Základní definice,
vztahující se k tématu kybernetické bezpečnosti

PRAHA 2009

Počítačová kriminalita (cyber-crime, kyberzločin): Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.[1] Často se pojem počítačová kriminalita používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu.[2]

Informační kriminalita (info-crime): Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.[3]

Kriminalita, související s pokročilými technologiemi (high-tech crime): Trestná činnost, zaměřená na vyspělou techniku jako cíl, prostředí nebo nástroj pachatele trestného činu (zpravidla se jedná zároveň aktivitu, označitelnou za „počítačovou“ či „informační“ kriminalitu).

Ve své podstatě přitom může jít ve všech výše zmíněných variantách o velmi různorodou směsici činů, kdy konkrétní technologie může být jak předmětem zájmu, objektem (prostředím) nebo nástrojem pro jejich uskutečnění. To v konečném důsledku může vést k přístupu, kdy je zmíněná množina aktivit chápána:

- značně široce („jakákoli trestná či jinak závadová činnost s prvky výpočetní techniky“), včetně případů, kdy je např. počítačoví sestava použita při padělání peněz nebo cenných listin;
- značně úzce tedy výhradně jako činy, spáchané proti informačním technologiím, které nemohou být spáchány žádným jiným způsobem ani proti jinému cíli.

Informační bezpečnost: Multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Je tak možné chápat odvětví, zabývající se snižováním rizik, vztahujících se k fenoménu informací a navrhující opatření, vztahující se k příslušným organizačním, řídícím, metodickým, technickým, právním a dalším otázkám, které s touto problematikou souvisí.[4] Někdy je možné se setkávat se s podstatně omezenějším chápáním daného pojmu, jako úzké disciplíny, týkající se výhradně bezpečnosti informačních a komunikačních technologií.

Počítač (computer, personal computer, PC): V souladu se zněním ČSN 36 9001 se jedná o „stroj na zpracování dat provádějící samočinné posloupnosti různých aritmetických a logických operací“, tedy, jinými slovy, stroj, charakterizovaný prací s daty, která probíhá podle předem vytvořeného programu, uloženého v jeho paměti.[5]

Internet: Celosvětová počítačová síť spojující počítače a počítačové sítě všech kontinentů. Internet nabízí různé služby, mezi nejznámější patří WWW (prohlížení webových stránek), elektronická pošta (e-mail) či FTP (protokol pro přenos souborů). Souhrn všech sítí a počítačů je vzájemně spojen přenosovým protokolem TCP/IP (Transmission Control Protocol – Internet Protocol). Každá síť a každý počítač, který je součástí Internetu, disponuje jedinečným doménovým jménem. Přidělování a správa doménových jmen jsou hierarchické: správce domény nejvyššího řádu (např. .cz) rozhoduje o přidělování domén druhé úrovně (např. mvcr.cz), správce domény druhého řádu rozhoduje o přidělování domén třetí úrovně, aniž by toto

[1] Definice počítačové kriminality, akceptovaná v rámci Evropské unie zní: Počítačová kriminalita je nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich znění.

[2] Pokud není uvedeno jinak, byly pojmy definovány na základě následujících podkladů:
Jirovský, V., Kybernetická kriminalita, Grada Publishing, Praha 2007 (ISBN 978-80-247-1561-2), str. 269-274.
Hník, V.; Krulík, O., Staňová, E., Základní definice, vztahující se k tématu kybernetických hrozeb (http://www.mvcr.cz/bezpecnost/informacni/zakladni_info.pdf).
Hník, V.; Krulík, O., Staňová, E., Základní definice, vztahující se k tématu kybernetických hrozeb; in: Security Magazine, 2 / 2007, str. 46-49.
Esser, M., Počítačová kriminalita (absolventská práce), TRIVIS - Střední škola veřejnoprávní a Vyšší odborná škola prevence kriminality a krizového řízení s. s r. o., Praha 2007.

[3] Požár, J., Trendy počítačové kriminality a kyberterorismu.

[4] Požár, J., Informační bezpečnost v organizaci; in: Bezpečnostní teorie a praxe, 1 / 2005, str. 107-112.

[5] Porada, V.; Konrád, Z., Metodika vyšetřování počítačové kriminality, Praha 1998.

přidělování konzultoval se správcem domény nejvyššího řádu atd. Komunikace mezi počítači probíhá na základě IP, ve kterém se počítače označují číselnými adresami (IP adresy). Před zahájením komunikace je vždy nutno zjistit, jaká IP adresa odpovídá zadanému doménovému jménu. Tomu slouží síť specializovaných počítačů, které na žádost, obsahující doménové jméno, zašlou odpověď s příslušnou číselnou adresu (nebo naopak). Systém těchto počítačů se označuje jako DNS (Domain Name System).

Kritická informační infrastruktura státu: Komplex informačních a komunikačních systémů a jejich služeb, sloužící k informačnímu zajištění řádné funkčnosti kritické infrastruktury. Sestává z částí, jakými jsou telekomunikace, počítačové systémy a jejich programové vybavení, Internet, přenosové sítě, poskytované služby atd.

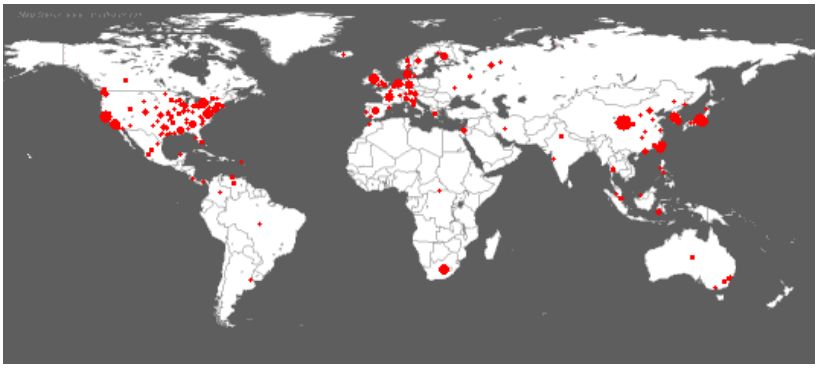
Informační systém: Funkční celek, nebo jeho část, zabezpečující systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.[6]

Malware (škodlivý software): Souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře zprávu v rámci elektronické pošty). Může se jednat například o:

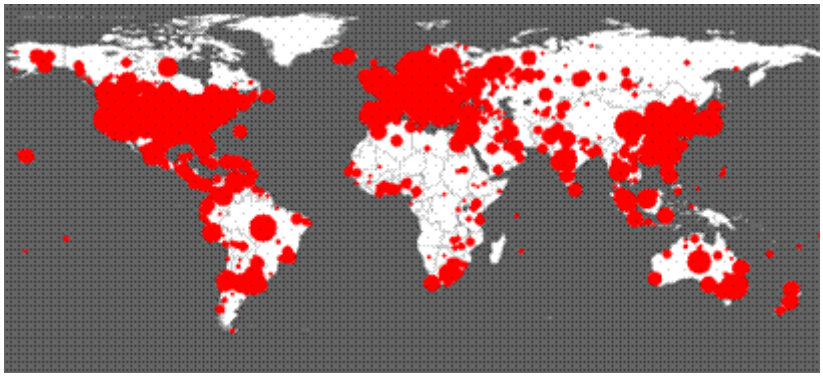
- ***Infoware*** může být specifikován jako aplikace pro informatickou podporu klasických bojových akcí, respektive jako soubor aktivit, které slouží k ochraně, vytěžení, poškození, potlačení nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem. Pojem *infoware* nelze zaměňovat s termínem *infowar*, tj. informační válka.[7]
- ***Spyware (špionážní software)*** jsou programy, skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.
- ***Adware (advertising supported software)*** je software, jehož cílem je předání reklamního sdělení (i proti vůli uživatele systému).

Vir (virus): Podmnožina *malware*. Parazitující soubor, který se připojí k určitým programům nebo systémovým oblastem, které pozmění. Může se nekontrolovatelně rozšiřovat, nebo po svém spuštění zahájit destrukční proceduru (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.). Existují viry, které mohou zároveň plnit funkci trojského koně a (nebo) vytvářet tzv. „zadní vrátka“ do napadeného systému. Počátek šíření počítačového viru může být distribuován v prostoru ohnisek, vytvořených na již kompromitovaných (zavirovaných) počítačích, což nesmírně urychluje celý proces šíření infekce.

Průběh virové nákazy v rámci kyberprostoru vykazuje řadu podobností. Již často neplatí, že biologický virus se postupně šíří region po regionu (viz např. SARS). Vir biologický a počítačový se liší pouze rychlostí migrace, odvozené od použitých komunikačních prostředků a technických možností (počítačové viry jsou rozšířené po celém světě prakticky hned).



[6] Smejkal, V., Legislativa na rozcestí; in: CHIP, 7 / 1999.
[7] Porada, V.; Konrád, Z., Metodika vyšetřování počítačové kriminality, Praha 1998.



Přes určitou podobnost se virová nákaza v rámci kyberprostoru od biologického viru liší: její doba šíření je zpravidla blesková (ilustrace popisuje šíření viru Code Red během 19 hodin od jeho prvotního zjištění); šíření nákazy se neděje směrem od jednoho epicentra, ale skokově: nejprve jsou zasaženy lokality, vyznačující se velkým počtem připojení k Internetu; technicky zaostávající lokality se nákaze de facto vyhnou.

Červ (worm): Podmnožina *malware*. Autonomní program, schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.

Trojské koně, keyloggery: Podmnožina *malware*. Programy, implantované do systému bez vědomí oprávněného uživatele, monitorující specifické činnosti, o které projevuje útočník zájem. Zaznamenávají např. znaky které oprávněný uživatel stiskl na klávesnici (zejm. hesla) nebo stránky, které navštívil. Tyto údaje předávají útočníku k dalšímu zpracování. Ten tak může získat přístupové informace k webovým stránkám, bankovním účtům nebo kontům elektronické pošty. Může se jednat i o textový editor, který zároveň ukládá text, který byl jeho prostřednictvím napsán, do skryté části systému, odkud může být vyzdvižen autorem trojského koně. Trojské koně často instaluje nevědomky sám oprávněný uživatel, když instaluje z Internetu nebo zdarma distribuovaných CD jiné programy, se kterými jsou však tyto trojské koně spojeny (např. hry či servisní programy - utility).

Přesměrovávače (re-dial, „pharming crimeware“): Podmnožina *malware*. Programy, jejichž úkolem je přesměrovat uživatele na určité stránky namísto těch, které původně hodlal navštívit. Na takových stránkách dochází k instalaci dalšího crimeware (virů), nebo touto cestou dojde ke značnému zvýšení poplatků za připojení k Internetu (prostřednictvím telefonních linek se zvýšeným tarifem).

Logické bomby (logical bombs): Podmnožina *malware*. Programy, které se tajně vkládají do aplikací nebo operačního systému, kde za předem určených podmínek provádějí destruktivní aktivity. Předem specifikovanou podmínkou startující logickou bombu může být například konkrétní datum (výročí určité události – viz např. „Virus 17. listopad“).

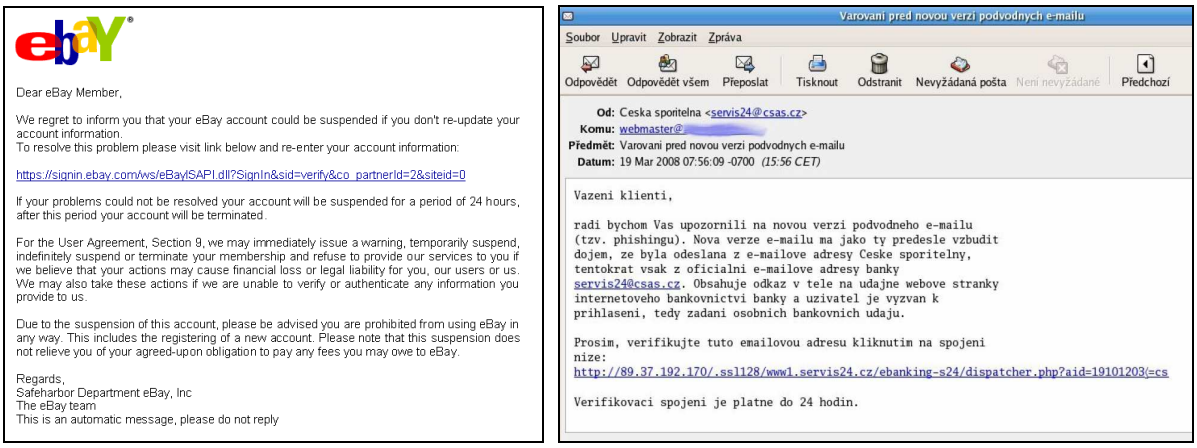
Replay: Situace, kdy je zachycená kopie legitimní transakce (datová sekvence), opětovně přehrána neautorizovaným subjektem, a to zpravidla s nelegálním úmyslem (např. pro otevření vozidla s centrálním zamykáním).

Hacking / cracking: Neoprávněný průnik do konkrétního informačního systému, provedený zvnějšku, zpravidla ze vzdáleného počítače. Samotný průnik je podmínkou pro další neautorizovanou činnost v rámci cílového systému. Pachatelé se zpravidla nepřipojují k objektu útoku (počítači) přímo, ale přes jeden i více internetových serverů v různých částech světa. Cílem takového postupu je podstatné snížení možnosti identifikace skutečného umístění počítače, který byl při útoku užit. Po spáchání činu na cílovém počítači je často možno zjistit pouze internetovou adresu předchozího počítače, k němuž byl pachatel připojen (a do kterého učinil popsaný zásah). Jednotlivé případy takových incidentů se liší zejména co se týče jejich motivace (vzrušení, zábava, msta, zvědavost, hmotný zisk). Samotný pojem „***hacking***“ bývá (zpravidla, ale nikoli výlučně) spojován z jinou než zištnou (či nezvratně ničivou) motivací; pojem „***cracking***“ bývá naopak užíván právě v případech, jejichž cílem je počitatelný zisk (respektive jejichž výsledkem je

nevratná škoda).

Defacement: Průnik do webových serverů protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník. Defacement není skryt, naopak: usiluje o medializaci. Jeho psychologická síla spočívá jednak ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy napadené strany, jednak v prezentaci ideologie či postojů útočníka.

Phishing („rhybaření", „házení udic"). Podstatou metody, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.), je vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky - tzv. **spoofing**).[8] Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN. **Prvním případem pokusu o uplatnění phishingu v prostředí bankovní sféry České republiky se v březnu 2006 stala Citybank**. V březnu 2008 kulminovala masivní kampaň, obsahující prvky phishingu, zaměřená na klienty České spořitelny a. s.



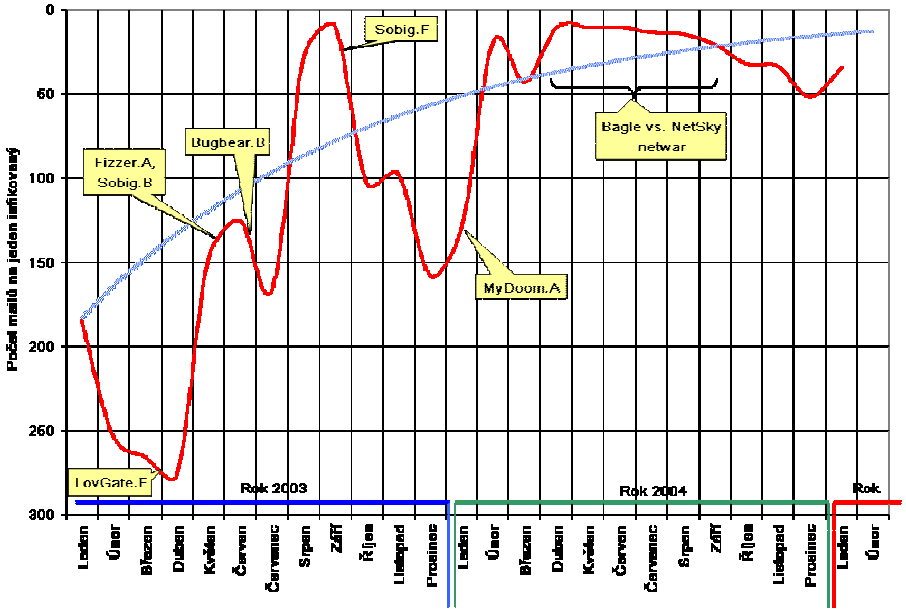
Příklad phishingu / skimmingu, souvisejícího s internetovým obchodem e-Bay (prosinec 2005) a s Českou spořitelnou a. s. (březen 2008).

Cyberstalking (stalk = plížit se): Nejrůznější druhy stopování a obtěžování s využitím elektronického média (zejm. prostřednictvím elektronické pošty), jejichž cílem je např. vzbudit v oběti pocit strachu. Informace o oběti pachatel získává nejčastěji z webových stránek, fór nebo chatovacích místností („**chat**" je způsob přímé (on-line) komunikace více osob prostřednictvím Internetu). Často je taková aktivita pouze mezistupněm k trestnému činu, který může zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání atd.

Nevyžádaná pošta (spam): Nevyžádané, v prostředí elektronické pošty masově šířené sdělení. V nejčastějším případě se jedná o reklamu nejrůznějšího charakteru, včetně nabídek afrodisiak, léčiv nebo pornografie. Není-li systém dostatečně zabezpečen, může nevyžádaná pošta tvořit značnou část elektronické korespondence (odhaduje se, že spam tvoří polovinu komunikace v rámci elektronické pošty dnešním světě). Spam nejenom obtěžuje, ale může představovat výraznou hrozbu pro konkrétního příjemce. Představuje nemalou zátěž pro server elektronické pošty (čímž může zapříčinit jeho zahlcení nebo alespoň omezení jeho výkonnosti). Dalším faktorem, který s existencí spamu souvisí, je ztráta času uživatele a často i ztrátu jeho financí. Jen v zemích EU se odhadují ztráty, způsobené ztrátou produktivity práce v souvislosti s existencí spamu, na 2.5 miliard eur ročně. Jako každá elektronická zpráva, i spam v sobě může nést, a často také nese, další hrozby (crimeware, spyware atd.). Častým jevem je například nevyžádaná instalace poštovního klientu, který spam (a mnohdy nejenom jej) rozešle na všechny adresy

[8] Na nebezpečí phishingu aktuálně upozorňují např. i oficiální materiály České spořitelny (bulletin z dubna 2006).

elektronické pošty, které nalezne v počítači nebo i v celém konkrétním informačním systému. Konkrétní uživatel či organizace se tak stávají nedobrovolnými rozesílateli spamu, který, vzhledem k tomu, že přichází z pohledu dalších adresátů z důvěryhodných zdrojů, nemusí být odfiltrován jejich antispamovými prostředky.



Statistika podílu infikovaných e-mailů z celkové e-mailové korespondence (leden 2003 - únor 2005).

Hoax: Specifická forma spamu, falešná či žertovná poplašná zpráva (mystifikace), vyzývající adresáta, aby něco učinil, nejčastěji, aby ji předal dál (nejlépe na několik adres), čímž se její šíření stává řetězovým.

WiFi (Wireles Fidelity): Bezdrátová technologie pro šíření dat („vzduchem“), vhodná pro tvorbu síťových infrastruktur tam, kde je výstavba klasické kabelové sítě nemožná, obtížná nebo nerentabilní (kulturní památky, sportoviště, veletrhy). Pro přenos dat postačí vhodně umístěné navazující přístupové body, lemující cestu od vysílače k příjemci.