pachatele označeny nacionalistické ruské hackerské skupiny. Ty vydaly bezprostředně před útokem prohlášení: "*Všichni hackeři této země se rozhodli se spojit, aby čelili nestydatým činům západních velmocí. Máme dost zasahování NATO na naši mateřskou půdu, máme dost ukrajinských politiků, kteří zapomněli*

[34]Zejména srp a kladivo, rudou hvězdu, svastiku, stejně jako hymny obou režimů.

na svůj národ a myslí pouze na své zájmy. A máme také dost estonských vládních institucí, které bezostyšně přepisují historii a podporují fašismus.“[35]

10.4 DOPADY

Vzhledem k nízké informační a komunikační infrastruktuře v Litvě byly dopady kybernetických útoků relativně nízké. Velkou úlohu sehrála i předem zveřejněná varování ruské hackerské komunity.

Kybernetické útoky na Litvu se dále opakovaly v roce 2009- proběhl izolovaný útok na litevskou daňovou správu, v roce 2013 – v době, kdy Litva předsedala EU, v roce 2014 – kdy Litvu navštívil Barack Obama. Všechny tyto útoky jsou vnímány jako výhružka ruského patriotického hackingu nebo Ruské Federace.

11. ANALÝZA ÚTOKU NA PORTÁL SECURITY - PORTAL

11.1 POPIS ÚTOKU

V další kazuistice popíši a analyzuji útok na portál webu security-portal.cz[36], který se zabývá bezpečností v kybernetickém prostoru.

K útoku došlo ve dnech 29. a 30. června 2013, výsledkem útoku bylo nahrání útočných skriptů, které měly sloužit k dalšímu napadení a infiltraci. Webový portál stránek je vytvořen redakčním systémem WordPress, který obsahuje několik zabezpečovacích prvků proti napadení, řada z nich funguje autonomně. V případě napadení provedou tyto bezpečnostní prvky automatickou blokaci a přidají útočníka s jeho IP adresou na tzv. blacklist. Útočníci se nedostali na server přes stránky www.security-portal.cz, nýbrž přes subdoménu stránek. Stránky běžely na sdíleném hostingu, proto nebyly dostatečně zabezpečené před napadením. Před útokem předcházelo takzvané oťukávání, které bylo vedeno z většího počtu IP adres s cílem testovat běžné soubory, například o jakou verzi redakčního systému jde, a jaké jsou na

[35]BOROVIČKA, V**.** překlad *Kybernetické konflikty v postspvětském prostoru.* Brno, 2015.

[36]*Security-Portal.* [Online] 2013. [cit:: 2015-12-30]. Dostupné z: http://www.security-portal.cz/clanky/anal%C3%BDza-c%C3%ADlen%C3%A9ho-%C3%BAtoku-%C4%8D%C3%A1st-prvn%C3%AD.

nich nainstalované moduly (pomocné aplikace webu). Útok byl veden pomocí běžných nebo upravených skriptů, které měly za úkol sběr informací. Byl veden čistě manuálně a zapříčinil nefunkčnost hlavní webové stránky a jejího fóra, který posílal chybu o zpracování skriptu. Prvním krokem k identifikaci útočníků bylo stáhnutí logu webového serveru, který obsahuje seznam IP adres navštívených počítačů.

Příklad:

awk '{ print $2 }' access_log | sort | uniq -c | sort -n

Předpokládalo se, že útočník bude mezi 10 IP adresami navštívených PC. Ukázalo se, že útočníci použili při útoku více jak 30 IP adres, některé z nich byly vedeny ze sítě Microsoft Network. Pomocí IP adresy lze přesně vystopovat útočníka, kam přistupoval a jaký dostal HTTP respons.

Důležité je:

- O jaký responce kód jde, a jestli byl útočníkovi přidělen při vstupu v administrační části.
- POST, informace, které útočník posílal na daný server.
- Jestli útočník přistupoval k souboru, který je neznámý a může vykazovat, že jde o nově nahraný script.
- Zda útočníků není více a nepokouší se o průnik z více adres.
- Snaha najít podpis útočníka.

Pokud se najde důkaz o napadení, musí se jít zpět na začátek a hledat, kdy poprvé útočník provedl něco podezřelého. Musí se stáhnout a projít logy IP adres a odstranit z nich soubory, které nemají nic společného s útokem, například obrázky, css, javascript. Log tak bude přehlednější.

Příklad:

grep -f soubor_s_IP_adresama.txt access_log | grep -vE "gif HTTP|png HTTP|js HTTP|css HTTP|jpg HTTP|ico HTTP|js?n HTTP|css?n HTTP" > filter.lo

Jako příklad uvádím rozbor ukázkového záznamu Apache logu:

convertor.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:28 +0200] "GET / HTTP/1.1" 200 1137 "http://www.bing.com/search?q=convertor+security" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"

1) convertor.security-portal.cz – host, na kterého byl dotaz směřován
2) 109.186.96.51 - IP adresa klienta/útočníka
3) [29/Jun/2013:22:41:28 +0200] - datum a čas požadavku
4) "GET /index.html HTTP/1.1" - požadavek na stažení/zobrazení (GET) souboru index.html umístěného v kořenovém adresáři hosta convertor...
5) 200 - HTTP kód 200 znamená vše v pořádku
6) 1137 - počet zaslaných bajtů klientovi
7) "http://www.bing.com/search?q=convertor+security" - referer, stránka, ze které na web přistupoval
8) "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1)..." - webový prohlížeč klienta, OS, případně i moduly

Útočníka lze dohledat podle podpisu, podle webového prohlížeče odkud přistupoval. Je nutné setřídit IP adresy se stejným podpisem a přidat ho do seznamu podezřelých. Použitý prohlížeč je dobrým identifikačním vodítkem. Musíme projít řádek po řádku a hledat v logu něco neobvyklého. Je důležité zapisovat IP adresy i jiné neobvyklé údaje či časy. Odstraníme opakující se záznamy a snažíme se o co nejpřesnější filtr tak, aby nedošlo ke smazání důležitých informací a záznamů.

Důležitá je i komunikace s hostingem, na kterém je nahraný web. Kvalitní a přístupný hosting může poskytnout mnoho informací o útoku. Především může zjistit, zda byl útok veden na více webů, a zajistit bezpečnostní opatření a předejít tak k možnému dalšímu útoku. Pokud známe čas a IP adresu, můžeme kontaktovat administrátora hostingu a zjistit, kdy byla provedena poslední záloha před napadením. Tyto zálohy pak slouží k obnovení webových stránek. Nelze je jen přehrát, neboť by na disku zůstaly takzvané backdoory. Musí jít o kompletní smazání disku a nahrání kompletní zálohy pro správnou funkčnost webu. Je nutné požádat administrátora hostingu o vypsání všech souborů, které byly modifikované ode dne útoku až po současný čas, kdy byly provedeny jejich zálohy.

Příkladem uvádím výpis testovací verze modulů WordPressu na subdoméně:
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:20 +0200] "GET /wp-content/plugins/twitter-facebook-google-plusone-share/tfg_style.css?ver=3.5.2

HTTP/1.1" 200 183 "http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:20 +0200] "GET /wp-content/plugins/wp-syntax/css/wp-syntax.css?ver=1.0 HTTP/1.1" 200 815 "http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:20 +0200] "GET /wp-content/plugins/wp-stats/stats-css.css?ver=2.50 HTTP/1.1" 200 436 "http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:42 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.8.3 HTTP/1.1" 200 33444 "http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:42 +0200] "GET /wp-content/plugins/mlanguage/mlanguage.js?ver=3.5.2 HTTP/1.1" 200 1077 "http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:09 +0200] "GET /wp-admin/css/wp-admin.min.css?ver=3.5.2 HTTP/1.1" 200 23842 "http://bflow.security-portal.cz/wp-login.php?redirect_to=http%3A%2F%2Fbflow.security-portal.cz%2Fwp-admin%2F&reauth=1" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"

Testovací výpis existence souborů:

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:02 +0200] "GET /UserFiles HTTP/1.1" 404 59060 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:03 +0200] "GET /userFiles HTTP/1.1" 404 59060 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:04 +0200] "GET /UserFile HTTP/1.1" 404 58933 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:05 +0200] "GET /userfile HTTP/1.1" 404 58933 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:06 +0200] "GET /CV HTTP/1.1" 404 59105 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:08 +0200] "GET /cv HTTP/1.1" 404 59105 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:10 +0200] "GET /upload HTTP/1.1" 404 63017 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:12 +0200] "GET /uploads HTTP/1.1" 404 58853 "-" "-

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:13 +0200] "GET /jobs HTTP/1.1" 404 60036 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:15 +0200] "GET /jobs/cv HTTP/1.1" 404 58916 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:16 +0200] "GET /jobs/cv/up.php HTTP/1.1" 404 59165 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:18 +0200] "GET /jobs/cv/upload HTTP/1.1" 404 58956 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:24 +0200] "GET //jops/cv/attachments HTTP/1.1" 404 59099 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:25 +0200] "GET /www.zip HTTP/1.1" 404 60955 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:27 +0200] "GET /public_html.zip HTTP/1.1" 404 59264 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:29 +0200] "GET /www(1).zip HTTP/1.1" 404 60175 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:31 +0200] "GET /www_1.zip HTTP/1.1" 404 60288 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:33 +0200] "GET /public_html(1).zip HTTP/1.1" 404 58996 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:34 +0200] "GET /www.zip HTTP/1.1" 404 60955 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:34 +0200] "GET /public_html.zip HTTP/1.1" 404 59264 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:35 +0200] "GET /www(1).zip HTTP/1.1" 404 60175 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:35 +0200] "GET /public_html(1).zip HTTP/1.1" 404 58996 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:36 +0200] "GET /up.zip HTTP/1.1" 404 58862 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:38 +0200] "GET /upload.zip HTTP/1.1" 302 - "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:58 +0200] "GET /forum.zip HTTP/1.1" 404 59137 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:00 +0200] "GET /forum(1).zip HTTP/1.1" 404 58866 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:02 +0200] "GET /forum_1.zip HTTP/1.1" 404 59045 "-" "-"

security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:03 +0200] "GET /iran.zip HTTP/1.1" 404 59043 "-" "-"

Testovací výpis chyb:

 # Full path disclosure = www.securitate.md/blog/drupal-7-x-search-module-full-path-disclosure/201...

security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:26:09 +0200] "GET /search?keys[0]=securitate.md HTTP/1.1" 200 13470 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

 # phpinfo

bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:22:42 +0200] "GET //wp-content/plugins/wp-syntax/test/index.php?test_filter[wp_head][99][0]=pi&test_filter[wp_head][99][1]=cos&test_filter[wp_head][99][2]=phpinfo HTTP/1.1" 301 20 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"

bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:24:14 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.8.3 HTTP/1.1" 200 33444 "http://bflow.security-portal.cz/wp-content/plugins/wp-syntax/test/?test_filterwp_head990=session_start&test_filterwp_head991=session_id&

test_filterwp_head992=system" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"¨

Výpis sběru subdomény pomocí vyhledávače bing.com:

ebook.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:28 +0200] "GET / HTTP/1.1" 200 1137 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
webirc.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:41 +0200] "GET / HTTP/1.1" 200 1181 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
paste.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:44 +0200] "GET / HTTP/1.1" 200 4601 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
convertor.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:49 +0200] "GET / HTTP/1.1" 200 1184 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
cm3l1k1.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:52 +0200] "GET / HTTP/1.1" 200 1672 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
network-tools.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:58 +0200] "GET / HTTP/1.1" 200 1424 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form=QBRE&p

q=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:44:58 +0200] "GET / HTTP/1.1" 200 746
"http://www.bing.com/search?q=ip%3a195.210.29.4+security&qs=n&pq=ip%3a195.210.29.4+security&sc=8-23&sp=-1&sk=&first=11&FORM=PERE" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
owasp.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:06:39 +0200] "GET / HTTP/1.1" 200 3528
"http://www.bing.com/search?q=ip%3a195.210.29.4+security&qs=n&pq=ip%3a195.210.29.4+security&sc=8-23&sp=-1&sk=&first=21&FORM=PERE1" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
tor.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:06:42 +0200] "GET / HTTP/1.1" 200 2420
"http://www.bing.com/search?q=ip%3a195.210.29.4+security&qs=n&pq=ip%3a195.210.29.4+security&sc=8-23&sp=-1&sk=&first=21&FORM=PERE1" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
convertor.security-portal.cz 41.102.154.48 - - [29/Jun/2013:23:18:45 +0200] "GET / HTTP/1.1" 200 1184 "http://www.bing.com/search?q=ip%3A195.210.29.4+security-portal.cz&go=&qs=n&form=QBRE&filt=all&pq=ip%3A195.210.29.4+security-portal.cz&sc=0-0&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"

Výpis a identifikace útočníka:

flack.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:22:12 +0200] "GET / HTTP/1.1" 200 746
"http://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fflack.security-portal.cz%2F&ei=_k_PUaeDLOTj4QS334HoCw&usg=AFQjCNEQPOZgkzKtfHNY26ITv4TZ7gsfkQ&sig2=cgpCXtAYpH2_whdOW5IgRQ&bvm=bv.48572450,d.bGE" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
paste.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:22:24 +0200] "GET /

HTTP/1.1" 200 4601
"http://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&cad=rja&ved=0CDAQFjABOAo&url=http%3A%2F%2Fpaste.security-portal.cz%2F&ei=C1DPUdLVDIGO4ASBmoC4Cg&usg=AFQjCNF8J3jyNzFOsC0aUBXCUOF9paltwQ&sig2=lHvHkgrDXl9cW7akmTGvYQ&bvm=bv.48572450,d.bGE"
"Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
cm3l1k1.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:22:31 +0200] "GET / HTTP/1.1" 200 1672
"http://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&cad=rja&ved=0CHgQFjAJOAo&url=http%3A%2F%2Fcm3l1k1.security-portal.cz%2F&ei=C1DPUdLVDIGO4ASBmoC4Cg&usg=AFQjCNGKg2fXK0v4rhjao3TBQoXgy-etyw&sig2=6Xe6GlIsV-_upZpm2eauaA&bvm=bv.48572450,d.bGE"
"Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Tak bylo zjištěno, že útočníci pochází z Alžírska. Útok byl proveden tzv. velkým počtem přístupů na administraci a přihlášením stránky z jedné ze subdomén. Jednalo se o téměř 3500 přístupů s frekvencí 10 sekund. To se na konec povedlo. Přístupové heslo k administraci mělo 16 znaků. Jakmile se útočník přihlásil, nahrál své moduly a skripty, přepsal kód některých základních prvků WordPressu, a tím si zajistil zadní vstup tzv. zadní vrátka v případě smazání ostatních skriptů.

Výpis nahrání modulů útočníkem:

 # Module upload
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:47 +0200] "POST /wp-admin/update.php?action=upload-plugin HTTP/1.1" 200 4658 "http://bflow.security-portal.cz/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
 # Plugin editor
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:35:12 +0200] "GET /wp-admin/plugin-editor.php HTTP/1.1" 200 14477 "http://bflow.security-portal.cz/wp-admin/post.php?post=419&action=edit" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

 # Akismet edit
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:35:52 +0200] "GET /wp-admin/plugin-editor.php?file=akismet/akismet.php&a=te&scrollto=0 HTTP/1.1" 200 14981 "http://bflow.security-portal.cz/wp-admin/plugin-editor.php" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Výpis útočného scriptu typu GET:

 # Module upload
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:47 +0200] "POST /wp-admin/update.php?action=upload-plugin HTTP/1.1" 200 4658 "http://bflow.security-portal.cz/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
 # Plugin editor
*bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:35:12 +0200] "GET /wp-admin/plugin-editor.ph**p** HTTP/1.1" 200 14477 "http://bflow.security-portal.cz/wp-admin/post.php?post=419&action=edit" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"*
 # Akismet edit
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:35:52 +0200] "GET /wp-admin/plugin-editor.php?file=akismet/akismet.php&a=te&scrollto=0 HTTP/1.1" 200 14981 "http://bflow.security-portal.cz/wp-admin/plugin-editor.php" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Zdrojové skripty:

Poté, co přijde výpis seznamu modifikací zaslaného od administrátora hostingu, musíme tento seznam důkladně prohlédnout, abychom byli schopni rozlišit, co je změněné a co není. Jde o to, abychom dokázali analyzovat, jakým způsobem se útočníci dostali do systému. Lze použít PHP dekodér, který dokáže odhalit nesmyslné znaky a upozornit na ně.

Výpis skriptu htccess:

bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:44 +0200] "GET /wp-admin/perl.php HTTP/1.1" 200 689 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Tento skript vytvořil htccess soubor, který ostatním souborům *.dam přiřadil CGI handler umožnující spouštění CGI skriptů a zapsání se do souboru perl.dam. Tímto útočníci obešli nastavení open_basedir umožnující PHP skriptům vyskočit na subdoménách jako root adresář SP. CGI skripty neběží pod stejnými právy jako PHP skripty. Mají obecně vyšší oprávnění. Došlo však k tomu, že nebyly CGI skripty na doméně webových stránek vypnuty, což byla zásadní chyba umožňující napadení stránek.

Výpis CGI skriptů:

Options FollowSymLinks MultiViews Indexes ExecCGI
AddType application/x-httpd-cgi .dam
AddHandler cgi-script .dam
AddHandler cgi-script .dam
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:44 +0200] "GET /wp-admin/perl/perl.dam HTTP/1.1" 200 1022 "http://bflow.security-portal.cz/wp-admin/perl.php" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:48 +0200] "POST /wp-admin/perl/perl.dam HTTP/1.1" 200 615 "http://bflow.security-portal.cz/wp-admin/perl/perl.dam" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Výpis skriptu dir.php do rootu SP útočníkem:

bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:59:38 +0200] "GET /wp-admin/perl/perl.dam?a=upload&d=%2fdata%2fs%2fe%2fsecurity%2dportal%2ecz%2fweb%2fimg HTTP/1.1" 200 691 "http://bflow.security-portal.cz/wp-admin/perl/perl.dam" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:59:47 +0200] "POST /wp-admin/perl/perl.dam HTTP/1.1" 200 662 "http://bflow.security-portal.cz/wp-admin/perl/perl.dam?a=upload&d=%2fdata%2fs%2fe%2fsecurity%2dportal%2ecz%2fweb%2fimg" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
security-portal.cz 41.100.181.234 - - [30/Jun/2013:00:00:10 +0200] "GET //img/dir.php HTTP/1.1" 200 1306 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Výpis bashe a base64 pomocí logů ukazující, kde se útočníci všude pohybovali:

grep 'dir\.php' access_log | cut -d'=' -f2,3,4 | cut -d'&' -f1 | cut -d' ' -f1 | grep -v security-portal > dir-path
for i in $(cat dir-path); do echo $(echo $i | base64 --decode) >> paths.log; done
cat paths.log | sort | uniq
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow/.htaccess
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow/forum
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow/forum/config.php
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/logs
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/logs/error_log-2013-06-29
/data/s/e
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/cm3l1k1
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/forum
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/forum/config.php

/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/kernelhunter
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/kernelhunter/wp-config.php
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/owasp
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/tor
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/web

Jak jsem již psal, útoku na SP předcházelo 3500 přístupů na stránku přihlášení z jedné subdomény, poté došlo k infiltraci i dalších míst portálu. Subdoména běží na redakčním systému WordPressu, který využívá po celém světě na 60 milionů uživatelů. V dnešní době je velice populární, a proto je i častým cílem útočníků. Útočníci používají tzv. automatizované útoky, kterými získávají informace o zabezpečení a hledají možné nedostatky využitelné k provedení útoku. Hlavní příčinou napadení jsou přídavné moduly třetích stran, které uživateli umožnují vylepšení redakčního systému. Tyto moduly mají často nedostatečnou ochranu a nelze všechny kontrolovat, zda je jejich napsaný kód dobře naprogramovaný. Jestliže si uživatel nahraje modul s pravděpodobnou zranitelností, je jen otázkou, kdy se stane terčem útočníků. Jakmile útočník převezme kontrolu nad Vaší doménou, může ji zneužít k provedení dalších útoků nebo nahrání dat z databáze a může fungovat i jako přechodné uložení dat útočníka. Po konzultaci s administrátorem bylo zjištěno, že bylo na webu pět modulů, kde se vyskytovaly exploity. Podle logu na serveru došlo sice k několika dotazům na moduly, ale nic nenasvědčovalo tomu, že by se o ně útočníci zajímali. Proto možná teorie, jak došlo k napadení, je slovníkový útok nebo útok hrubou silou. Je zde otázka, jak bylo prolomeno jediné bezpečnostní heslo o 16 znacích. Taková dlouhá hesla slovníky neobsahují.

Další možnou teorií, jak k průniku došlo, je napadení senssion cookie za pomocí cracknutí seedů pomocí náhodného vygenerovaného klíče cookie. Session cookie je časově omezený kód, který je přiřazen uživateli serverem, a chce po každém dotazu tento kód zadat. Server dále může přiřadit uživateli různá oprávnění a na základě toho může přístup umožnit nebo odepřít. Jestliže útočník zjistí session cookie, je schopen

manipulovat s účtem uživatele i bez přístupového hesla. Soubor senssion cookie je uložen nejčastěji na serveru v dočasném adresáři. Byla tady možnost, že soubor senssion cookie má nějakou slabinu a proto lze tento soubor predikovat. Tato teorie byla také zavržena, jelikož by bylo značně náročné zjistit přesný čas přihlášení uživatele do systémů a získat tak senssion cookie. Navíc pokud by došlo k expiraci senssion cookie, útok by se nikdy nezdařil. Navíc pokud by došlo k expiraci senssion cookie, útok by se nikdy nezdařil.

Závěrečnou teorií útoku je, že útočník cracknul přístupové heslo pomocí vlastního web hostingu. Většina hostingů ukládá senssion cookies do jednoho souboru v podadresáři /tmp. Cesta je nadefinována v PHP proměné session_save_path. Senssion cookie funguje jako One Time Password zkráceně OTP, zde patrně byla ta chyba, kterou útočníci využili k proniknutí. Jakmile jej útočník dokáže zjistit, může se přihlásit jako uživatel s příslušným oprávněním. Po prozkoumání všech access logů bylo zjištěno, že útočníci věnovali pozornost i dalším serverům za pomocí referu, který se jim podařilo prolomit pomocí dump databáze subdomény. Získali tak plný přístup sice k jinému webu, ale na stejném serveru jako web security-portal.cz. Útočníci si vypsali všechny senssion cookies a zkoušeli se tak přihlásit ke každé z nich do administrace subdomény, což se povedlo na 3500-tý pokus.

11.2 AKTÉŘI ÚTOKU NA SP

Za útokem na webové stránky security-portal.cz bylo vyhlášení hackerské soutěže jednoho arabského fóra. Bylo vytvořeno pět týmů, které se měly pokusit hacknout stránky na předem vybraných serverech, a umístit zde kontrolní soubor v txt s číslem daného týmu. Bylo zjištěno, že útočníci si nechali otevřená zadní vrátka pro pozdější vstup do systému. Celý incident se vyřešil velice rychle, ať už byl záměr útoku jakýkoli.

11.3 OBRANA PROTI PODOBNÉMU ÚTOKU

Útoku se lze bránit, pokud identifikujeme a odstraníme slabá místa v systému. Musíme si uvědomit, jakou cenu mají data a informace uložené na discích a tomu přizpůsobit jeho ochranu. Pokud máme server v naší firmě a ne na sdíleném hostingu, je zapotřebí provádět aktualizace firmwaru či operačních systémů a síťových prvků na aktuální verzi. Cílem je zamezit útoku typu DoS a DDoS.

ZÁVĚR

Kybernetický prostor může být chápán jako pojem filozofický, sociologický, kulturní, vojenský.

Podle § 2 písm. a) zákonu č. 127/2005 Sb. „*se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací“*.[37]

T. Gřivna kyberprostor definuje *„Kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a další existence je však závislá na světě reálném. Vznik kyberprostoru byl esenciálně spjat s určitou úrovní technologické vyspělosti společnosti, s rozvojem informačních a telekomunikačních technologií. Připojením na komunikační a informační služby vytvářejí jednotliví uživatelé určitý druh společného prostoru, který lze nazvat „kyberprostorem“.*[38]

Jednotlivec může chápat kyberprostor jako virtuální realitu. *„Virtuální realita ve svém nejsilnějším významu popisuje zvláštní druh interaktivní simulace, ve kterém má průzkumník tělesný pocit, že je ponořen do situace definované databází“*. [39]

Z vojenského hlediska lze považovat kybernetický prostor vedle země, vzduchu, vody a vesmíru za pátou oblast vojenských aktivit. Možná by bylo možné zahrnout „kybernetické zbraně“ mezi ZHN (zbraně hromadného ničení) – existují počítačové viry, virové útoky, odvirování počítače či antivirové programy. Přesná a úplná terminologie pro kybernetickou problematiku není ještě vytvořena.

Kybernetická válka je podle některých expertů vyústění kybernetického terorismu. Jedna z definic zní: „ *Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem, je tzv. kyberprostor….a prováděné*

[37]Zákon č. 127/2005 Sb.; o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů

[38]GŘIVNA, T. *Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva.* Praha : Karolinum, 2008. 21-34 s. ISSN 0323-0619.

[39]LÉVY, P. *Kyberkultura.* Praha : Karolinum, 2000. 25 s. ISSN 80-246-0109-5.

.

prostřednictvím počítačové sítě.“[40] Kybernetické nástroje mohou výrazně změnit geopolitické rozložení sil.

Podle dostupných informací by se mohlo zdát, že některé země již v kybernetické studené válce jsou. Jedním z příkladů studené kybernetické války je údajné sestřelení amerického bezpilotního letounu nad územím Íránu v roce 2011.[41] Američané toto nejprve popřeli, později připustili, že o jeden letoun přišli. Usuzuje se, že díky počítačovému viru byla změněna jeho dráha letu a přistál na území Iránu, aniž by byl poškozen. Toto by mohly zrealizovat pouze zkušené týmy počítačových expertů. V podezření je spolupráce Íránu s Čínou nebo Ruskem. Už jen tato podezření mohou výrazně ovlivnit mezinárodní vztahy. Dalším příkladem může být již popsaný supervir Stuxnet. Velmi propracovaný a koordinovaný útok v Búšehru ukázal sílu spojení světových mocností při dosažení určitého cíle.

Kybernetické nástroje se používají nejen ve vojenské oblasti, řada útoků probíhá i proti jiným systémům kritické infrastruktury. Objekty kritické infrastruktury stále nemají dostatečné kybernetické zabezpečení. Jako příklady byly analyzovány útoky na Estonsko a Litvu. Zde útoky ovlivnily chod celého státu. V Litvě k tomu stačil útok hackerské organizace jiného státu, která prosazovala svoje nacionalistické smyšlení.

Kybernetické hrozby se nevyhýbají ani České republice. Zatím se naše republika nestala cílem kyberterorismu, stoupá ale četnost kybernetických útoků, které ochromily funkci nebo činnost některých organizací či institucí. Jako příklad mohu uvést ukradení emisních povolenek za 450 miliónů Kč z českého elektronického registru v roce 2011. Za útočníky byl označen gang rumunských hackerů.

Velkým problémem u kybernetického útoku je vypátrat pachatele útoku a identifikovat skutečný cíl, nelze totiž vyloučit ani možnost, že útok, který byl odhalen, sloužil jen jako krycí manévr, který měl odvést pozornost od skutečného cíle a pachatele.

[40]Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu. Praha: Ministerstvo vnitra České republiky, odbor bezpečnostní politiky, 2004.

[41]*Rozhlas.cz*. [Online] 2011. [cit: 2015-12-30]. Dostupné z: http://www.rozhlas.cz/zpravy/blizkyvychod/_zprava/iran-tvrdi-ze-sestrelil-americke-bezpilotni-letadlo--985595.

Řada zemí na obranu proti kybernetickým útokům zřídila své zvláštní kybernetické jednotky a kybernetické agentury. Kybernetická hrozba má vážné geostrategické důsledky, proto i spojenecké organizace jako NATO, EU či OSN mají svá kybernetická centra. Česká republika má svoje Národní centrum kybernetické společnosti (NCKB) v Brně.

Rychlý rozvoj informačních a komunikačních technologií vyžaduje jejich spolehlivost a bezpečnost. Jen tak se zajistí správné fungování organizací ve státním a veřejném sektoru. Každá nová technologie sebou přináší riziko zranitelnosti a zneužití. Dříve ojedinělé útoky se stávají častějšími a sofistikovanějšími. Mění se i cíl útoků. Dříve to byl jedinec či organizace, nyní se cílem stávají objekty kritické infrastruktury, jejichž narušením může dojít k destabilizaci společnosti. Kybernetická bezpečnost je založena na spolupráci mezi veřejným a státním sektorem, mezi civilními a ozbrojenými složkami a velmi důležitá je mezinárodní spolupráce. Bezpečnost tudíž začíná u občana, u každého, kdo pracuje s PC a je připojen do počítačové sítě. Možná by se měla stanovit pravidla bezpečnosti pro používání kyberprostoru pro jednotlivce, pro organizace, pro veřejné a státní instituce, pro poskytovatele počítačových služeb. Jejich počítač nebo počítačová síť by se stala odolnější a bezpečnější proti vnějšímu i vnitřnímu útoku. Možná se v brzké budoucnosti zavede výuka kybernetické bezpečnosti i do škol.

Jeden americký kybernetický expert řekl: „Je to jiný svět, bomby už nepotřebujeme…“

SEZNAM POUŽITÝCH ZDROJŮ

SEZNAM POUŽITÝCH ZDROJŮ

BOROVIČKA, V. *Kybernetické konflikty v postspvětském prostoru.* Brno, 2015.

DUNNINGAN, J. *Bojiště zítřka.* Praha : Baronet, 2004. ISBN 80-7214-642-4.

GAVORA, P. *Úvod do pedagogického výzkumu.* Bratislava : Univerzita Komenského Bratislava, 2008. ISBN 978-80-223-2391-8.

GIBSON, W., překlad NEFF, O. *Neuromancer.* Praha : Laser, 2010. ISBN: 80-85601-27-3.

GŘIVNA, T. *Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva.* Praha : Karolinum, 2008. ISSN 0323-0619.

HARIS, S., HARPER, A. a EAGLE, CH. *Hacking - Manuál hackera.* Praha : Grada Publishing a.s., 2008. ISBN 978-80-247-1346-5.

HINDLS, R., HOLMAN, R., HRONOVÁ, S a kolektiv. *Ekonomický slovník.* Praha : A plus, 2003. ISBN: 978-80-903804-5-5.

CHENÍČEK, J. *Terorismus a my.* Praha : Computer Press, 2001. ISBN 80-7226-584-9.

JANOUŠEK, S. *Kyberterorismus: terorismus informační společnosti.* Praha : ComputerPress, 2006. ISSN 1214-6463.

KUNEŠOVÁ-SKÁLOVÁ, J., SKÁLA, M. *Vymezení pojmu nehmotný majetek.* Praha : Tributum, 1998.

LÉVY, P. *Kyberkultura.* Praha : Karolinum, 2000. 80-246-0109-5.

LONG, J. *Google - Hacking.* Praha : ZonerPress, 2005. ISBN 80-86815-315.

MATES, P., MATOUŠOVÁ, M. *Evidence, Informace, systémy – právní úprava.* Praha : Codex Bohemia, 1997.

MICROSOFT. *Microsoft Press slovník výpočetní technik.* Praha : Plus, 1993 . ISBN 80-85297-48-5.

Sbírka zákonů ČR. Ostrava : Sagit, a.s., č. 127/2005. ISBN 978-80-7208-736-5.

SCHMITT, M. *Tallinnský manuál a mezinárodní právo pro kybernetickou válku.* Cambridge : Cambridge University Press, 2013. ISBN 978-1-107-61377-5.

SMEJKAL, V. *Kybernetická kriminalita.* Plzeň : Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

Standarty státního informačního systému ČR. Praha : ÚSIS, 1996.

SEZNAM INTERNETOVÝCH ZDROJŮ

iDNES. [Online] 2015. [cit: 2015-12-28]. Dostupné z: http://zpravy.idnes.cz/nato-proveruje-svou-kyberobranu-d4o-/zpr_nato.aspx?c=A151120_130834_zpr_nato_inc.

Novinky.cz. [Online] 2015. [cit: 2015-12-26]. Dostupné z: http://www.novinky.cz/zahranicni/amerika/383774-usa-a-eu-ucinily-kroky-ke-zruseni-sankci-proti-iranu.html.

Právní prostor. [Online] 2015. [cit: 2015-12-27]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/kratky-nahled-na-soucasnou-problematiku-kybernetickych-utoku.

Halonoviny. [Online] 2014. [cit:: 2015-12-22]. Dostupné z: http://www.halonoviny.cz/articles/view/16724657.

Revue pro média. [Online] 2001. [cit: 2015-12-22]. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm.

ÚVTMU zpravodaj. [Online] 2011. [cit:: 2015-12-23.] Dostupné z: http://ics.muni.cz/bulletin/articles/395.html.

Vlastik Chytrák. [Online] 2001. [cit: 2015-12-22]. Dostupné z: http://www.vlastik.chytrak.cz/definice_pocitace.htm.

APWG. [Online] 2016. [cit: 2016-1-8]. Dostupné z: http://www.antiphishing.org/.

Národní centrum kybernetické bezpečnosti. [Online] 2011. [cit: 2015-12-22]. Dostupné z: http://www.govcert.cz.

Národní bezpečnostní úřad. [Online] 2014. [cit: 2015-12-27]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/.

Eretz. [Online] 2011. [cit:: 2015-12-29]. Dostupné z: http://eretz.cz/2011/11/maae-iran-usiluje-jaderne-zbrane/.

Pbweb. [Online] 2001. [cit: 2015-12-29]. Dostupné z: http://pbweb.cz/Pocitacovy%20utok/Kryptograficke/stuxnet.html.

Press Report. [Online] 2013. [cit: 2015-12-29]. Dostupné z: http://www.press-report.cz/clanek-3158877-informace-o-viru-stuxnet-prozradil-ctyrhvezdickovy-general-celi-vysetrovani.

Echo24.cz. [Online] 2016. [cit: 2016-1-8]. Dostupné z: http://echo24.cz/a/wQUSF/zapad-privital-dohodu-s-iranem-usa-ale-oznamily-nove-sankce.

Security-Portal. [Online] 2013. [cit:: 2015-12-30]. Dostupné z: http://www.security-portal.cz/clanky/anal%C3%BDza-c%C3%ADlen%C3%A9ho-%C3%BAtoku-%C4%8D%C3%A1st-prvn%C3%AD.

Rozhlas.cz. [Online] 2011. [cit: 2015-12-30]. Dostupné z: http://www.rozhlas.cz/zpravy/blizkyvychod/_zprava/iran-tvrdi-ze-sestrelil-americke-bezpilotni-letadlo--985595.

SEZNAM ZKRATEK

ZNV – Zbraně hromadného ničení

CERT – Národní centrum kybernetické společnosti

EW – Elektronický boj

IO – Informační operace

CSUT – Rakety dlouhého doletu

PC – Osobní počítač

LAN – Lokální síť

PAN – Osobní síť

WAN – Vzdálená síť

IP – Internetový protokol

ČR – Česká republika

RRT – Tým rychlého nasazení

MAAE – Mezinárodní agentura pro atomovou energii

NCA – Národní kybernetický úřad

DoS – Odmítnutí služby

DDoS – Odmítnutí služby

RMA – Koncept informační války

EMP/T a HERT – Bomby pro ničení veškeré elektroniky

TC – Útok s převzetím kontroly nad PC

EW/IO - Informační operace

HDD – Pevný disk PC

GSM, EDGE, UMTS, CDMA, LTE – Mobilní široko pásmové sítě

GPS- Zaměřovací systém pozice

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Lubomír Černý

Obor: Bezpečnostní studia

Forma studia: Kombinované studium

Název práce: Kyberterorismus a kybernetická kriminalita

Rok: 2016

Počet stran textu bez příloh:58

Celkový počet stran příloh:0

Počet titulů českých použitých zdrojů: 15

Počet titulů zahraničních použitých zdrojů: 0

Počet internetových zdrojů: 16

Vedoucí práce: PhDr. Aleš Zoubek, Ph.D.