BusinessIT.cz
ebook

# Kybernetická kriminalita: Od hackerů ke kybernetickým válkám

Stanislav Kužel pro BusinessIT.cz

Kybernetická kriminalita: Od hackerů ke kybernetickým válkám. Edice BusinessIT ebooks 2012

# Kybernetická kriminalita: Od hackerů ke kybernetickým válkám

**Stanislav Kužel pro BusinessIT.cz**

---

Edice: BusinessIT ebooks
Autor: Stanislav Kužel

Vydáno v roce 2012 v Bispiral, s.r.o.

web: www.BusinessIT.cz

---

Podceňujeme nebezpečí digitálního světa, nebo je spíše přeceňujeme? Jak se změnil svět kybernetické kriminality - od časů hackerů pracujících pro zábavu k dnešním kybernetickým zločincům? Jsou termíny jako kybernetický terorismus nebo kybernetická válka označením pro nějaké existující hrozby, nebo jde jen o výplod fantazie autorů sci-fi? Na takové i

řadu podobných otázek hledá odpověď kniha známého publicisty Stanislava Kužela, kterou máte před sebou.
Kniha vyšla i jako seriál na stránkách BusinessIT.cz.

Redakce BusinessIT.cz

---



---

## Co se děje v kyberprostoru

S lehkou nadsázkou lze říci, že kyberprostor je pátou dimenzí našeho bytí – realitou, se kterou a ve které se musíme naučit žít. Je dnes prostorem pro podnikání, vzdělávání – vyhledávání či získávání informací, a pro většinu populace i pro zábavu. Skýtá tak neuvěřitelné možnosti, že je ještě ani nedokážeme domyslet, ale současně je otevřený i

hackerům, crackerům či aktivistickým skupinám jako jsou Anonymous a, bohužel, i teroristům. Také proto dává dobrý smysl zamyslet se nad jeho bezpečností. A právě to bude činit seriál, který tímto příspěvkem otevíráme.

Kyberprostor (cyberspace) lze považovat mimo jiné za prostor pro kybernetickou kriminalitu či kyberterorismus a v neposlední řadě jako novodobé bojiště, kde se přinejmenším velmoci usilovně připravují k vedení válek skutečných, byť možná bez jediného výstřelu. I když je samozřejmě třeba dívat se na údaje o škodách s určitým odstupem, statistiky znějí impozantně: Více než 50 tisíc lidí se podle údajů společnosti Symantec každou hodinu stane obětí kyberzločinu, účet kyberkriminality za loňský rok se rovná 7,5 bilionům Kč (388 miliard USD). Přitom 41 % lidí na celém světě si podle stejného zdroje svoje data nechrání.

Problémem je, že bohužel zřejmě zdaleka ne každý má alespoň tušení, co se v kyberprostoru děje, když zapíná svůj počítač nebo Ipad. Pokud chceme něco z kyberprostoru získat, musíme mu něco poskytnout, a tak každý, kdo do kyberprostoru vstoupí, balancuje na pomezí soukromí a bezpečnosti. Bohužel, ne

všichni si to uvědomují a nejmarkantněji to je vidět na tzv. sociálních sítích (Facebook, Twitter, Linkedin, Líbím se ti, Spolužáci apod.).
Všichni totiž v kyberprostoru zanecháváme „datovou stopu“ – i když ještě nežijeme ve světě a´la MATRIX. Pozor! Někteří z nás ale už skoro ano, protože Facebook jej začíná připomínat. Pavučina kyberstruktury si nás omotává, aniž tušíme, jak dokonale. Řada uživatelů si dopady virtuálního světa na svůj každodenní život nepřipouští, a když se v některých případech vyhrotí, neumí si leckdy s nimi poradit.

## Internet jako základní činitel virtuální reality

Terabajty dat proudí ve struktuře sítě sítí po datových linkách, spolu s našimi e-maily, fotkami, viry, červy, malwarem či trojskými koňmi i jiným smetím a jejich počet den ode dne roste a plní kyberprostor tvořený onou celoplanetární sítí více jak miliardy počítačů, propojených do internetu. Na rozdíl od virtuální reality nemá kyberprostor přesně určené hranice. V síti navzájem propojených počítačů nelze mnohdy

přesně určit žádný začátek, ani konec toku dat. Tak, jak se kyberprostor rozevírá s tím, že nemá hranice, ani limity nějaké svobody projevu, přináší s sebou i jisté nové či modifikované sociální jevy. A jedním z těchto jevů je např. tvorba virtuálních komunit, jež jsou v zásadě výtvorem jedinců, často virtuálních individuí, která se prezentují na internetu. Jejich hlavní nebezpečí (o výhodách sociálních sítí jistě všichni víme) spočívá v tom, že řada jedinců si neuvědomuje nejen bezbřehost virtuálního světa, ale ani hranice svého vlastního jednání před počítačem, jehož displej je jakými falešným stínítkem anonymity. „Bohužel, právě pocit anonymity na internetu je veskrze falešný a neoprávněný. Vždy, když bude potřeba dotyčného autora vyhledat, tak ho vyhledáte, s výjimkou skutečně zkušených, technologicky zdatných jedinců, kteří dokáží za sebou tzv. zamést. Co jednou zanecháte na síti sítí, to tam prostě zůstane, ať už jde o vaše radosti, strasti či průšvihy," říká Doc. Ing. Václav Jirovský, Csc., vedoucí Ústavu bezpečnostních technologií a inženýrství, proděkan Fakulty dopravní ČVUT.

## Trocha terminologie

Kyberprostor existuje díky kybernetické infrastruktuře, kterou tak lze chápat nejen v zúženém hardwarovém a softwarovém smyslu, ale i jako faktor umožňující vše to, o čem bude na dalších stránkách hovořit.
Upřesněme si to:
Z hardwarového hlediska patří do kyberstruktury jak velké, tak uživatelské (PC) počítače (vč. notebooků, netbooků, Ipadů atd.) či telefony (mobilní vč. smatphonů i pevné), přenosové sítě včetně mobilních, servery, routery, switche, kabeláže, radiová pojítka…
Díky tomu kyberprostor zaplňují data, což je jakási virtuální projekce člověka. Lidská komunikace na sítích pak vytváří i nefyzické virtuální světy, kde se nacházíme během komunikace zprostředkované počítačem či telefonem.
Možná předpokládáte, že termíny jako kyberprostor (cyberspace) či kybernetická infrastruktura (cyberinfrastructure) jsou slangové výrazy, vniklé v IT či hackerské komunitě v posledních letech. Omyl. Termín Cyberinfrastructure byl poprvé použit už na

tiskové konferenci v květnu 1998 Richardem A. Clarkem, národním koordinátorem pro bezpečnost, ochranu infrastruktury a boj proti terorismu vlády USA (PDD-63) a Jeffry Hunkerem, právě jmenovaným ředitelem Úřadu pro bezpečnost kritické infrastruktury.
„Cyberinfrastructure“ vznikla jako odvozenina z termínu “National Information Infrastructure”, propagovaného viceprezidentem Al Gorem v devadesátých létech v rámci prezidentské směrnice NSC-63 (Presidential Decision Directive NSC-63) o ochraně Americké kritické infrastruktury, na které závisí americké vojenské síly a ekonomický blahobyt obyvatelstva, jako jsou například elektrické rozvodné sítě, energovody jako takové, doprava, rozvody pitné vody i odpadních vod a pod.
Termín "cyberinfrastructure" byl pak převzat USA National Science Foundation (NSF), v roce 2003 a postupně se stal součástí IT slangu.

## Kyberprostor jako pojem

Většina dějů, které nás budou dále zajímat, se díky

vzniklé kyberstruktuře odehrává ve virtuálním kyberprostoru. Ano, řekli jsme si, že to je pátá dimenze našeho bytí, ale to je poněkud básnická licence. Kyberprostor ovšem lze definovat z několika pohledů, byť v současné době neexistuje definice, která by zahrnovala vše a kterou by bylo možné jednotně a bez výjimek používat.
Např. Věra Zelinková z Filozofické fakulty Masarykovy univerzity jej s využitím zahraničních pramenů definuje jako „nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Toto prostředí umožňuje vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace. Zahrnuje počítače a databáze propojené komunikačními systémy, jako například celosvětovou síť internet. Kyberprostor využívá nové možnosti komunikace, jako jsou například emaily, webové stránky, počítačové sítě, telefony, faxy a videokonference.
Nicméně je imaginárním místem, na které se nevztahují omezení fyzického světa. To mimo jiné umožňuje vznik nových identit - uživatel „opouští“ své fyzické tělo a pobývá v tomto (virtuálním) prostředí bez něj.“

Termín „kyberprostor“ sám o sobě je ale třicet let starý, byť teprve v posledních 10 – 15 letech získává reálnou podobu. Vymyslel jej už v roce 1982 známý americký spisovatel sci-fi William Gibson (zakladatel literárního směru zvaného „kyberpunk“), který ho použil nejprve v povídce s názvem Burning Chrome a později ve svém slavném románu Neuromancer z roku 1984. Termín kyberprostor (cyberspace) pak používalo mnoho dalších (především SF) autorů a zdomácněl časem i v odborném slangu, neboť hackeři, počítačoví a síťoví experti tento termín přebrali a používali pro IT infrastrukturu, t.j. počítačové sítě a zejména pak internet.
Gibsonova definice kyberprostoru zní: „… konsensuální halucinace každý den prožívaná miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky ... grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat…
Podle Wikipedie se termín kyberprostor/cyberspace definuje pregnantněji: používá se pro „označení virtuálního světa

vytvářeného moderními technologiemi (počítači, telekomunikačními sítěmi apod.) paralelně ke světu „reálnému...“
Jistě, Gibsonovo vyjádření kyberprostoru je poněkud básnické, nicméně ve světě popisovaném Gibsonem informace získávané z onoho kyberprostoru znamenají moc. Kdo je má, vládne. A jeho vize Matrixu, kdy lidská společnost postupně nahrazuje přírodu a tradiční život globální sítí informací zvanou Matrix, na kterou se lidé připojují a stávají se na ní závislými, se dnes nejeví ani tak moc fantastická. Navíc už dávno – a tím spíše dnes - platí, že informace mají cenu zlata a leckdy i života.

## Za svobodu internetu! ACTA a Anonymous

Počátek letošního roku byl, alespoň pokud jde o události v kyberprostoru a kolem něj, dosti bouřlivý. Demonstrace, napadání vládních webových stránek od USA po Českou republiku, stále ještě demonstrativní ale dosti účinné útoky dnes celosvětové hackivistické skupiny Anonymous. Vypadalo to jako začátek kybernetické války

„anonymních“ uživatelů internetu proti oficiálním státním strukturám. Za zákony SOPA a PIPA v USA a mezinárodní dohodou ACTA (Anti-CountefeitingTrade Agreement), k níž se zpočátku hlásila i česká vláda, ovšem stojí finanční zájmy hudebního a filmového průmyslu a ovšem i knižních nakladatelství.

Ano, hudba se už dnes prodává stále méně na nosičích jako je CD a častěji se stahuje. Konkrétně tržby z prodeje hudby v loňském roce (2011) celosvětově klesly o tři procenta na 16,2 miliardy USD (315,4 miliardy Kč) a tak pokračovaly v klesajícím trendu, který však zpomalil z osmi procent v roce 2010 na citovaná 3 %. Vyplývá to ze zprávy, kterou zveřejnila 24. ledna 2012 Mezinárodní federace hudebního průmyslu (IFPI). Odhaduje ale, že 28 procent uživatelů internetu se měsíčně připojilo na neautorizované služby.

Aa s filmy to začíná být obdobné – proč platit v multikině 150 Kč za vstupenku (kde jsou ty doby, kdy stála první řada 3 Kčs), když si premiérový film za pár dní lze stáhnout i s dabingem např. z Ulozto.cz nebo přepálit od kamaráda... A na internetu lze nalézt stovky a tisíce knih – oskenovaných, v pdf a

dnes i přizpůsobených pro elektronické čtečky – od vědeckých publikací po pohádky či sci-fi. Zadarmo. Samozřejmě, že si lze leccos koupit, ale mnozí uživatelé si zjevně řeknou: Proč utrácet, když to jde zdarma nebo za směšný poplatek za rychlost stahování...

Lobby především zábavního průmyslu začala nutit zákonodárce k jakési regulaci dění v kyberprostoru. Jak se ale ukazuje, s křížkem po funuse. Jediná konkrétní věc, která se vládním strukturám podařila (nemyslíme nyní pobouření milionů zejména mladých lidí, kteří už jsou v kyberprostoru jako doma), bylo zatčení Němce zvaného Kim Dotcom, majitele serveru Megaupload, který údajně okradl nahrávací a filmové společnosti o nějakou tu půlmiliardu dolarů… Jistě, nebude to lehké Dotkomovi dokázat, ale všichni víme, že to, co umožňoval jeho server, bylo nejen inflagrantní porušování copyrightu, ale i jasným důkazem, že se na mírných poplatcích za rychlost nelegálního stahování dá i slušně vydělat. Generální problémem ACTA ovšem není možnost postihovat internetové pirátství, ale například i kopírování už zakoupených děl z desktopu na notebook či iPad, či převedení z formátu např.

Windows Media Player na formát jiný. Snaží se sice ochránit duševní vlastnictví primárně na internetu, ale výkladem svých obecných formulací může způsobit problémy např. i ve farmacii, kde by důsledným uplatněním mohla zlikvidovat např. výrobu tzv. generických léků. Nepřizpůsobuje tedy ochranu autorských práv digitálnímu věku, ale snaží se zabetonovat současný stav copyrightu. A – upřímně řečeno – komu by se chtělo nechat např. celníky na letišti hrabat se ve svém notebooku, a přesvědčovat je, že film, či skladba, které tam jsou uložené, byly zakoupeny na DVD, které ale uživatel přece nebude vozit s sebou…

Celosvětové pobouření internetových komunit a nakonec i řady odborníků, vyvolané snahou o regulaci alespoň části dění v kyberprostoru především výše jmenovaným návrhem dohody ACTA většinu vlád vyděsilo a zase stáhly chvost. Alespoň prozatím.

Aktivity hnutí Anonymus ukázaly, že před soustředěnými, byť většinou „jen“ DDoS útoky nejsou bezpečné stránky nejen české ODS, ale ani americké FBI či Bílého domu.

Anonymous údajně plánovali v rámci tzv. operace

Global Blackout 31. března vyřadit přetížením 13 kořenových DNS serverů internet po celém světě, což v některých kruzích vyvolalo mírnou paniku. Do protiakcí se vložili nejen armádní IT specialisti, ale i Interpol. K žádnému většímu výpadku ale nakonec nedošlo, kompletní destrukce sítě sítí je přeci jen obtížná – odněkud se ostatně útoky musí šířit - ale stejně se dlouze diskutovalo o tom, proč se nakonec útok nerealizoval.

„Vypadá to, že operace Global Blackout mohla skutečně v sobotu ochromit internet," konstatoval tehdy pro server CWZ šéf Interpolu Ronald Noble. Zatím byl hacktivistmus spíše považován za jakési „pubescentní hnutí", které přímo neškodilo, neohrožovalo. Ovšem to, co tzv. Anonymous a jejich příznivci nyní předvedli, možná byla taková stínová ukázka toho, jak by mohla vypadat kybernetická válka…

Zatím i tomu říkáme počítačová kriminalita, zkráceně – kybernalita. Což je poměrně bezpečný podnik. Sedíte doma nebo lépe v kavárně u kávy, nikdo vás fyzicky nevidí, nezná… Proto se jen velmi těžko prokazuje, že právě vy jste pachatel.

## Komu co chybí či nechybí

Že nějaká regulace dění na internetu, nebo – chcete-li v kyberprostoru – je nutná, uznává leckdo. Otázkou ale je, proč se s ní nezačalo už dříve, než se tolik rozmohlo ono nejsvobodnější médium – internet. Svět je bohužel o dost složitější, než jej vidíme prostřednictvím svých displejů. Např. neexistuje ani společná evropská legislativa definující, co to vlastně počítačová kriminalita je.

„Vezměte si, že současná zákonodárství staví na staletých tradicích, a kyberprostor existuje dejme tomu tak 50 let, kdy začínala první komunikace mezi počítači, kdy sice neexistoval internet, ale vznikl už ARPANET. A my se snažíme modifikací zákonů, prověřených staletími, postihovat něco, co existuje historicky kratičkou chvíli – a tudíž to neumíme," konstatuje např. doc. Václav Jirovský, proděkan Fakulty dopravní ČVUT.

„A tak ani nemůže existovat pořádná společná evropská legislativa. Jediné co existuje, je mezinárodní úmluva o boji s počítačovou kriminalitou, ke které přistoupila většina států EU.

Zůstává však spousta nevyřešených problémů, například problém jurisdikce. Čin spáchaný v jednom státě nemusí být tam činem trestným, ale může být trestným ve státě, kde se projevil jeho účinek. Jenomže tam ten pachatel není, protože sedí úplně v jiné zemi… To je tzv. problém distančního deliktu. Bohužel, vnímání práva v kyberprostoru je – řekl bych – velmi problematické…“

Je to krásné, že ona mezinárodní úmluva o boji s počítačovou kriminalitou v EU existuje, ale např. v České republice – na rozdíl třeba od USA a jiných vyspělých států, neexistuje ani standardizace pojmů pro kyberinfrastrukturu, natož něco obdobného, jako např. v americkém státě Oklahoma, kde existuje iniciativa zvaná Oklahoma EPSCoR’s Cyber Infrastructure (CI) Plan . Což je celostátní strategická iniciativa, zahrnující výchovu a vzdělávání pomocí celostátních vzdělávacích programů, seminářů a sympozií, vedených univerzitními kapacitami, výzkumnými pracovníky a instruktory tzv. celostátní CI Poradní skupiny. (Více zde.)

„Představa, že internet je absolutně svobodné médium a jakýkoliv zásah do něj je proti „přírodě a Bohu“ je, šetrně řečeno, scestná. Stejně jako

představa, že dění na internetu nikdo nesleduje. Přitom je podrobováno monitoringu z různých důvodů, z různých směrů a do různé hloubky - nejen zpravodajskými službami - téměř od samého počátku," říká JUDr. Martin Maixner, jeden z předních renomovaných právních znalců IT u nás. A dodává: „Internet je prostě jisté prostředí, které má zákonitě nějaká pravidla. A pokud dnes lidé, reprezentovaní např. skupinami Anonymous, bojují DOS útoky i na vládní www stránky za svobodu internetu, tak se ptám, čeho a čí svoboda to má být. Ovšem s autorským právem to je složité. V nějaké formě existovalo autorství vždycky, ale jeho konkrétní podoba a koncepce, jak ji známe nyní, existuje vlastně posledních 150 let. Je také zjevné, že v té podobě, jak je nastaveno dnes, není úplně použitelné pro moderní technologie, jako je např. právě internet a elektronický trh. Informační technologie totiž mění celé principy, ze kterých právo vzniká.
Platí, že právo je vždy o krok pozadu za životem. Technologie, o kterých hovoříme a které souvisí s internetem, ty jsou ještě o krok před běžným životem… To znamená, že právo je v takových případech „zpožděné" dvakrát, a tudíž neexistuje

šance, aby právo regulovalo něco, co teprve – možná – ovlivní náš život.“
Na druhou stranu internet nemůže být bezbřehým mořem absolutní svobody, protože se dá, stejně jako řada jiných technologií, byť vyvinutých v dobré víře, zneužít. A že zneužíván je – je tu extremismus, kybernetická kriminalita, kyberterorismus, kybernetický extremismus či pornografie - je prostý fakt.
Jenomže platí, že technologie samy o sobě nejsou nebezpečné, nebezpečný je lidský faktor. Bohužel – orwellovský „Velký bratr“ už na nás juká ze všech stran a přesto se novými a novými kanály řine proud kybernality. A někde v pozadí možná čeká ještě něco horšího – cyberwar. Leccos koneckonců v uplynulých měsících naznačil virus Flame.

## Sociální sítě jako médium budoucnosti i skrytá hrozba

Vzhledem k tomu, že se podle posledního odhadu společnosti Intel zvýší do roku 2015 reálný počet

uživatelů internetu ze stávajících dvou miliard na tři, poroste dál i objem globální datové výměny - do roku 2015 se ztrojnásobí a přesáhne 4,8 zetabajtu ročně. Na každého obyvatele Země přitom připadnou v průměru dva přístroje s vlastní IP adresou. Množství nového obsahu souvisí mimo jiné s fenoménem sociálních sítí, které s sebou kromě nových komunikačních možností přinášejí nemalá rizika. Každých 60 sekund lidé nahrají na YouTube 30 hodin obrazového materiálu a současně jiní skouknou na 1,3 milionu videí. 277 tisíc lidí se přihlásí na svůj účet na Facebooku, na Twitteru se objeví sto tisíc nových tweetů a současně zde přibude 320 nových uživatelů.

Každé dva dny nyní na internetu vzniká tolik informací, jako tomu bylo od počátku civilizace do roku 2003. V průměru přes každého z nás nyní denně projdou data v objemu více než 1 GB. Za tři roky bude každý uživatel generovat denně průměrně více než 4 GB dat. Do uvedených přenosů nejsou započítány rozhlas, televize, noviny. Jde jen o síť sítí, o náš virtuální život.

Existují lidé, kteří jsou-li dvě hodiny bez „spojení“ a nevidí na e-maily, tak se hroutí (tzv. netholici).

Pravda, za dvě hodiny se může odehrát v byznysu i na ulici před vaším domem spousta věcí, a svět nezanikne. Ovšem lze litovat ty, kteří si moc berou k srdci, že za šedesát sekund se na internetu:

- globálně přenesou IP data v objemu 639 800 GB
- že proběhne více než dva miliony vyhledávaní na Googlu (v r. 2011 jen 694 455)
- že se odešle se na 204 milionů e-mailů (před rokem jen 168 milionů)
- že je staženo 47 tisíc aplikací
- že se zobrazí na šest milionů webových stránek
- dojde k zaregistrování 1300 nových mobilních telefonů.

## Sociální sítě: pozitiva a negativa

Jak už bylo zmíněno, během každé minuty se z téměř miliardy uživatelů se přihlašuje na Facebooku cca 300 tisíc lidí. Nejste mezi nimi? Sociální, neboli komunitní sítě jsou fenoménem současné doby a virtuálními světy zítřka. Zárodkem Matrixu. Možná.

Možná?
Každopádně jejich existence nepoukazuje jen na lidskou potřebu se sdružovat a chatovat, plkat si s „přáteli“, ale hovoří i o osamění lidí ve světě reálném a hledajícím náhražku ve světě virtuálním.
Kyberprostor totiž nabízí řadě lidí s vypěstovanou závislostí na internetu a sociálních sítích virtualizaci života fyzické osoby, „náhražkový“ virtuální život těm, kteří se nedokáží srovnat s problémy života reálného, fyzického.
Mimo jiné – zakomplexovaní lidé dostávají možnost vyrábět si virtuálně osobnost podle vlastní představy. A taková virtuální osobnost je pak mnohem bližší tomu, jak by dotyčný chtěl vypadat, než jaký ve skutečnosti je.
Sociální sítě ovšem nepřináší jen nové možnosti a radosti, ale také strasti a nebezpečí, stejně jako tomu je v reálném životě. A mnohdy to může být ještě horší. O vašich poklescích se totiž rychlostí světla dozví celý svět. Doslova a do písmene.
Navíc v psychiatrii už dnes rozeznáváme diagnózy, které vycházejí z povahy komunikace v kyberprostoru. Jsou to tak zvaný netholismus (od

workholismus) a netomanie, které jsou projevem závislosti na internetu. Má to podobné abstinenční příznaky jako drogy – máte třeba neustálé nutkání podívat se na e-mail, zda něco nepřišlo? Tak to je začátek netomanie.
Pak přichází nepříjemné pocity při odpojení ze sítě – nejsem ve své kůži, necítím se dobře… až po to, že vlastně neexistuji! Samozřejmě, netýká se to celé populace, ale bohužel, podíl netomanů se stále zvyšuje.
To pak má podle doc. Ing. Václava Jirovského, proděkana Fakulty dopravní ČVUT (info) další konsekvence: „Konečnou fází této závislosti pak je tzv. Jekyll – Hyde syndrom (viz knihu Dr. Jekyll a Mr. Hyde R. L. Stevensona), kdy dochází až k úplnému rozštěpení osobnosti na virtuální a reálnou. Život ve virtuální realitě je totiž mnohem snadnější a tak začíná převažovat virtuální osobnost. Dotyčný člověk pak časem není schopen žít v normální, reálné společnosti...“
Sociální sítě ovšem zaplňují kyberprostor množstvím datové (obsahové) hlušiny, na druhou stranu i v ní lze vyhledat mnoho cenných informací, které často nevědomky poskytují lidé svým „přátelům“. Navíc se

tyto tzv. sociální, lépe řečeno komunitní weby, stejně jako blogy, stávají nástrojem pro manipulaci s lidmi. Jde o něco, čemu říkáme perception management, jinými slovy ovlivňování vnímání okolního dění pomocí vhodného mírného zkreslení skutečnosti.
Proto je už vyspělým dítkem tohoto kyberprostorového jevu Analýza sociálních sítí (SNA). „Vědecká disciplína, která interpretuje svět jako síť složenou ze struktury lidských vazeb. Používá rozmanité zdroje dat, aby zobrazila neviditelnou síť vazeb lidské kooperace. Tato schopnost ji umožňuje překvapivě široké uplatnění v marketingu, organizačním řízení a mnoha dalších oblastech…“ (marketingový výzkumník Jan Schmid)

## Definice úlohy sociálních sítí

Wikipedie konstatuje že: „... sociální síť, zvaná též společenská síť, komunitní síť či komunita, anglicky social network, je propojená skupina lidí… V užším, moderním a značně převažujícím pojetí se sociální sítí nazývá služba na Internetu, která registrovaným členům umožňuje si vytvářet osobní (či firemní)

veřejný či částečně veřejný profil, komunikovat spolu, sdílet informace, fotografie, videa, provozovat chat a další aktivity. Komunikace mezi uživateli sociálních sítí může probíhat buď soukromě mezi dvěma uživateli, nebo (nejčastěji) hromadně mezi uživatelem a skupinou s ním propojených dalších uživatelů. V současnosti nejznámější a největší sociální sítí na světě je Facebook.com s téměř 800 milióny registrovaných uživatelů (leden 2012).“
Definice stručnější může znít asi takto: „Sociální síť (nebo také komunita) je propojená skupina lidí, kteří se navzájem ovlivňují. Tvoří se na základě zájmů, rodinných vazeb nebo z jiných důvodů.“
Z těchto několika slov a vlastních zkušeností si může v podstatě každý vytvořit definici vlastní.
Téma sociálních sítí je velmi živé už řadu let, takže se k nim vyjadřuje i církev: Např. arcibiskup Vincent Nichols, hlava katolické církve v Anglii a Walesu (The Sunday Telegraph, srpen 2009) v této souvislosti konstatoval „že internet a mobilní telefony „dehumanizují“ komunitní život. Uživatelé se sice druží, komunikují, ale nemají osobní vztah a úctu jeden k druhému, jako při reálném setkání. Internetové komunity jsou navíc zpravidla velmi

rozsáhlé a otevřené, navázat zde pevné přátelství je prakticky nemožné, pokud vztah nemá základ v reálném světě.“
Nemusel to být právě arcibiskup, abychom tento fakt registrovali, ale jeho hlas byl hodně slyšet.
Robert Vlach, lektor, konzultant a provozovatel webu Na volné noze konstatuje ve své analýze (info), že podle řady nezávislých zdrojů se právě sociální sítě staly nejčastější aktivitou v kyberprostoru, čímž na internetu sesadily pornografii. Běžní uživatelé tráví v online komunitách tolik času, že se již začíná hovořit o generační proměně webu jako takového. Zatímco jeho současná podoba je formována vizí zakladatelů firmy Google o maximální přístupnosti a dohledatelnosti všech informací, konkurenční Facebook na tyto pravidla hry drze odmítá přistoupit. Jeho úspěšná vize staví na rozlišitelné online identitě jednotlivce a více či méně uzavřených komunitách.

## V hlavní roli Facebook

Nejznámější sociální sítí je dnes Facebook. Tato síť byla původně určená pro studenty Harvardské

univerzity. Dnes jde o rozsáhlý společenský webový systém sloužící hlavně ke komunikaci mezi uživateli, ke sdílení multimediálních dat, k udržování vztahů a k zábavě. Se svou už snad miliardou aktivních uživatelů je zřejmě největší společenskou sítí na světě. Facebook je mladá sociální síť. „Mladá“ z hlediska lidského vnímání času, z hlediska internetového je to už „dospělec“, který má za sebou i letošní skok na burzu… Byl založen Markem Zuckerbergem, poprvé spuštěn v únoru 2004 a během krátké doby se rozšířil i na ostatní univerzity. Od srpna roku 2006 je umožněn vstup každému jednotlivci staršímu 13 let.
Otázka ale zní: Dodržuje někdo toto věkové omezení? Proč si pár let nepřidat…? Ostatně, Mark Zuckenberg prý hodlá spustit Faceboou pro děti do 13ti let (ČTK 07.06.2012), což vzbudilo v zahraničních médiích řadu rozporuplných reakcí. Mají mít malé děti přístup k těmto formám komunikace? Jsou na ně připravené? A co jim hrozí?
Podle zakladatele této sítě je ale třeba "začít s výchovou dětí ve vztahu k Facebooku co možná nejdříve", aby si osvojily pravidla a bezpečné chování na internetu.

Podle jiných hlasů nejsou děti mladší 13 let připraveny na tento způsob komunikace - neumějí rozlišit, co je vhodné zveřejnit, nechápou problémy spojené s narušením soukromí, mohou se stát obětí kyberšikany či zanedbávat spánek. "Navíc se v určité fázi vývoje vyhnou budování reálných vztahů a jejich sociální komunikace se přesune do virtuálního světa," upozorňují odborníci ze společnosti American Academy of Pediatrics v časopisu Time.

Skutečnost je ovšem taková, že už přes 7,5 milionu dětí mladších 13 let, z nichž dvěma třetinám je méně než deset let, vlastní aktivní účet na Facebooku, přestože by podle pravidel neměly mít k této aplikaci přístup. Vyplývá to z údajů London School of Economics, podle kterých děti bez výčitek uvedou při registraci špatné datum narození. Ve většině případů je k porušení pravidel navedou sami rodiče…

Facebook samozřejmě není osamoceným komunitním virtuálním světem, ale při „sdružování“ lidí zašel nejdál. Nyní „mluví“ se svými uživateli v 70 jazycích včetně češtiny a tak se stal nerozšířenějším komunitním webem i u nás. Navíc každého „přítele“, kterého autorizujete do svého profilu, oslovuje s

nabídkou přidat si také vaše „přátele“, a recipročně i vám nabízí přátele vašich přátel. Měřítko počtu přátel na Facebooku se především u „náctiletých“ stává měřítkem úspěšnosti, byť s tím roste míra rizika ztráty soukromí.

## Další sociální sítě

Mezi další nejnavštěvovanější sociální sítě patří:
**Google+** – (vznik - 2011 jako obdoba sítě Facebook, kde hlavní rozdíl spočívá v nastavení sdílení přes tzv. kruhy a sdílet dané věci lze od počátku jen s těmi, pro které to má přínos, nebo se jich to týká.
**Myspace** – vznik 2003, druhá nejpoužívanější sociální síť na světě
**Twitter** – vznikla v roce 2006 a sloužila především pro mikroblogy
**LinkedIn** – vznikla v roce 2003, pracovní sociální síť, především používána v businessu - pro internetové profily a pro pracovní životopisy
A české sociální sítě? Mezi nejoblíbenější patří:
**Lidé.cz** – chatovací server. Slouží jako internetové

fórum, k blogování, jako internetová seznamka, pro ukládání a sdílení fotografií atd. a je uživatelsky spojen se sociální sítí Spolužáci.cz.

**Spolužáci.cz** – slouží pro internetové profily, jako chatovací server. Je určen pro spolužáky a (zejména) bývalé spolužáky, uživatelsky je spojen se serverem Lidé.cz. Obdoba amerického Classmates.

**Líbímseti.cz** – slouží pro internetové profily lidí, jako internetová seznamka, jako chatovací server, pro blogy mládeže atd. Kde jsou ty časy, kdy se dívky se svými utajovanými zážitky svěřovaly papíru způsobem „Milý deníčku, představ si, on mi dnes dal pusu…“?

Teď se to napíše „přátelům“ na Líbímseti.cz či Facebook a ještě doplní fotografiemi, případě z mejdanu, kde jsme byli všichni strašně „cool“. Pak se třeba dotyčná po letech při pracovním pohovoru dozví, že by se neměla pokoušet o striptýz v zaměstnání podobně, jako tenkrát na školním výletě s gymnáziem. Problémem je to, že byť se snažíte později své „hříchy“ z internetu (např. z Facebook) vymazat, stejně v pletivu internetových sítí někde zůstanou. Zamést za sebou totiž umí na síti sítí jen skuteční machři. A těch je nemnoho.

## Jak to na Facebooku funguje?

Každý uživatel má svoji osobní nebo firemní stránku, na které má mimo jiné také svou fotku či logo, základní osobní údaje, případně další zajímavé informace o své firmě či oboru podnikání.
Každý má na své stránce neomezeně velký prostor pro sdělení svých novinek, plánů, akcí, fotografií nebo oblíbených videí. Sám si vytváří skupinu přátel či fanoušků jejich pozváním na své stránky, přičemž osobní stránku mohou navštívit rovněž ti, kteří o to požádají nebo v případě firemních stránek ti, kterým se stránky jednoduše líbí. Prostě stisknou tlačítko s obrázkem palce nahoru a textem "To se mi líbí" a je to. Informace o této akci se zobrazí také přátelům na jejich stránce. Systém má vestavěné komunikační nástroje, které sdílení informací usnadňují a dělají z komunikace zábavu.
Soukromí vůbec je v souvislosti s Facebookem často diskutovaným pojmem, protože uživatelé na něj svěřují velké množství svých osobních informací. Poslední velká diskuse se v tomto ohledu strhla

počátkem prosince 2009, kdy Facebook změnil výchozí nastavení soukromí uživatelů tak, aby maximum jejich informací a dat bylo veřejně přístupných.
Zároveň všem uživatelům změnil nastavení pravidel ochrany soukromí do tohoto výchozího nastavení. Uživatelé pak po přihlášení na Facebook přivítalo okno s informací o změnách nastavení, jež dále odkazovalo do „Průvodce soukromí na Facebooku“, který nejprve chystané změny vysvětlil a poté dále navedl do menu, kde bylo možné provést změny nastavení.
Nutno ovšem podotknout, že některé formulace vysvětlující a obhajující změny nastavení byly spíše marketingové povahy a měly za úkol navést uživatele k tomu, aby nastavení definované provozovatelem neměnil, než aby měly na paměti skutečnou ochranu soukromí uživatelů.
Už při registraci je uživatel vyzván, aby sdělil své křestní jméno, příjmení, e-mail, pohlaví a datum narození. Bez jejich vyplnění není registrace možná. Krom těchto základních informací nutných pro registraci může uživatel do svého profilu zanést další informace o své osobě, jako například informace o

své rodině, příbuzenských vztazích, politických a náboženských postojích, povolání, ale také další kontaktní informace včetně čísla mobilního telefonu. Nepřímo je k tomu uživatel vybízen i ve Facebook's Privacy Policy…

Dále Facebook ukládá záznamy o všech aktivitách, které uživatel v rámci této sítě provádí. Archivovány tak jsou záznamy o aktualizacích statusu, komentářích statusů ostatních uživatelů, komentářích k fotografiím či videím a samozřejmě také záznamy o tom, jak který uživatel kliká na reklamní bannery umístěné na Facebooku. V tomto případě pak Facebook po 180 dní ukládá údaj o tom, který konkrétní uživatel kliknul na kterou konkrétní reklamu. Facebook sice deklaruje, že všechny tyto shromažďované informace mají napomáhat zkvalitňování služeb uživatelům, v případě úniku jsou však tyto informace velmi lehce zneužitelné. Šikovný útočník se díky informacím o přenosu mezi uživatelem a serverem provozovatele může např. zkonstruovat falešný požadavek pro server, díky kterému poté získal všechna práva k napadenému profilu, jako jeho majitel. Zná tak nejen uživatelovo jméno a příjmení, datum narození, pohlaví a e-mail,

ale ví i to, kdy, z jaké IP adresy, jakého počítače a jaké lokality k Facebooku přistupuje. Krom toho všeho má k dispozici seznam internetových stránek, které uživatel navštěvuje, se kterými dalšími uživateli je v kontaktu a na jaké reklamy na Facebooku kliká. Z výše uvedeného jasně vyplývá, že pokud uživatel dodržuje všechna ustanovení z Facebook's Statement of Rights and Responsibilities, disponuje provozovatel tohoto komunitního serveru úplným profilem jeho osobnosti. (Viz: Soukromí na internetu: případy Googlu a Facebook; Mgr. Jakub Jansa, Masarykova univerzita, Fakulta sociálních studií) Takže nedivme se, že Facebook může fungovat na burze s akcemi za 13,5 mld. USD, když na něm lze nalézt nepřeberné množství osobních dat, profilů osobností (jeho hvězdou se stal i americký prezident Barack Obama při své první předvolební kampani, i u nás se na Facebooku objevuje řada politických osobností vč. bývalého premiéra Topolánka) a v neposlední řadě výborných marketingových informací.

Pokud tedy uživatel doplní do svého profilu další nepovinné údaje, jako například místo svého studia či zaměstnání, dochází k dalšímu zpřesnění jeho

osobního profilu, který o něm provozovatel Facebooku může sestavit. Navíc musí mít na paměti, že všechny tyto informace o jeho osobě jsou uloženy na serverech v USA a nakládání s nimi tak podléhá tamějším zákonům.

## Ach ti uživatelé

Asi nemůžeme po uživatelích Facebooku chtít, a by toto všechno znali, či si to uvědomovali. Tím spíše, že obraz světa náctiletého puberťáka je značně zkreslený možná i vzhledem ke komunikaci na síti. Ta mu ovšem poskytuje širokou paletu možností hrát si na pana inkognito, či na někoho úplně jiného. Doc. Václav Jirovský (info) k tomu říká: „..je potřeba si uvědomit, že kyberprostor je prostředí, kde celá řada naprosto běžných zvyků normální lidské komunikace zcela chybí. Například zcela chybí tzv. mimoverbální komunikace, gesta, mimika… Používání emotikonů to nemůže nahradit, protože v normální situaci vy toho člověka vidíte, nemůže vám namluvit, jak vypadá, jak se tváří…“
Nedostatky této mimoverbální komunikace pak

skýtají možnosti skrývání některých rysů osobnosti, na druhé straně dávají možnost si tu osobnost virtuálně vyrábět podle vlastní představy. A taková virtuální osobnost je pak mnohem bližší tomu, jak by dotyčný chtěl, aby vypadal, než jaký ve skutečnosti je. Jde hlavně o to, že komunikace v kyberprostoru nevyžaduje, aby člověk dělal kompromisy jako v reálném životě. V mnoha případech se na chatech vyskytují lidé, kteří mají problém se ztotožněním sama se sebou. Například: internet nabízí možnost, že když budu obrazně řečeno komunikovat s lidmi v jedné místnosti a ti s semnou nebudou souhlasit, tak se seberu a přejdu do místnosti jiné, kde spřízněné duše najdu…“

## Kyberšikana nejen na Facebooku

Na sociálních sítích se tak na celém světě sdružují lidé z různých sociálních skupin, jako je například rodina, kolegové z práce, spolužáci, partner/partnerka, přátelé, další na řadě jsou pracovní či obchodní kontakty apod. Bohužel, při výchozím nastavení profilu jen otázkou času, kdy

dojde k nějaké kolizi.
Nebezpečí a nástrahy číhající na internetu jsou rok od roku zákeřnější. Kybernetická šikana je technicky snadná. Odeslání škodlivých zpráv nebo zveřejnění škodlivého textu široké řadě lidí lze provést několika klepnutími myší.
Mezi lidmi je všeobecně rozšířen názor, že sociální sítě jsou doménou hlavně generace teenagerů, nicméně tento názor neodpovídá skutečnosti. V současné době silně převažují dospělí uživatelé. Pro ilustraci může posloužit věková struktura uživatelů Facebooku v České republice, kde cca 50 % uživatelů je tvořeno věkovou skupinou od 20 do 35 let.
Nicméně nejohroženější skupinou uživatelů na internetu vůbec patří děti a dospívající mládež. Je potřeba poukázat na fakt, že kromě nových hrozeb už děti nejsou jen poškozenými, ale často i pachateli tzv. kyberšikany.
V zahraničí existuje řada případů, kdy byly děti např. spolužáky dohnány až k sebevraždě, u nás se vzhledem k rozšířenosti mobilních telefonů s fotoaparáty stává šikana hitem na YouTube. A nejde jen o šikanu mezi dětmi nebo mezi dospělými, ale i

např. šikanu dětí školou povinných vůči učitelům (viz známý případ nasazování odpadkového koše učiteli na hlavu). Při tom je zarážející, že si “pachatelé“ těchto „legrácek“ ba dokonce brutalit neuvědomují fakt, že po umístnění na internetu mohou být účastníci „té legrační akce, když jsme nakopali Pepíka“ velmi rychle lokalizováni a potrestáni. Otázkou je, zda kyberprostor je viníkem obrovské ztráty sociálního cítění mezi mládeží a obecné neúcty k autoritám, mezi nimiž jsou např. učitelé, ale i rodiče nejbližším cílem.

Jak je vidět, problematika bezpečnosti a tudíž i kyberšikany na internetu se dotýká nejen dětí, ale zejména rodičů a pedagogů. Je třeba dětem vštípit, aby nikdy neposkytovaly svou adresu, telefonní číslo či žádné jiné osobní informace, včetně toho, kam chodí do školy nebo kde si rády hrají, kdy budou či nebudou doma, říci jim, že se by se neměly setkávat s přáteli z internetu osobně, protože „přátelé z internetu“, kteří po nich chtějí „pár fotek“, nemusejí být těmi, za které se vydávají. Dítě si může zdánlivě povídat na internetu se stejně starým kamarádem, který může být ve skutečnosti úplně někdo jiný. Dotyčný na druhé straně pak může získávat od dítěte

cenné osobní informace, telefon, adresu nebo intimní materiál.
Bohužel, ne všichni jsou si tohoto vědomi a největší nebezpečí číhá zejména v domácnostech, kde děti ovládají počítače lépe než rodiče a v kyberprostoru se pohybují mnohem jistěji – a nezodpovědně. Ukazují to velmi jasně i výsledky loňské jarní studie společnosti GFI, týkající se domácího využívání internetu rodiči a jejich dospívajícími dětmi. Umožňují lépe pochopit, jak se obě skupiny chovají online.

## Hrozivá čísla

Studie Parent-Teen Internet Safety Report (zveřejněná 28. června 2011) identifikuje chování rodičů a jejich dospívajících dětí na internetu z pohledu obsahu, komunikace a ohrožení škodlivým obsahem. Studie zjistila, že pokud jde o kontrolu přístupu na internet v domácnosti, rodiče a děti hrají obvyklou hru „na kočku a na myš“, avšak obě skupiny se chovají tak, že vystavují sebe – a v případě rodičů ještě navíc i své zaměstnavatele – zbytečným rizikům.

Průzkumu, který byl proveden mezi 22. březnem a 5. dubnem 2011, se zúčastnilo 535 párů dospělých a dospívajících (tj. celkem 1 070 respondentů) z amerických domácností s přístupem k internetu. Respondenti byli dotazováni na témata online obtěžování, interakce dospívajících dětí s cizími lidmi, technologie internetové bezpečnosti, vzdělávání v oblasti internetové bezpečnosti, návštěvy webových stránek pro dospělé, domácího využívání pracovních počítačů a používání Facebooku.
Klíčová zjištění průzkumu zahrnují:

- 15 % všech dospívajících dívek uvedlo, že bylo obtěžováno po internetu nebo prostřednictvím textové zprávy.
- 31 % náctiletých přiznává, že online někomu sdělili něco, co by nikdy neřekli z očí do očí při osobním setkání.
- 65 % rodičů uvádí, že nejméně jeden z jejich domácích počítačů byl napaden virem a 62 % z nich pocítilo nějaké či vážné problémy vyplývající z tohoto napadení.
- 90 % rodičů, kteří doma využívají pracovní počítače, sdělilo, že je používají také pro

nepracovní účely a 37 % z nich přiznává, že je nechávají používat i svými dospívajícími dětmi.

- 31 % dospívajících chlapců přiznává, že navštěvuje webové stránky určené pro dospělé, a 53 % všech náctiletých, kteří tyto stránky navštívili, přiznalo, že lhalo při uvádění svého skutečného věku, aby získali přístup.
- 34 % dospívajících uvedlo, že si vytvořilo online účty, o kterých jejich rodiče nevědí.
- Pouze 28 % rodičů, kteří používají antivirový software, sdělilo, že denně aktualizují své virové definice, 24 % si není jisto, zda vůbec virové definice aktualizují.
- Téměř dvě třetiny (29 %) náctiletých byly kontaktovány po internetu cizím člověkem a 23 % z nich nějakým způsobem odpovědělo.
- Pouze 36 % rodičů využívá software pro webový monitoring nebo pro filtrování webových stránek, aby věděli o online aktivitách svých potomků a aby mohli blokovat nevhodný obsah.

(viz: report)
Martin Říha, ředitel pro strategii společnosti GFI

Česká republika a Slovensko tyto výsledky komentoval takto: „Není vůbec překvapující, že dospívající mládež se na internetu často chová velmi rizikově, stejně jako se chová v reálném životě. Co je ale překvapující, je přístup rodičů, kteří těmto hrozbám prakticky napomáhají nezodpovědným chováním, jako je například poskytování svého pracovního počítače k soukromým aktivitám nebo laxnost při aktualizování virových definic. Výsledkem je fakt, že využívání domácího internetu je významným rizikem nejen pro rodiny, ale také pro zaměstnavatele rodičů. Závěry této studie provedené v USA jsou přitom v souladu se zkušenostmi, které máme v České republice – není vůbec důvod se domnívat, že čeští rodiče a jejich děti jsou v rámci využívání domácího internetu jakkoliv zodpovědnější či osvícenější."

I závěry českého výzkumu bohužel potvrdily to, co dlouhodobě naznačují také výsledky zahraničních výzkumů prováděných např. v USA, Velké Británii a dalších zemích: Téměř polovina českých dětí je vystavena některé z forem kyberšikany (46,8 %). V rámci výzkumu byly sledovány nejčastější projevy kyberšikany, mezi které patří např. dehonestující

útoky (nadávání, urážení nebo ponižování realizované pomocí SMS zpráv, e-mailů, v chatu, diskuzi a publikací zesměšňujících fotografií, audio nebo audiovizuálních nahrávek), vyhrožování a vydírání, útoky na elektronické účty (e-mailové, diskuzní, účty ke vzdělávacímu prostředí atd.) a jejich manipulaci, případně zneužití např. ke kyberšikaně. Z těchto projevů jsou děti nejčastěji vystaveny nadávkám, urážkám nebo ponižování v rámci SMS zpráv, e-mailů, v chatu nebo diskuzi (15,8 %), dále musí řešit např. napadení svého elektronického účtu (13,5 %) nebo výhrůžky a zastrašování (8,9 %). Problematickou skutečností, která nahrává šíření kyberšikany, je zveřejňování osobních fotografií nebo videozáznamů na internetu nebo jejich rozesílání pomocí mobilního telefonu. V rámci výzkumného šetření bylo sledováno rozesílání především sexuálně laděných fotografií, které poměrně často slouží jako nástroj pro vydírání, sexuální obtěžování atd. Svou obnaženou fotografii již zveřejnilo 10,1 % dotazovaných dětí, což je o polovinu méně ve srovnání s odesíláním sexuálně laděných zpráv – ty odeslalo 22,7 % dětí. Většina dětí však toto chování považuje za rizikové – v případě zpráv to uvedlo 68,4

% dětí a u fotografií 73,3 % dětí. Přesto je ale patrné, že 1/3 dětí se tomuto vysoce rizikovému chování, označovanému termínem sexting nebo sextování, nebrání.
Děti si také často neuvědomují, že své osobní údaje mohou sdílet, i když je někomu přímo nesdělují. Značné množství z nich si totiž zakládá své osobní účty na internetových portálech, kde jsou pak jejich osobní údaje včetně fotografií dostupné komukoliv (např. Facebook, Lidé.cz atd.). Pozor, 99,5 % dětí zná alespoň jednu sociální síť. Navíc soutěží, kdo má o kolik více „přátel“.

**Rodina online**

Bohužel, právě z počtu tzv. přátel vyplývá občas nějaké to nebezpečí, byť jde třeba o kybešikanu. Na to aktuálně upozorňuje zpráva společnosti Symantec Norton Online Family ze dne 23. 11. 2011. Poukazuje na rizika spojená s digitálními technologiemi jako je kyberšikanování učitelů žáky a především nový fenomén, kdy děti učitele provokují a v momentě, kdy mu dojde trpělivost a lidově řečeno

vybouchne, celou situaci natáčí na mobilní telefon a následně zveřejní na internetu.
Hlavní fakta:

- 1 z 5 učitelů má s kyberšikanou od žáků osobní zkušenost nebo zná učitele, který něco podobného zažil
- 67 procent pedagogů říká, že přátelství se studenty na sociálních sítích je vystavuje riziku
- Pouze 51 procent učitelů uvádí, že jejich škola má kodex pro komunikaci mezi učiteli a studenty na sociálních sítích
- 23 procent rodičů, kteří nechali děti používat jejich debetní nebo kreditní kartu pro on-line nákupy, tvrdí, že děti překročily limit.
- 30 procent rodičů zároveň uvádí, že děti použily debetní nebo kreditní kartu k on-line nákupu bez souhlasu.

(Další info.)
Reálná, tedy nikoliv virtuální šikana, je ve škole obvykle omezena na dobu vyučování, ale pomocí internetu může obtěžující osoba dosáhnout na oběť kdykoli. Na internetu také naleznete více lidí, které

mohou šikanovat.
Anonymita a nízké riziko toho, že budou chyceni, vedou dospělé lidi a tím častěji děti a teenagery k tomu, že zkouší věci, které by jinak nedělali, říkají věci, které by při osobním kontaktu neřekli, sdělují údaje, které by ani na papír nenapsali. Kyberprostor je přeci vrba, do které mohu našeptat cokoliv, a nikdo nemusí vědět, že jsem to já, kdo má oslí uši. Otevírá se zde prostor jak pro virtuální exhibicionismus, tak pro shromažďování dat operátory či kyberkriminálními živly právě při využívání (zneužívání) internetových služeb a sociálních sítí.
Kyberšikana je dnes globální problém a s cílem omezit ji v co největší míře, přijímá mnoho zemí různá protiopatření. Ve Velké Británii byl například nedávno na školách spuštěn speciální program, který jim říká, jak s kyberšikanou bojovat. V USA je kyberšikana, tedy anonymní zastrašování, urážení nebo obtěžování přes internet či telekomunikační síť, dokonce federálním zločinem.

## Ovládání mas

Na sociálních sítích ovšem nesedí jen chatující mládež či osamělí lidé, toužící po hřejivém slovu, kterého se v práci či v parku nedočkají, ani úchylkové, lovící nevinná děvčátka nikoliv na pytlík bonbonů, ale na šustění bankovek. Na Facebook se dnes velmi snadno organizují nejen různé zájmové, ale i politické komunity, které dokáží rozpohybovat masy. Typickým příkladem toho je tzv. arabské jaro – série revolučních převratů v arabských zemích Tuniskem počínaje, přes svržení Kadáfího v Libyji či současnou občanskou válkou v Sýrii konče. Facebook nebo Twitter jsou tak neustále inovovaným zdrojem rozsáhlého a zajímavého zdroje dat, jehož využívání se stalo zcela běžným například v rámci monitoringu sociálních sítí. Takoví „názoroví vůdci“ v on-line komunitách jsou ovšem lehce vysledovatelní, patří mezi vzácných 5 % uživatelů internetu, vytvářejících jeho obsah. Díky tomu jsou také jejich názory dostupné i on-line a výzvědné služby či tajná policie je má z čeho analyzovat. Navíc, pro analytické využití dat ze sociálních sítí už dnes nejsou nutné ani programátorské schopnosti. V posledních měsících se totiž objevují nástroje, které

dolování dat ze sociálních sítí značně usnadňují – jmenujme za všechny např. Social Importer pro excelovský plug in NodeXL nebo extenzi programu Google Refine.
Ale to vše jsou jenom software, které snad slouží jen ke statistickým, ale i marketingovým účelům. Jiné, mnohem lepší nástroje mají chlapci z oddělení profesionálního monitoringu ze známých organizací, jenž vše ostatní mimo názvu přísně utajují. Mají ale neostražitější oči a uši. Ale o tom snad příště.

## Nakročeno ke kyberterorismu

Počítačová kriminalita má za sebou dlouhou cestu od doby, kdy v ní šlo většinou jen o digitální formu vandalismu. Vyvinula se v trestnou činnost provozovanou za účelem zisku a obrana stojí miliardy. V dnešní době jsou už útoky na elektronická data samostatným vědním oborem, kterým se zabývají specifické skupiny lidí s pokročilou dělbou práce – specializují se a zaměřují každá na něco jiného. A ne nadarmo se říká, že jediná informace, která je zcela bezpečná, je ta, která ještě nevznikla.

Kybernalita a kyberterorismus se stávají fenoménem počátku 21. století. Útočník – například všehoschopný programátor – dokáže dnes z výkonného počítače zlikvidovat obchodní konkurenci, vykrást banku, vloupat se do utajovaných dat podniků, odstavit energetickou síť, či narušit vojenské operace.

Internet je zneužíván nejen k propagandě a prosazování různých ideologií, získávání nových příznivců, ale v neposlední řadě právě ke kybernetickým zločinům. I když většina zemí intenzivně sleduje počítačové sítě a analyzují provedené útoky, odhalování útočníků ztěžují obecně platná lidská práva, anonymita, kterou internet poskytuje, útoky vedené napříč více státy a další faktory, jako například nedostatečně sladěná či chabá legislativa v jednotlivých zemích, včetně těch v EU.

Potenciální dopad kyberzločinnosti nesmí být podceňován. Názorně to ukazuje níže uvedený výběr zpráv za poslední měsíce roku 2011 a za 1. pololetí roku 2012.

## Účet: Bilion dolarů

Keith Alexander, ředitel americké Národní bezpečnostní agentury, řekl účastníkům konference Maneuvering in Cyberspace, konané v říjnu, že globální náklady kyberzločinu se odhadují na jeden bilion amerických dolarů. Britská policejní jednotka PCeU, která má na starosti e-zločiny, zveřejnila v listopadu, že v uplynulých šesti měsících zabránila kyberzločinům v hodnotě více než 140 milionů britských liber.
Ponemon Institute, americké informační bezpečnostní výzkumné centrum, uvádí, že v minulém roce vzrostla průměrná cena kyberkriminality o 56 procent a firmy nyní stojí v průměru šest milionů dolarů ročně. (AVG Community Powered Threat Report – Q3 2011)
Po finanční krizi v roce 2008 začala organizace OECD přezkoumávat dnešní potenciální „globální šoky“. Vedle hrozeb, které očekáváte – finanční krize, pandemie a sociální nepokoje, musíte také brát v potaz „kybernetická rizika“. Například britská vláda jen v letošním roce vyčlenila 63 milionů liber na

boj proti počítačové kriminalitě. (J.R. Smith, CEO společnosti AVG Technologies; The Future Laboratory Report for AVG Technologies, září 2011)

## DuQu a sociální inženýrství v podnicích

Až 48 % dotázaných podniků a firem se stalo obětí sociálního inženýrství. Dotazované podniky zažily v posledních dvou letech 25 a více útoků a způsobené ztráty dosahovaly od 25 000 po 100 000 USD za jeden bezpečnostní incident. Výjimkou nebyly ani vyšší náklady. Zpráva „Riziko sociálního inženýrství v informační bezpečnosti“ označuje phishing a nástroje sociálních sítí za nejčastější zdroje hrozeb sociálního inženýrství. Informuje tak podniky o nutnosti silné kombinace bezpečnostních technologií a povědomí uživatelů, která vede k minimalizaci četnosti a ztrát z útoků. (Check Point Software Technologies Ltd - The Risk of Social Engineering on Information Security: A survey of IT profesionals, September 2011)
Společnost Symantec identifikovala v roce 2010 více než 286 milionů unikátních variant škodlivého

kódu, což je nárůst o 19 % ve srovnání s 240 miliony v roce 2009. V uplynulém roce se obětí kyberzločinu stalo 431 milionu dospělých a celkové roční náklady spojené s kyberzločinem činí 388 miliard dolarů (zahrnuje finanční ztráty i ztrátu času), což je podstatně více, než je částka spojená s černým trhem s marihuanou, kokainem a heroinem (288 miliard dolarů). (Symantec Internet Security Threat Report 2011/16)

Objevil se Malware DuQu – zaznamenán měl být rovněž v Íránu, kde ale na rozdíl od svého možného předchůdce, červa Stuxnet, údajně nezpůsobil větší škodu. Alexander Gostev z Kaspersky Lab uvedl, že DuQu je přizpůsoben na míru každému jednotlivému příjemci (např. úprava názvu wordovských dokumentů v příloze zprávy, každé oběti se dostalo vlastního řídicího serveru i souboru exploitu). Zajímavou vlastností také je, že malware s instalací vyčkává až do okamžiku, kdy uživatel právě infikovaného počítače ukončuje činnost. (The Register, 7. září 2011)

Další příklad je z konce listopadu 2011. Jak uvedl 24. 11. britský list The Telegraph, z účtů tisícovek uživatelů herní konzole Xbox společnosti Microsoft

zcizili v 35 zemích dosud neznámí hackeři milióny liber. Jen britským uživatelům zmizelo z účtů Xbox Live v průměru 100 liber (2950 korun), někteří ale přišli o více než 200 liber. Není podle listu dosud jasné, kolik uživatelů oblíbené herní konzole bylo takto okradeno a o kolik peněz se celkem jednalo.
"Na falešné webové stránce nabízeli hackeři údajnou možnost získat zdarma Microsoft Points, za které si uživatelé mohou kupovat hry a další zábavu. Právě na této stránce pak poškození uživatelé sami hackerům poskytli detaily o svém účtu, včetně přístupových hesel," uvedli dle zdroje zástupci společnosti Microsoft v tiskovém prohlášení.
A hackeři z hnutí Anonymous napadli a zablokovali některé webové stránky francouzského ministerstva vnitra. Útok byl veden tradiční metodou DDoS skupiny Anonymous, tedy přetížením serveru velkým množstvím připojení. Ministerstvo upřesnilo, že napadený web se zabývá přistěhovalectvím ve Francii. Hnutí prý reagovalo na to, že Paříž podporuje smlouvu ACTA. Hnutí Anonymous poté napadlo i některé české a slovenské servery včetně stránek vlády. (AFP/ČTK 30. 1. 12)

# Demonstrace kybernetické války a hacktivismus

Ani v prvním pololetí letošního roku (2012) se situace (celkem pochopitelně) o mnoho nezlepšila: Lednová studie McAfee Labs předpovídá, že rostoucí množství útoků bude směřovat proti mobilnímu bankovnictví, virtuálním měnám a vestavěným hardwarovým zařízením. Budou podle ní pokračovat trendy z loňského roku: Typy útoků rostoucí v loňském roce se letos stanou dominantními. Laboratoře McAfee Labs předpovídají, že významné budou mj. politicky motivované útoky, demonstrace kybernetické války a vysoce cílené útoky na firmy fungující v určitém oboru. Kybernetičtí zločinci se prý letos více zaměří na systémy rozvodných sítí, na nichž závisí velké množství lidí v každodenním životě – například energovody (elektřina, plyn, paliva) či doprava, jež jsou často navzdory svému významu zabezpečeny nedostatečně. To se týká zejména řídicích systémů těchto provozů (SCADA – supervisory control and data acquisition).

Pokrok v zabezpečení moderních operačních systémů prý způsobí, že se útočníci budou snažit napadat vrstvy pod OS, přibudou tedy útoky na úrovni hardwaru a firmwaru. Ty sice nejsou snadné, ale v případě úspěchu umožňují podvodníkům vytvořit malwarovou vrstvu na úrovni síťových karet, disků nebo přímo BIOSu.
K dalším trendům tohoto roku má patřit využívání podvržených digitálních certifikátů. Hacktivismus v on-line světě bude stále více propojen i s politickými aktivitami ve světě fyzickém. Více než dříve budou tyto akce mířit proti politikům, soudům, policejním složkám, ale i vrcholným manažerům. (2012 Threat Predictions)
Hackerské útoky hnutí Anonymous se nevyhýbají ani České republice. Na konci ledna se mu podařilo napadnout oficiální stránky Vlády České republiky. Hackeři útočili také na stránky Ochranného svazu autorského (OSA). Sérii útoků rozpoutalo zablokování serveru Megaupload. (Informace ČTK: 26. ledna 2012)

## Proti ignoranci politiků

V dubnu 2012 na web unikla další data o členech ODS – mj. i rodná čísla a kontakty. Důvodem útoku měl být nezájem politiků o názor občanů České republiky. ČTK (2. 4. 2012) citovala zástupce ODS, podle které šlo o data odcizená již v únoru.
A jak vypadalo první čtvrtletí 2012 v číslech? Podle údajů společnosti Kaspersky Lab byla zjištěna a neutralizována téměř 1 miliarda škodlivých objektů, což je o 28 procentních bodů více než v předchozím čtvrtletí. Online pokusy o proniknutí malware tvořily 50 % všech útoků. To je až o 10 procentních bodů více než v předchozím čtvrtletí. Bylo zaznamenáno 95 080 549 URL sloužících k šíření škodlivého kódu, což je o 61 % více než ve 4. čtvrtletí 2011. (Info)
V oblasti malwaru během května přepustil HTML/ScrInject.B trůn na vrcholu žebříčku celosvětových a evropských škodlivých kódů hrozbě INF/Autorun, která tak zaznamenává velký návrat s podílem 6,36 % na celém světě a 4,99 % v Evropě. Na druhém místě setrvává HTML/Iframe.B s podílem 4,84 % ve světě a 4,81 % v Evropě. Hrozba HTML/ScrInject.B se propadla na třetí pozici, v květnu zaznamenala celosvětový podíl 4,09 %, v

Evropě pak 4,35 %. Šíří se především přes vyměnitelná média, nejčastěji USB flashky a externí pevné disky. Na pozoru by se uživatelé měli mít i před řadou dalších nezvaných návštěvníků. Vyplývá to z květnové statistiky antivirové společnosti Eset. Druhou příčku ve statistikách obsadil virus Iframe.B, jenž přesměrovává internetové stránky na podvodné weby. Třetí příčka patřila škodlivému kódu ScrInject.B, který se vyskytuje na podvodných a napadených webových stránkách a automaticky stahuje po jejich návštěvě do počítače další viry. Ten byl přitom ještě minulý měsíc nejrozšířenější hrozbou vůbec.

„Jedinou dobrou zprávou je, že Flamer, nejnovější státem podporovaný digitální terorismus v podobě malware, v dohledné době pravděpodobně váš počítač nezasáhne. Pokud tedy nejste vládní úředník v jedné ze zemí Blízkého východu nebo nepracujete pro některou z těchto vlád na vývoji zbraní," konstatuje bezpečností expert společnosti ESET Stephen Copp. (Info)

## Analýza řídicí infrastruktury viru Flame

Tvůrci malwaru Flame jej využívali pro kyber-špionáž a k infikování počítačů, z nichž pak virus odcizoval data a citlivé informace. Odcizená data virus odesílal jednomu ze svých řídících serverů (C&C). Právě toto vyplývá z výsledků podrobné výzkumné zprávy společnosti Kaspersky Lab, která C&C infrastrukturu viru Flame intenzivně monitoruje.
Kaspersky Lab zveřejnila odhalení vysoce sofistikovaného škodlivého programu Flame až 28. května. Virus byl aktivně využíván jako kybernetická zbraň zacílená na instituce v několika zemích. Byl odhalen odborníky během vyšetřování provedeného na popud Mezinárodní komunikační unie (ITU), jejímž zřizovatelem je OSN. Analýza zákeřného programu potvrdila, že se jedná o dosud nejrozsáhlejší a nejkomplexnější kybernetickou sadu nástrojů. Kaspersky je přesvědčen, že za tímto počítačovým virem stojí nějaká bezpečnostní služba. Flame je totiž schopen nahrávat zvuky přes mikrofon počítače (sám si jej zapne), pořizovat snímky obrazovek, přepínat BlueTooth rozhraní v počítači a z dalších BT zařízení stahovat jména a telefonní čísla. (Info)
Velmi populární se stala zpráva z letošního června o

tom, že se na webu (české) Poslanecké sněmovny 19. června objevila sbírka filmů a porno. Hackeři využili bezpečnostní díry a umístili na ně sbírku filmů, a to včetně nejméně jednoho pornografického klipu. Stránky byly chvílemi nedostupné.
O nedokonalé ochraně poslaneckého webu se ovšem už nějakou dobu vedou diskuse na serveru soom.cz kde se scházejí i hackeři. "Dá se tam toho najít opravdu hodně. To nejmenší, co si z podrobného prozkoumání databáze odnesete, je detailní znalost systému. Stačilo by využít exploity a je to vaše. Mimo to je tam spousta 'zajímavých' věcí," napsal jeden z uživatelů.
„Web poslanecké sněmovny byl nekvalitně zabezpečen už dávno. Na darknetu se infomace potřebné k prohlížení vnitřního systému šíří už od září loňského roku. Podobně nízká úroveň zabezpečení je i u jiných institucí. O tomto katastrofálním stavu a neschopnosti jsme informovali už mnohokrát…“ (Info)

## Kybernetická kriminalita

Výše uvedené citace jen z posledních měsíců ukazují na konkrétní dopady nebezpečí kybernetické kriminality (tzv. kybernality) a na paletu možností zneužití kyberprostoru ke kyberterorismu. Prudkým vývojem prochází mimo jiné vysoce cílený (spear) spam spojený s phishingovými podvody - a s ním spojené aktivity současnosti jsou zaměřeny jak na samostatné počítače, notebooky, iPady či tzv. chytré telefony (smartphone) připojené na internet. Hlavním cílem útočníků už není vytvořit škodlivý kód, který způsobí uživateli problém, ale kód, který umožní ovládnutí počítače pro jeho následné zneužití, a to k finančním krádežím i spamovým útokům. Takto ovládané počítače jsou i obchodovány a zneužívány pro další kriminální činnosti, z nichž nejviditelnější je právě využití těchto PC k rozesílání spamu či DDoS útokům na vybrané cíle, které si lze u skupin profesionálních tzv. Hackers for Hire - H4H – za patřičný honorář objednat.
Např. DDoS útok na webový portál lze údajně pořídit za 5 až 10 dolarů na hodinu, za 40 až 50 na den; za 350 - 400 dolarů může útok trvat až týden, 1.200 USD stojí útok měsíční. (Info).
Aktivity těchto skupin pozorujeme zejména v oblasti

tzv. kyberterorismu, kdy napadají servery protistrany ze zištných či ideologických důvodů, ale například také z důvodů ekonomických (finančí ztráty, vyřazení konkurence apod).
Zvláštní podskupinou je pak tzv. hacktivismus (složenina ze slov hack and activism), jakési protestní hackerské hnutí proti politickému establishmentu. Nejvýraznějším představitelem v současnosti jsou tzv. Anonymus.
Termín hacktivismus byl poprvé použit v r. 1996 partou hackerů Omega, provozujících od roku 1984 stránky Cult of the Dead Cow na farmě v Lubbocku v Texasu. Cult of the Dead Cow, neboli CDC, je organizace založená v roce 1982. Mezi jejich nářadí patří osvědčené hackerské nástroje, jako jsou např. web site defacements, redirects, DoS (Denial-of-Service attacks), web site parodie, virtual sit-ins, virtuální sabotáže, ale třeba i tzv. typosquatting.
Je ovšem nepopiratelným faktem, že skutečně technicky zdatných a dokonalých hackerů je velice málo. I tito útočníci používají automatizované systémy vyhledávání zranitelností a jakýkoliv nezabezpečený systém či počítač se může stát (prý není otázkou zda, ale za jak dlouho) cílem útoku a zneužívání.

„V komunitě, která spadá do té šedivé zóny na internetu, rozeznáváme dnes celou řadu typických skupin. Já osobně za jednu z nejnebezpečnějších považuji skupinu tzv. „skript kiddies“, což jsou začínající nezkušení hackeři, kteří snad ani nechtějí škodit, ale někde stáhnou z internetu nějaký exploit a snaží se jej použít. A tím, že neví, o co jde, tak to někde shodou okolností zafunguje, a oni pak neví, co s tím,“ konstatuje doc. Václav Jirovský z fakulty dopravní ČVUT. „Skript kiddies je totiž hodně, neboť chlubení se v hospodě před kamarády nebo před děvčaty, kam všude jsem se naboural, patří k normálnímu profilu této kybernetické generace. Proto vidím v této skupině opravdové, největší nebezpečí.“

## Síla a slabiny

Výkon dvoujádrových a čtyřjádrových procesorů dovolí rychle prověřit řadu kombinací přístupových hesel. O novém počítači v síti se tak během jejich snahy nedozví zřejmě většina administrátorů, natož aby měli čas reagovat. Za takovým průnikem už

samozřejmě není konkrétní člověk u počítače, ale robotizované systémy, které běží – na napadených počítačích.
Není ale divu, protože zejména domácí počítače a notebooky jsou velmi často málo zabezpečené a uživatelé je chrání primitivními hesly, jejichž seznamy si hackeři vyměňují. Řada i firemních počítačů, ba i firewalů, zůstává pak ve firemním (defaultním) nastavení, což útočníkům zjednodušuje práci.
Společnost Splash Data zveřejnila v listopadu 2011 žebříček 25 nejhloupějších hesel, která lidé na internetu v daném roce používali. Při vytváření statistiky přitom vycházela ze seznamů přihlašovacích jmen a hesel, která se podařilo hackerům od ledna až doposud lidem odcizit.
Jak je podle následující tabulky patrné (uvádíme jen 10 hesel), nejčastěji lidé používají jako heslo jednoduše slovo – „heslo“ (anglicky password).
Zde je **10 nejhloupějších hesel**:

- 1. password
- 2. 123456
- 3. 12345678
- 4. qwerty

- 5. abc123
- 6. monkey
- 7. 1234567
- 8. letmein
- 9. trustno1
- 10. dragon

Mimochodem: Speciální programy hackerského podsvětí dokáží čtyřmístné heslo, složené z číslic od nuly do devítky, prolomit za dvě minuty.
Zdá se ale, že od doby zveřejnění výše uvedené tabulky se nic nezměnilo – lidé nadále používají stejná hloupá hesla. Ukázala to nedávná kauza LinkedIn. Na začátku letošního června se podařilo hackerům ukrást více než šest miliónů přístupových hesel k uživatelským účtům na sociální síti LinkedIn. Toho využil bezpečnostní analytik Mark Burnett a z dostupných dat sestavil seznam nejpoužívanějších hesel. Nejpoužívanějším heslem je nadále – password. Toto slovo lidé používají neustále i přesto, že odborníci před ním varují už několik let. Zpravidla jej totiž hackeři používají jako jeden z prvních klíčů při prolamování účtů. To samé platí i o číselné kombinaci 123456, která se umístila ve statistikách

na druhém místě.
„Zatímco mnoho lidí zlepšilo bezpečnost a sílu svých hesel, je stále obrovské množství těch, kteří používají již dávno profláknutá hesla. Ve skutečnosti 91 procent uživatelů z testovaného vzorku používá jen tisíc různých kombinací hesel," konstatoval Burnett.
Seznam **20 nejpoužívanějších hesel, který vytvořil Mark Burnett z uniklých dat ze sociální sítě LinkedIn**:

- 1. password (heslo)
- 2. 123456
- 3. 12345678
- 4. 1234
- 5. qwerty
- 6. 12345
- 7. dragon (drak)
- 8. pussy (kočička)
- 9. baseball
- 10. football (fotbal)
- 11. letmein (pusť mě dovnitř)
- 12. monkey (opice)
- 13. 696969
- 14. abc123

- 15. mustang
- 16. michael
- 17. shadow (stín)
- 18. master (mistr)
- 19. jennifer
- 20. 111111

Výsledky jsou znovu dost šokující - hlavně prvá tři místa se vyskytovala ve více než 90 % veškerých příspěvků. Za povšimnutí stojí i heslo na 10. místě, a další, která s bezpečností opravdu nemají nic společného (viz např. 111111 či frekventované pussy apod.).
Daleko lépe naše data a soukromí ochrání alespoň osmimístná hesla. Na osmimístné heslo totiž připadá 72 057 594 037 927 900 kombinací. Delší hesla je také zpravidla dobré kombinovat s číslicemi a různými znaky, aby se nejednalo pouze o běžně používaná slova. Tato svatá pravidla bohužel nedodržují nejen v domácnostech, ale často ani ve firmách a organizacích. Standardně nejlehkomyslnější jsou firmy kategorie SMB, a to jak v Evropě, tak na ostatních kontinentech.

## SMB sektor

Řada výzkumů dokazuje, že většina malých a středních firem žije v přesvědčení, že se díky své velikosti oběťmi kybernetického zločinu stát prakticky nemohou. Kyberzločinci ovšem mezi firmami z hlediska jejich velikosti už dávno nerozlišují. Každá firma z kategorie SMB, dokonce i velmi malá, má přeci údaje o svých zákaznících nebo finanční informace, které mohou narušitelé zneužít. Aplikační servery totiž, ať už se jedná o datové, poštovní, databázové či jiné servery, jsou častým cílem útočníků právě proto, že skrývají zpravidla to nejcennější, čím společnost disponuje – know-how, databáze klientů, finanční informace atp. Často jsou kompromitované servery a na nich uložená data zneužívána k nelegální činnosti a důvěra klientů se pak jen těžko získává zpět.
Na konkrétních faktech to ukazuje například studie SMB Threat Awareness Poll společnosti Symantec Corp., která byla uvolněna už 18. listopadu 2011. Podle jejích výsledků se malé a střední firmy nepovažují za cíle kybernetických útoků, přestože

mají o možných rizicích a hrozbách relativně velké povědomí.
Vzhledem k tomu, že se o nebezpečí útoků na SMB firmy důrazně upozorňuje přinejmenším posledních deset let, přinesl výzkum dosti otřesné poznatky. Zatímco dvě třetiny podniků sledují a omezují počet lidí s přihlašovacími údaji, 63 procent vůbec nezabezpečuje ani počítače, které jsou využívány pro elektronické bankovnictví. 61 procent dotázaných nemá nainstalován antivirový program na všech počítačích, 47 procent nechrání své e-mailové servery nebo služby.
Tato skutečnost je otřesná i vzhledem k tomu, že jde o data stále aktuální - výzkum byl realizován telefonicky v září 2011 a dotazováni byli správci a IT manažeři, kteří spravovali výpočetní techniku. Zúčastnilo se ho 1 900 organizací z celého světa. Jedna čtvrtina respondentů spadala do kategorie firem s 5 až 49 zaměstnanci, druhá měla 50 až 99 pracovníků, třetí čtvrtina zaměstnávala 100 až 249 lidí a poslední 250 až 499 osob. (Zdroj: Report: SMB Threat Awareness Poll Global Results 2011)
SMB firmy tak vlastně otevírají dveře dokořán útočníkům v době, kdy kyberzločincům stojí zato

ukrást údaje z vaší kreditní karty a vybrat z vašeho konta pár tisíc dolarů, natož pak vybrat z banky firemní konto, či prodat obchodní informace, hacknuté z vybraného firemního serveru.
Bezstarostnost lidí, starajících se o firemní počítačové sítě a jejich zabezpečení je až zarážející i vhledem k chatování zaměstnanců na sociálních sítích či prohlížení různých (včetně pornografických) webových stránek. A to i v tak informaticky vyspělé zemi, jako jsou USA, což mj. dokazuje i nedávný průzkum společnosti GFI Software, dodavatele infrastruktury právě pro malé a středně velké podniky. Ta udává, že SMB společnosti ve velké většině nevlastní adekvátní bezpečností řešení a ani nemají nastavenou politiku v oblasti využívání podnikového internetu vlastními zaměstnanci, sloužící k ochraně proti škodlivým webovým stránkám a dalším online hrozbám.
Významně ovšem rostou bezpečnostní rizika i v souvislosti s používáním USB klíčenek a dalších výměnných paměťových médií. Statistiky, které má GFI Software k dispozici, například ukazují, že 48 % zaměstnanců připouští, že v případě výpovědi by si s sebou při odchodu vzalo důvěrné firemní informace.

39 % zaměstnanců by si uložilo informace firmy v případě, že by jejich budoucnost ve firmě byla v ohrožení. Opět se ukazuje, že nehorší je tzv. vnitřní nepřítel, tedy lidé, pracující ve firmě.
Tak na 40 % všech SMB podniků rovněž registrovalo prolomení bezpečnostní ochrany kvůli brouzdání zaměstnanců po webových stránkách obsahující malware. Průzkum byl proveden ve 200 amerických podnicích s 5 - 249 zaměstnanci výzkumnou agenturou Opinion Matters s cílem porozumět procesům SMB firem v oblasti webmonitoringu a filtrování obsahu webu. (Info)

**A ještě jednou: Sociální inženýrství**

V mnoha případech je využíváno tzv. sociální inženýrství, a to zpravidla v rámci cílených útoků. Jeho podoba se ve světě výrazně liší v závislosti na jazykových a kulturních rozdílech, nicméně cílem je většinou pomocí klamavých www stránek či e-mailu získat osobní (firemní) data s přístupovými kódy např. k bankovnímu kontu.
Jak dokládá zpráva společnosti McAfee (McAfee

Threats Report: Third Quarter 2011), množství spamu sice zůstává na nejnižší úrovni od roku 2007, ale vysoce cílený (spear) spam spojený s phishingovými podvody však prochází prudkým vývojem. Rostoucí efektivita a sofistikovanost těchto podvodů s sebou nese vyšší úroveň ohrožení. Útočníci se snaží tyto podvody měnit také v průběhu roku (Vánoce, Svatý Valentin, Velikonoce a další svátky, prázdniny apod.) a přizpůsobovat je aktuálním událostem. V USA se dnes spam nejčastěji maskuje jako oznámení (Delivery Service Notifications, tj. falešná zpráva o problémech při doručení e-mailu), ve Velké Británii jsou rozšířené „nigerijské“ podvody, v Rusku zase farmaceutický spam (nabídky léků). V Německu a dalších středoevropských zemích se spam obvykle maskuje jako nabídka třetích stran.

## Situace v ČR

Nedělejme si iluze, že v ČR a v sousedních evropských státech je situace lepší – v loňském roce zaznamenala Policie ČR zhruba 600 případů

internetových podvodů, nejčastějším případem jsou fiktivní prodeje zboží a služeb. (Otázkou ovšem samozřejmě je, nakolik lze toto označit za internetový podvod. Byl by případ, kdy by nabídka přišla poštou, označen jako poštovní podvod? Asi ne...)
Vlastní zkušenost s DSN v ČR: v podobě výzvy providera UPC o sdělení nejnovějších osobních údajů a přístupových hesel, údajně kvůli rozšíření e-mailové schránky a služeb uživatelům z 18. listopadu t. r., přičemž klientské centrum na tento útok přes výzvy nereagovalo a klienty neupozornilo.
V poslední době ale Policie ČR zaznamenala nová rizika v podobě stále častějších krádeží identity. Na negativní trend vývoje internetové bezpečnosti reagovaly už společnosti Microsoft, Česká spořitelna a Seznam.cz a společně založily projekt Bezpečnýinternet.cz za podpory Policie České republiky.

## Útoky na chytré mobily

Letošní rok (2012) by měl být z pohledu bezpečnosti IT vůbec nejrušnější v celé historii. Počet přenosných

počítačů a mobilních zařízení s přístupem na internet totiž letos vzroste na sedm miliard a poprvé převýší počet obyvatel planety. Do roku 2015 by se pak měl počet mobilních zařízení zvýšit na 15 miliard. Vyplývá to z červnové prognózy společnosti Intel.

Tvůrci malwaru těží především z popularity „chytrých“ mobilních telefonů, tzv. smartphonů s operačním systémem Android, který je nyní nejrozšířenějším a tudíž nejnapadanějším. Na tuto platformu cílí prakticky veškerý nový mobilní malware. K nejrozšířenějším podvodům patří trojské koně odesílající SMS, které shromažďují osobní informace a působí uživatelům i přímé finanční škody. Objevují se i první botnety, které kyberzločincům slouží pro správu ovládnutých mobilních přístrojů. Např. stáhnou jeho obsah přes rozhraní Bluetooth i na určitou vzdálenost. Viry a další typy škodlivého softwaru mohou kromě krádeže nebo smazání informací uživatele poškodit například i tím, že nepozorovaně odesílají SMS zprávy nebo realizují volání na speciálně tarifikovaná čísla. K šíření malwaru mohou podvodníci používat protokol Bluetooth nebo dokonce kódy QR (quick response).

Soukromá zařízení používaná na pracovišti pak

představují pro firmy další bezpečnostní výzvu. Ukazuje to i poslední studie společnosti Fortinet, která analyzovala trend pronikání soukromých mobilních zařízení do pracovního prostředí (Bring Your Own Device, BYOD).

Průzkum byl zaměřen na mladé, aktivní uživatele mobilních zařízení, kteří přicházejí na pracoviště s představou, že zde mohou využívat své vlastní přístroje. Výsledky ukazují zejména jednu znepokojivou skutečnost: 1 ze 3 respondentů uvedl, že v případě, že by firemní bezpečnostní politika používání soukromých zařízení pro pracovní účely zakazovala, pak by předpisy svého zaměstnavatele byli ochotni porušovat a obcházet. Závěry průzkumu podtrhují fakt, že podniky musí vyvinout bezpečnostní strategie, které jim umožní se s trendem BYOD vyrovnat.

Na pracovišti nebo pro pracovní účely používá svá osobní mobilní zařízení až 74 % respondentů průzkumu. Ještě důležitější je, že 55 % z nich tuto možnost vnímá mnohem spíše jako své „právo“ než jako „výsadu“. Z pohledu uživatelů je hlavní motivací pro toto chování požadavek mít neustálý přístup ke svým oblíbeným aplikacím, především k sociálním

sítím a soukromé komunikaci. Závislost na osobní elektronické komunikaci je velmi silná: 35 % respondentů si nedokáže představit den bez přístupu k sociálním sítím, 47 % bez psaní SMS zpráv.

Mladí zaměstnanci přitom často chápou, že trend BYOD může pro jejich organizaci představovat bezpečnostní riziko. 42 % připouští, že výsledkem může být únik dat a vystavení firemního IT systému dalším hrozbám. I tak ale více než třetina (36 %) respondentů připouští, že porušují nebo by byli ochotni porušovat firemní zákaz používat osobní zařízení pro pracovní účely. Ovšem až 30 % dotazovaných uvádí, že nejsou ochotni dodržovat ani firemní zákaz používat neschválené aplikace. Toto riziko roste, protože uživatelé si mnohdy představují, že by měli mít možnost si pro pracovní potřeby sami vybírat nejen zařízení, ale i aplikaci. Dokonce se pro tento trend již objevilo i speciální označení: BYOA (Bring Your Own Application).

Ještě horší se z pohledu zabezpečení zdá, že zaměstnanci nejsou nadšeni z možnosti, že by jim firmy měly na jejich soukromá zařízení instalovat bezpečnostní software. 66 % respondentů si myslí,

že zabezpečení zařízení je jejich vlastní věc, a to i když ho používají pro pracovní účely. Odpovědnost zaměstnavatele zde uznává pouze 22 % dotazovaných.

Průzkum Fortinet Internet Security Census 2012 byl proveden v květnu a červnu 2012. Na objednávku společnosti Fortinet ho realizovala nezávislá výzkumná firma Vision Critical a výsledky jsou založeny na datech z celkem 15 států (USA, evropské a východoasijské země). Dotazováni byli především absolventi vysokých škol a zaměstnanci ve věku 21–31 let, kteří vlastní smartphone, tablet nebo notebook.

Vzhledem ke geometrickému nárůstu počtu mobilních zařízení. Postoje právě těchto mladých uživatelů smartphonů či iPadů apod. do budoucna nevěstí nic dobrého.

Nicméně se potvrzuje se známý fakt, že zatímco útočníci a škodlivé programy jsou stále důmyslnější a je obtížnější je zjistit, uživatelé se stávají nejslabším článkem, protože jsou méně ostražití v ochraně svých on-line zařízení. Kombinace těchto dvou faktorů představuje potenciálně katastrofální scénář

počítačové trestné činnosti.

## Rizikové implementace

To, co rovněž ohrožuje chod a bezpečnost našich dat, je častá dostupnost informací o používaných technologiích a postupech. Taková znalost samozřejmě případnému útočníkovi zjednoduší práci. Jak je možné, že jsou takové citlivé informace často zcela jednoduše dostupné?
Jde o střet protichůdnosti různých požadavků. Prvním z nich je totiž transparentnost a co nejnižší cena nakupovaných technologií, a tím i zveřejňování informací, jaké technologie používáme a kdo je případně implementoval. Právě přes sdělení, kdo implementoval danou technologii, je často možné se dostat k případovým studiím, a tím i k šablonám v postupu implementace a konfigurace (nejsnáze prolomitelné jsou podle českých hackerů sítě postavené na hardware Cisco – protože jsou nejrozšířenější ve světě).
Nicméně z uvedeného vyplývá, že čím méně informací je o nás veřejně a v podstatě zdarma

dostupných, tím je vše pro případného útočníka dražší a složitější.
Pokud jde o specifika České republiky, to, že jsme malá země, neznamená, že jsme na tom co se týče internetového propojení hůře. Ovšem co nám z hlediska bezpečnosti chybí, jsou jasné zákonné normy, jak bojovat proti útočníkům – proti lidem, kteří pěstují např. phishing, vyberou cizí konto, nebo spamem vyřadí firemní server - a to jsme ještě nezažili – podobně jako Estonsko masivní DDoS útok neřku-li útok na SCADA systémy via Stuxnet.
Je potřeba znovu zdůraznit, že bychom měli mít legislativní procesy nastaveny tak, abychom byli schopni mezinárodní spolupráce proti organizované počítačové kriminalitě a zejména pak - kyberterorismu. Vzhledem k sofistikovanosti útoků se však často pojmy kybernalita a kyberterorismus poněkud stírají.
Kybernetická kriminalita, byť se zdá, že jde většinou „jen“ o peníze, ovšem zůstává jakýmsi předstupněm kyberterorismu. Otázkou je, kdy daný jednotlivec či skupina přestoupí onu pomyslnou hranici, která je stále tenčí.
Bohužel, neexistuje univerzální nástroj, který by nás

chránil, který by oddělil to vadné, maligní, od toho dobrého. My musíme reagovat na to, jak se svět kolem nás, tedy i ten virtuální, vyvíjí, a proto sice vyhráváme bitvy, ale mohli bychom prohrát válku…

## Hacktivismus a kyberterorismus

Na internetu jsou dnes závislé nejen miliony - a snad lze říci že i miliardy - lidí, ale na datech běhajících po síti sítí dnes často závisí také úspěšnost fungování jak jednotlivých firem, tak celých průmyslových odvětví; a do jisté míry i národních vlád či nadnárodních institucí. To s sebou nese jak výhody, tak i novou zranitelnost společnosti. Rovnice je zde jednoduchá – čím vyspělejší stát, tím větší zranitelnost prostřednictvím datových sítí. Mimochodem – dovedete si představit ministerstva, policii či armádu bez výpočetní techniky a tykadel do kyberprostoru? Nedivme se tedy, že prostřednictvím kyberprostoru lze například ochromit infrastrukturu celého státu, jak se to stalo před pár lety v Estonsku, či v Gruzii a v Litvě.
To, že se tzv. Anonymous podařilo shodit servery

FBI, Scottland Yardu nebo Bílého domu, zveřejnit hesla a e-maily lidí z NATO či české ODS, je proti tomu legrace, možná s výjimkou ohlášené, ale nedokonané snahy o shození celého internetu útokem na základní DNS servery z března letošního roku (tzv.operace Global Blackout), kterou už lze označit za teroristický útok.
Bohužel neříkáme nic nového - internet je stále více zneužíván nejen hacktivisty a´la citovaní Anonymus, ale přímo extremistickými a teroristickými strukturami, které zde šíří jednak svoji ideologii a propagandu, jednak mohou útočit na fyzické tj. průmyslové, vládní či vojenské objekty či energovody, napojené – jak jinak – na internet.

## Co už je kyberterorismus

Kyberprostor tak dnes čelí drsnějším formám hrozeb, než je „pouhá“ kriminalita, byť je v řadě případů složité odlišit, zda jede o pouhý „kriminální“ čin, nebo o teroristický útok. Pokusme se tedy vymezit, co je obecně pokládáno za kyberterorismus.
Obecně řečeno: Jde o tzv. neletální (nikoli smrtící)

formu teroristické činnosti realizovanou skrze služby, které podporuje a sdílí daná informační či komunikační síť. Sekundárním důsledkem kyberútoku ale může být i fyzická likvidace konkrétního objektu nebo systému, což může vést i k ztrátám na lidských životech. Ovšem – zde se většinou (zatím) nejedná o primární cíl útoku. Kyberterorismus je tedy souhrnným názvem pro teroristické aktivity, jejichž cílem, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“ a virtuální či fyzické objekty nacházející se v kyberprostoru. Komplikovanější je však samotná definice toho, co ještě lze zahrnout do kybernality a co už do kategorie kyberterorismus – je jím např. elektronický teror žáků vůči učitelům na školách (jejich zesměšňování např. na YouTube apod.), kybergrooming, sexting – nebo až SCADA útok na tranzitní trasu sibiřského plynovodu či atomovou elektrárnu?
Klasická - nebo chcete-li oficiální definice kyberterorismu formulovaná Dorothy E. Denningovou zní následovně: „Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku

proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“
Bohužel, tato známá americká analytička dění v kyberprostoru chápe jako akty kyberterorismu téměř výhradně útoky směrované proti kritické infrastruktuře, jež mají za cíl získání informační nadvlády. Paradoxně častěji jsou na internetu zaznamenávány útoky narušující funkci určité služby či jejích součástí, aniž by daný útok byl veden proti konkrétní společnosti nebo vládě s konkrétním účelem (např. vydírání).
I ve svém příspěvku Whither Cyber Terror? k desátému výročí útoku na WTC, (věnovaném především tzv. „Džihad teroru”) ale konstatuje, že v zásadě „…žádná teroristická skupina zatím neprokázala schopnosti ani zájem o využití kyberprostoru k rozpoutání teroru jako takového. Tyto skupiny používají kyberprostoru především pro šíření svých informací a výzev k zapojení se (jejich příznivců) do dalších aktivit, které podpoří jejich konečné cíle...“ (Poznámka autora: A to v té době ještě nezačalo tzv. Arabské jaro…)

To podle Dorothy Denningové ale neznamená, že kyberprostor je bez vážných hrozeb. Naopak, podle ní se v posledních deseti letech ukázalo, jak zranitelné jsou počítačové sítě a jak škodlivý může být útok. Přitom jsou zatím tyto tzv. incidenty častěji charakterizovány jako činy počítačové kriminality, špionáže, nebo jako protest proti něčemu (viz ACTA – pozn. autora), než – kyberterorismus.
A připomíná několik destruktivních (už poměrně známých) DDoS útoků, jako byl ruský útok na Estonsko v r. 2007, na Gruzii v r. 2008 v období války o Jiží Osetii a také hacktivistické útoky skupin Anonymous či LuzSec. (Pozn. autora: Nešlo vlastně už v Gruzii o ukázku cyberware?)
Kybernetické útoky mají (nejen podle D. E. Denningové) jen zřídkakdy za cíl fyzické poškození či zničení objektu či aparatur - i když existují výjimky, jako např. při incidentu, kdy mladí polští hackeři v roce 2008 rozvrátili elektronické řídicí systémy čtyř tramvají (pomocí upravených ovladačů na televizi) a zranili při následné havárii desítky osob.
Jako zatím nejpozoruhodnější příklad uvádí Denningová případ Stuxnet, červa, který se šíří prostřednictvím Microsoft Windows a cíleně napadal

SCADA systémy společnosti Siemens (viz napadení Íránských zařízení na výrobu obohaceného uranu), a varuje před obdobnými útoky na systémy zodpovědné za monitorování a kontrolu kritických infrastruktur, jako jsou rozvody elektrické energie, ropy a zemního plynu a vody. (info)

## Průmyslový vysavač dat

Kdeže ovšem ty časy Sutxnetu jsou! Tento worm („červ“), autonomní program schopný proniknout a ovládnout jiné systémy, měl celosvětový dopad - zasáhl, infikoval během roku 2009 odhadem 100 000 počítačů, z nichž většina – 60 procent – byla v Íránu.
Jeho cíle? Siemens S7-417 controller v íránském nukleárním centru Bushehr, a druhý, rovněž Siemens (S7-315), na íránské adrese Natanz, v centru Centrifuge operation. V poušti, více než 20 metrů pod povrchem v bezpečně zabetonovaném prostoru, kam hned tak nějaká bomba nepronikne, došlo v roce 2009 k snad nejznamenitějšímu aktu sabotáže v historii. Řekněme – do té doby!

Tvůrci tohoto malwaru jsou totiž nadále aktivní. Jeho bezprostředním nástupcem byla už též dobře známá hrozba označovaná jako DuQu. Na rozdíl od Stuxnetu není DuQu navržen za účelem sabotáže systémů řídících průmyslové procesy, ale především pro útoky na weby certifikačních autorit. Další cílem malwaru DuQu je špionáž – zejména krádeže duševního vlastnictví z informačních systémů průmyslových podniků (většina dat údajně putovala na servery do Číny). (info)
A abychom od tohoto tématu hned neutekli, zmiňme, že ruská softwarová firma Kaspersky Labs odhalila nedávno (viz ČTK 28. května 2012) mohutný počítačový útok dalšího červíka patrně ze stejné líhně, jehož účelem je sběr soukromých informací v zemích Blízkého východu včetně Izraele (zřejmě) a Íránu. Tento doslova špionážní virus Flame (Plamen) se šíří minimálně od srpna 2010, ale odhaduje se, že řádí už od března onoho roku. A že tak dlouho? Běžné antiviry jej totiž vůbec nebyly schopny zaznamenat!
Lidé od Kasperského označili Worm.Win32. Flame za "jednu z nekomplexnějších bezpečnostních hrozeb, jaká byla kdy odhalena.“ Zatímco dříve

odhalené viry měly paralyzovat jaderná zařízení v Íránu (Stuxnet) a sbírat citlivá data v průmyslových podnicích (DuQu), cílem viru Flame je shromáždit široké množství nejrůznějších soukromých, citlivých a tajných dat. Zástupce této ruské firmy Vitalij Kamluk uvedl, že na rozdíl od svých předchůdců Flame zřejmě nezpůsobuje žádné materiální škody.
"Jakmile je ale systém napaden, Flame spouští komplexní řadu operací včetně čmuchání v provozu sítě. Pořizuje snímky obrazovky (screenshots), zaznamenává zvukové konverzace (Skype), zachycuje pokyny přes klávesnici a tak dál," prohlásil Kamluk. Podle něj bylo zasaženo více než 6000 specifických cílů od jednotlivců přes podnikatelské subjekty a akademické instituce až po vládní systémy.
Podle Kamluka je virus natolik důmyslný, že za ním těžko mohou stát osamocení počítačoví piráti. Pravděpodobnější podle něj je, že ho sponzoruje nějaká vláda.
"V současnosti existují tři typy hráčů vyvíjejících viry a špionážní programy: hackeři, počítačoví zločinci a národní státy. Flame neslouží k tomu, aby bral z bankovních účtů peníze, také je odlišný od spíše

jednoduchých hackerských nástrojů a virů. Takže když vyloučíme počítačové zločince a hackery, docházíme k závěru, že je to nejpravděpodobněji třetí skupina," poznamenal ruský expert.
Profesor Alan Woodward z Univerzity v Surrey, britský počítačový odborník, označil Flame za „v podstatě průmyslový vysavač citlivých informací."
Cílem útoku se staly fyzické i právnické osoby v Íránu, Izraeli, Súdánu, Sýrii, Libanonu, Saúdské Arábii a Egyptě, což je snad v zásadě dalším důkazem, že útok organizuje nějaký stát.

## Hra teprve začíná

"Obávám se, že ta hra teprve začala," řekl sám šéf společnosti Jevgenij Kasperskij v Tel Avivu 8. června na konferenci o počítačové bezpečnosti. A uvedl, že hrozí další podobné viry s mimořádně ničivým účinkem.
"Je logické, že vznikly další kybernetické zbraně, a je možné, že jsou napadeny i další počítače a že o tom ještě nevíme," prohlásil.
Dle Kasperského je Flame dvacetkrát účinnější než

Stuxnet, který byl použit před třemi lety proti systémům v íránských jaderných provozech (viz výše). Hovořilo se tehdy o útoku na státní úrovni a spekulovalo se o vině Izraele. Spojovat Izrael s novým červem Kasperskij sice odmítl, faktem ale je, že virus byl objeven měsíc potom, co Írán ohlásil, že musel kvůli virovému útoku zablokovat počítačové systémy ve svém ropném průmyslu...
Kaspersky ovšem upozornil na důležitou věc – že totiž virus s tak ničivou kapacitou nemusí být nutně vyvinut jenom v zemích s rozvinutou počítačovou technologií. Ovšem podle jeho odhadu přišel Flame autory na "nejméně 100 miliónů dolarů" (dvě miliardy korun), což téměř jednoznačně ukazuje na státem financovaný útok (víceméně se však koncem června potvrdily informace, že za zrodem Flame stály Izrael a Spojené státy).
„ Hrozba kybernetického válčení je jedním z nejzávažnějších témat na poli informační bezpečnosti v posledních letech. Viry Stuxnet a DuQu patřily do řetězce útoků, který zvýšil obavy z kybernetických válek po celém světě. Malware Flame se zdá být další fází této války a je důležité pochopit, že takové kybernetické zbraně mohou být snadno použity proti

kterékoliv zemi. Narozdíl od konvenční války jsou v těchto případech nejzranitelnější rozvinutější země," řekl m.j. Kaspersky. (info)

Přesto podle toho, co Jevgenij Kasperský prohlásil v Izraeli, v tomto případě nejde o kybernetickou válku, ale o kybernetický terorismus. Vypadá to, že si občas poněkud protiřečí...

Skuteční počítačoví zločinci (či státem podporovaní „hackeři") se dnes už nezajímají ani tak o informace na bankovních účtech nebo platebních kartách. Trh s těmito údaji je už dostatečně nasycený a ceny, za které lze tyto údaje prodávat, nízké. A tak se na současném černém trhu výborně prodávají především státní tajemství, zdrojové kódy softwaru, databáze softwarových chyb, archivy firemních důvěrných e-mailů, znění právních smluv, technická dokumentace k výrobkům nebo údaje o konfiguraci systémů SCADA (aplikace pro řízení průmyslových procesů). A stále více se zvětšuje pomyslný otazník – je to stále ještě „pouhá" kyberkriminalita, nebo už kyberteror? A není toto či ono už vlastně válečným aktem? Pravda, kdyby na íránský Bushehr spadla bomba, za válečný akt by se to jistě považovalo.

Jak je vidět, náš liberální svět se brání tomu si

přiznat, že se zločinci a extremismem v kyberprostoru jsme už dávno ve válečném stavu. Za co např. označit další nedávnou obrovskou krádež dat – viz případ LinkedIn ze 6. června? Jde o více než šest miliónů přístupových hesel k uživatelským účtům na této sociální síti!
LinkedIn má na celém světě 161 miliónů členů a loni své akcie uvedla na burzu. Zaměřuje se na lidi, kteří hledají kvalifikovanou práci, a vychází vstříc poptávce firem po zaměstnancích. Má tedy dosti cenné údaje. Následně se stejné skupině hackerů se podařilo získat přístupová hesla k některým uživatelským účtům z populárního hudebního webu Last.fm, což nejspíše souvisí s únikem miliónů hesel ze jmenované sítě LinkedIn. Jistě, může to být považováno za pouhý kyberkriminální čin.
Ukázkou dalšího dobře organizovaného útoku je zneužití 200 serverů na území ČR neznámou hackerskou skupinou k napadení vybraných cílů metodou DDoS v Lotyšsku z 11. června (2012). Vůči jakému konkrétnímu subjektu byl útok veden, počítačoví experti s ohledem na probíhající vyšetřování do doby napsání této statě neupřesnili. Jaká byla reakce ČR? Od lotyšských expertů šla

první informace o útoku na český IT security tým CSIRT (Computer Security Incident Response Team), který řeší bezpečnostní incidenty v počítačových sítích provozovaných v České republice.
A výsledek „obranných“ kroků? Poznání, že ovládnout takové množství serverů se hackerům údajně podařilo díky jejich špatné konfiguraci. A ti jich mohli využit k útoku typu DNS Amplification attack. Pracovníci CSIRT zpracovali údaje poskytnuté Lotyšským týmem a předali je dál správcům jednotlivých zneužitých DNS serverů. Jak se ale ukázalo, útok na Lotyšsko odhalil jen špičkou ledovce. Zneužít takové množství serverů (především těch, které jsou provozovány na routerech Mikrotik) se totiž útočníkům podařilo i přesto, že sdružení CZ.NIC, které je správcem české národní domény a zároveň provozovatelem týmu CSIRT, před špatnou konfigurací řady serverů u nás už dříve varovalo. Ovšem, pokud administrátoři nastavení opět nezmění, mohou se podobné útoky kdykoliv opakovat, podobně jako v případě webu ministra M. Kalouska. Tomu, lépe řečeno jeho

webmastrovi pak nechali vzkaz: „Opravdu oceňujeme jaký je na vás spoleh. Zcela dle našich předpokladů jste úplně zbytečně vynaložili úsilí na opravu stránky, ale nějak jste opomněli zlepšit zabezpečení... Jaký to má smysl, když jste nezměnili přihlašovací údaje a neopravili chyby, které jsme využili při prvním útoku.“
Podobného poděkování se však většina správců nabouraných stránek či serverů nedočká.

## Mediální a reálný kyberteror

Zatím nejmarkantnějším projevem kyberterorismu je – jak je vidět – tzv. mediální terorismus. Jde jednak o extrémisticky zaměřené internetové noviny a časopisy, či mediální nátlak určité skupiny lidí (viz tzv. ekoterorismus, zneužívající často demokratické principů řešení sporů, včetně tzv. procesního terorismu), ale i haktivistický spam atd. To se však postupně mění a mediální kyberteror v sobě skrývá latentní útočnost v reálném světě, kde kyberprostor je jen prostředím, útok umožňujícím.
Projekce obecných hrozeb do kyberprostoru je pak

doprovázena skutečností, že společnost jej stále neakceptovala jako součást svého životního (byť virtuálního) prostoru a moderní technologie pak často negativně ovlivňuje nepřipravenou společnost. Lze tedy obecně zasadit kyberterorismus do prostředí terorismu jako takového? Graficky se to pokusil vyjádřit ve své přednášce doc. V. Jirovský už v r. 2006 (viz obr. vpravo).
Dnes, po téměř šesti letech by tento graf vypadal zřejmě jinak – černá plocha kyberterorismu by byla jistě mnohem větší. Nicméně lokace kyberterorismu v celkové „aktivní zóně“ terorismu zůstává platnou. Jen se do ní přelévá více aktivit.

## Dělení kyberterorismu

Podle zaměření a působnosti lze kyberterorismus dělit na dva směry: První směr je čistě propagandistický a inklinuje k negativní či odmítavé reakci na aktuální stav mezinárodní či národní politické situace (propagace jednotlivých extremistických či teroristických skupin, propagace ideologií, náboženství apod.).

Druhý směr ovšem realizuje přímá napadení konkrétních informačních sítí a likvidace síťových služeb a je tudíž výrazně nebezpečnější. Z hlediska informační nadvlády je to maximální informační výhra - nejsou-li informace, bude protivník dezorientovaný a nebude schopen reagovat na souběžné útoky na různá místa.
Tyto útoky lze ovšem rozdělit alespoň rozdělit do tří úrovní:

- **řízení sympatizantů** a podobných lidských „zdrojů“ – teroristická skupina využívá informačních technologií k řízení svých lidí, rozptýlených po celém světě pro předávání úkolů a reportů mezi jednotlivými členy skupiny.
- **lokální kyberútok** – samostatný přímý útok na konkrétní technologii či službu. Nebezpečnost tohoto druhu útoku je závislá na zkušenostech, cílech a možnostech dané skupiny.
- **souběžný útok** – nejnebezpečnější varianta útoku, kdy dochází k několika paralelním útokům na konkrétní oblasti či cíle na různých úrovních. Kyberteroristický útok v této je fázi pouze jakousi přípravou pro napadení útočníka

nebo přímou podporou pro jeho dezorientaci a likvidaci, která může jít v přímé součinnosti s chystanými vojenskými akcemi, zejména v narušení funkcí jednotlivých prvků vládních a armádních institucí, sítě nebo služeb, které poskytují. (info)

## Kyberválečník a Politický aktivista

K nejnebezpečnějším typům kyberteroristů zřejmě patří kategorie specifikované jako Kyberválečník a Politický aktivista.
Kyberválečník je zpravidla profesionál, zabývající se primárně ochranou IT systémů před narušiteli, odborník s hlubokými technologickými znalostmi a často speciálním tréninkem, díky čemuž se stává velmi těžkým protivníkem a ideálním útočníkem. Motivace tohoto typu útočníků je buď ve vlastenectví nebo sounáležitost s náboženskou, sociální či jinou entitou (typicky názorově blízký ideologii teroristické skupiny). Typické útoky jsou vedeny za účelem destabilizace a poškození integrity dat či informačních systémů, především na úrovni kontroly

rozhodovacích procesů.
Politický aktivista je možná nejhorší druh útočníka. Většinou se jedná o znalce z oblasti IT, jehož snahou je skrze kyberprostor reagovat na aktuální politické dění. Často se jedná o fanatika nebo idealistu zastávající extrémní politické názory, za něž vášnivě bojuje. Ke svým útokům využívá plně svých znalostí z oblasti a tudíž pro dosažení politických cílů může využívat široké spektrum různorodých metod – od propagandistického defacementu po přímé napadení a likvidaci státních informačních systémů. Tady si opět připomeňme hacktivistmus skupin a´la Anonymus či LuzSec.
Otázkou, zejména dnes aktuální, zůstává, zda je vůbec správné Anonymous označit pouze za hackery, když jejich hacktivistické aktivity přitáhly pozornost tisíců lidí po celém světě, kteří se (dobrovolně) zapojili do veřejných protestních akcí, častokrát spoluorganizovaných či podporovaných hnutím Anonymous? O kom všem se dá prohlásit, že patří k Anonymous, kdo všechno je členem, když Anonymous videa rozesetá po YouTube i na dalších místech deklarují, že „Anonymous je nikdo a každý?“ Jejich poselství z posledních let je v prosté informaci

– změna je možná a je potřeba se o ni snažit.
Okamžité svolání davu („flash mob“) se ukázalo jako efektivní zbraň v boji proti jakémukoliv režimu, což obyčejní občané zdá se pochopili mnohem dříve, než např. vládnoucí struktury v arabských zemích v průběhu tzv. „Arabského jara“.
Nicméně řada jejich akcí může být jako teroristický čin chápana. Viz např.:

- Operace „Payback“, (2010): Jedna z nejznámějších akcí Anonymous spuštěná na podporu Wikileaks. Skupina v prosinci podnikla tzv. DDoS útoky na webové stránky bank, které zmrazily konta WikiLeaks a další cíle (více o operaci „Payback“).
- Útok na Fine Gael, (2011): Během volební kampaně v Irsku napadli Anonymous stránky vládní strany Fine Gael a nahradili je svým vlastním provokativním projevem.
- Jarní arabské revoluce, (2011): Anonymous se podíleli na podporování a svolávání protestů v Tunisku, Egyptě a Libyi (menší mírou i v Jordánsku a dalších arabských státech, do kterých revoluční vlna dorazila později), také

prováděli řadu DDoS útoků na vládní a policejní weby zmíněných států. Podporují i opozici v Sýrii.
- Operace „AntiSec“, (od června 2011): Společně se skupinou LulzSec (viz Jake Davis, Shetleand Islands) spustili Anonymous operaci „AntiSec“, která má být tažením proti jakýmkoliv vládním webům (více zde).

O aktivitách Anonymus a jejich příznivců v souvislosti s úmluvou ACTA už ani nemluvě (viz 1. díl seriálu).

## Reálná rizika

V běžném životě – a aktivity Anonymus jsou toho příkladem – některé typy útoků splývají a některé se mohou dále detailněji členit, což ovšem podléhá i času.
Můžeme tak uvažovat nad tím, zda např. defacement webových stránek je jen kriminálním činem, nebo už kyberterostickým útokem. Jsou některé islamistické weby navádějící k výrobě bomb a´la „vyrob si bombu v mámině kuchyni…“ teroristickým aktem, nebo až samotný výbuch bomby?

Jana Hybášková, exposlankyně Evropského parlamentu (m.j. známá arabistka) ve svém vystoupení na konferenci CYTER 2009 pod názvem „Radikální islám na internetu: Kde začíná a končí nebezpečí," velmi pregnantně definovala metodiku ideologického působení na islámskou populaci. A to už od dětství, kdy v zásadě nenápadně začíná na síti výchova k sebeobětování ve jménu islámu a likvidace „nevěřících" často pomocí otřesných teroristických činů. Na takovýchto webech pak nejsou výjimkou ani návody na výrobu třaskavin a jejich použití, ale také videa s ukázkami brutálních vražd např. podřezáním.
Hybášková rovněž upozornila na liknavost a nejednotnost Evropy v přístupu k těmto militantním stránkám, proti kterým se lze zatím bránit jen odpojením jejich IP adres providery. V podstatě tak definovala nemohoucnost západního tzv. liberálního světa v boji proti militantnímu islámu (a nejen islámu) na internetu.
Ptejme se tedy: Kdy vlastně terorismus přerůstá v kybernetickou válku? Až v momentě, kdy si podle návodu na internetu doma v garáži někdo vyrobí atomovou bombu? (Ale je to pak kybernetická

válka? Vždyť je vlastně reálná a internet je zde prostě jen jedním z prostředků.)
Nicméně podle docenta V. Jirovského (FD ČVUT, www.Cyter.cz) v současné době spočívá největší nebezpečí kyberterorismu v nově vznikajících hrozbách. Jde především o ohrožení už citovaných SCADA systémů, což jsou systémy pro řízení výrobních procesů, energetické sítě, ropovody, železnice apod. Není to tak dlouho, co byl podniknut útok na řídicí systém dálnic v Německu, před už časem byl podniknut útok na SCADA systém atomové elektrárny v Ohiu, či energetickou síť města New Orleans, o „íránském“ případu s červem Stuxnet už ani nemluvě.
Vyvstává ovšem reálné nebezpečí, že budoucí útoky postupně smažou rozdíly mezi kybernalitou a kyberterorem a bude jen záležet na chápání incidentu.
Tato fakta právo (ani mezinárodní) zatím nebere na vědomí a pokud, tak jen z hlediska státního zájmu. Kyberterorismus a na něj potenciálně navazující kyberválečné akty proto vyvstávají jako nová hrozba, které je nutné čelit a dostatečně dobře se na ní

připravit – jak technologicky a personálně, tak především znalostně.

## Cyberwar už není Sci-Fi

Ne, ještě nepochodují po bitevních polích robotičtí vojáci. Zůstávají na displejích počítačových her. Zatím. Ještě se v kybernetických válkách nesčítají mrtví a ranění a v novinách se neobjevují fotografie ruin zasažených měst. Přesto jde o nesmírně nebezpečný způsob vedení boje, jehož výsledkem mohou být ochromené komunikační sítě protivníka, jeho tzv. kritická infrastruktura – dopravní tepny, energovody (voda, plyn, ropa) i elektrárny - včetně atomových. Bezpečnost napadené země je pak totálně nalomena i proto, že nepřítel např. zneužije vládní informační zdroje či média, pronikne do serverů jejích bezpečnostních složek vč. armádních apod. V kyberprostoru už nepanuje ničím nerušený klid a mír.
Kyberprostor se v současnosti mimo jiné stává novodobým bojištěm, kde musíte posilovat síťovou obranu, chránit zejména tzv. kritickou infrastrukturu a

nevyhnutelně spolupracovat s (důvěryhodnými) spojenci. Kybernetická válka 21. století je ale – bohužel – vnímána spíše jako určitá forma hry na válku na internetu, v rámci zlobivých počítačových hackerů, čímž je strategická obrana na síti zcela zbytečná. Bohužel, takto toto nebezpečí vidí i řada vrcholových politiků – a nejen u nás. Realita je prostě jiná. Jde v zásadě o válku informační, jejímž cílem je získání a zneužití informací. Ovšem pozor: Už nejde o vybílení vašeho bankovního konta. Jejím cílem může být i ochromení elektronických, obranných (útočných) vojenských systémů, samozřejmě pak vládních úřadů (což se daří velmi jednoduše i u nás) a dalších civilizačních prvků, jako jsou rozvodné sítě v energetice, doprava, zdravotnické systémy, útoky proti mobilním zařízením nebo počítačovým cloudům a také tzv. zahlcení kyberprostoru.
Toto jsou slova Richarda Clarka, muže, který měl ještě nedávno v Bílém domě ve Washingtonu na starosti boj s terorismem. „Při promyšleně vedeném kyberútoku postačí na vyřazení protivníka patnáct minut.“ A je to tady - patnáctiminutová bitva. Vítězství bez výstřelu. O tom si doposud plánovači konvenčních operací v genštábech mohli nechat jen

zdát.
Jistě, mnohé státy masivně zbrojí. Ale místo do tanků, raket a dalších palných zbraní dnes investují velké sumy do počítačové techniky a softwaru. V čele kyberpeletonu jsou USA, Izrael, Rusko, Velká Británie a – Čína.
Cvičení proti simulovanému masivnímu útoku nedávno absolvovaly i země Evropské unie. Posílení vlastních kapacit kybernetické obrany v horizontu této dekády je také jeden ze základních strategických cílů zemí NATO. Státy se na tom dohodly na nedávném summitu v Lisabonu. Varovná slova generálního tajemníka NATO Anders Fogh Rasmussena o otm, že takový útok může být velice devastující, nelze brát na lehkou váhu Napadený stát či společnost může podle něj utrpět velké škody. Možná se plavíme na Titaniku a nevíme, kde na nás čeká ledovec.

## Útoky na SCADA

Z tohoto hlediska zůstávají nejnebezpečnější tzv. SCADA (Supervisory Control and Data Acquisition)

útoky (čtěte: útoky na SCADA systémy), které by dokázaly ochromit ekonomiku a bojeschopnost i velkého státu, natož ČR. Stačí jen představit si, jak by asi dopadly vojenské i civilní komunikace, pokud by útočníci např. dokázali ochromit či vyřadit z provozu družicové komunikační systémy, včetně sítě GPS. A co by se asi dělo ve chvíli, kdyby útočníci ovládli řídící systém takové jaderné elektrárny, jako je např. Temelín? Nemožné?
Už se stalo. Pravda, je to už pár let, kdy se hackeři pokusili prolomit obranu americké atomové elektrárny v Ohiu. Na jejích firewallech si sice vylámali zuby, ale skulinku přeci jen našli. Podle doc. Václava Jirovského (fakulta dopravní ČVUT), který o tomto případu referoval na jedné z nedávných konferencí o kybernetické zločinnosti CYTER, využili zapomenuté telefonní linky, kterou si společnost, jenž elektrárnu stavěla, poloilegálně natáhla pro svoje interní potřeby. A hle, ještě po letech posloužila útoku, který málem uvedl reaktory do varu, podobně jako se stalo v Černobylu chybnou obsluhou. Hackeři mj. pronikli i do energetického systému USA. Podle expertů došlo k tzv. mapování tohoto systému, a proto by nemuselo být obtížné způsobit i

výpadek celé energetické sítě. Cílem útoku pravděpodobně bylo zjistit, jak systémy fungují a kdo všechno je na ně napojený. Podle světových agentur mohla by být ve hře i průmyslová špionáž – údajně se jednalo o akci objednanou z Číny či Ruska.

## Varovné signály

„Nechci o tom mluvit, ani na to myslet. Ale jsme velmi blízko kyberterorismu a kyberválkám. Možná už internetoví zločinci prodali své služby teroristům," prohlásil ruský odborník Eugene Kaspersky loni v listopadu na londýnské konferenci o kybernetické bezpečnosti. „Známe už kyberšpionáž, kyberzločiny a případy kyberútoků politických aktivistů. Brzy budeme čelit i státem řízenému kyberterorismu. To už je na pomezí toho, čemu říkáme cyberwar,"dodal. V loňském říjnu např. vyšlo najevo, že evropské firmy působící v oboru jaderného strojírenství a jiných klíčových odvětvích, se v předchozích měsících staly terčem útoku počítačového viru zvaného DuQu, shromažďujícího velmi citlivá data.
Následně pak byly zveřejněny detaily o počítačovém

programu NITRO, určeném k narušení počítačových sítí chemických (výbušniny) a jiných společností (zbrojovky) pracujících pro ministerstva obrany v USA, Británii a Bangladéši. Podobné ataky se stávají stále častějšími, a proto se mnozí odborníci domnívají, že brzy zasáhnou i klíčové státní infrastruktury.

Potvrzuje to i lednová studie McAfee Labs Hrozby roku 2012. Demonstrace kybernetické války a hacktivismus, to je to, co nás podle ní čeká. Studie předpovídá, „…že významně porostou politicky motivované útoky (už se stalo), demonstrace kybernetické války (viz. např. útok prostřednictvím českých serverů na Lotyšsko) a vysoce cílené útoky na firmy fungující v určitém oboru (viz Flame).“

A opět se objevuje varování, že se kyberzločinci více zaměří na systémy rozvodných sítí, na nichž v každodenním životě závisí velké množství lidí (např. elektřina, plyn), ale často jsou vzhledem ke svému významu nedostatečně zabezpečeny. To se týká – jak už bylo uvedeno – zejména řídicích systémů těchto provozů (SCADA) – a nedivme se – i v ČR. Hlavním cílem „ukázkových akcí“ v oblasti cyberwar

bude podle McAfee Labs (zatím) spíše testování možností těchto útoků. Až dosud vlády vyspělých zemí chránily především své vládní a vojenské sítě. Dnes si musejí uvědomit i míru škod, které mohou způsobit akce proti tzv. kritické infrastruktuře (viz výše).

## Kyberteror přerůstá v kybernetickou válku

Agrese ve formě kybernetického útoku se stále ještě nepovažují za napadení v pravém slova smyslu, nanejvýš za kyberteroristický akt. Ostatně tak charakterizoval i Eugen Kaspersky situaci po napadení zemí Středního východu červem Flame. Jenomže – můžeme se opětovně ptát, zda už útok na Estonsko v roce 2007 (vyřadil webové stránky významných státních institucí, parlamentu a ministerstev, ale i zpravodajských serverů či bank) byl válečným aktem, nebo jen kybernetickým terorem a tak pořád dokola, přesné definice totiž neexistují. Jsou známy případy, kdy byly ve Spojených státech napadeny stránky či servery ministerstva financí, dopravy, ministerstva vnitřní bezpečnosti, tajné

služby USA (Secret Service) a Federální obchodní komise. V Jižní Koreji pak weby ministerstva obrany, parlamentu i úřadu prezidenta, ale také bank a médií. Je to pořád ještě „jen“ terorismus? (A lze to označit za terorismus? Vyvolává to strach?) Problémem tak zůstává neexistence přesných pravidel – je téměř nemožné určit, kdy jde o politickou reakci, a kdy už je oprávněná hrozba vojenské akce.

Pokud jde např. o případ „FLAME“, už 21. června 2012 list The Washington Post napsal, že tento počítačový virus, namířený především proti Íránu, společně vyvinuly Spojené státy a Izrael. Americký deník to uvedl s odvoláním na nejmenované západní činitele, kteří tak potvrdili předchozí spekulace. Program údajně mapoval a sledoval íránské počítačové sítě a odesílal svým tvůrcům informace, na jejichž základě lze plánovat další kybernetické útoky.

Jde tedy o počátky cyberwar mezi Izraelem a Íránem? Možná to je jen vrchol ledovce, o řadě dalších případů zřejmě zatím nevíme, protože i Flame byl vlastně časovanou bombou. Víme jen, že potichu pracoval neodhalen více než rok.

Že první salvou v novém druhu válečného střetu, aniž by došlo ke krveprolití, byl už Stuxnet, tvrdí mj. i Eric Chien, technický ředitel společnosti Symantec se specializací na bezpečnost sítí. Stuxnet totiž předvedl in natura, jak by budoucí válka mohla vypadat, a že útoky z virtuálního světa mohou způsobit velké reálné škody ve světě skutečném. Navíc - cílem příštího útoku už nemusí být íránská odstředivka od Siemensu, ale třeba nukleární reaktor, virem a´la Stuxnet úspěšně roztavený. Podle The Washington Post jsou nové informace o viru Flame dokladem první vytrvalé kampaně kybernetických sabotáží Spojených států, namířených proti jejich protivníkovi. "Jde o přípravu bitevního pole na další typ tajné akce," řekl podle ČTK deníku bývalý vysoce postavený americký zpravodajec. Dodal, že jak Flame, tak Stuxnet, jsou součástí širší ofenzivy, která stále pokračuje. Nicméně pak list dodává, že „ …v tomto konkrétním případě šlo o jednostrannou operaci Izraele, která jeho americké spojence zaskočila.“

## Válka na Síti sítí

Na loňské mezinárodní konferenci o kybernalitě – CYTER 2011 - vystoupil mimo jiné i Jan Machník ze společnosti PCS/McAfee. A zabýval se ve své přednášce právě kybernetickou válkou.

„Může se stát, že vláda jedné země s cílem zmást napadeného, využije počítačových odborníků z jiné země (viz opět případ Lotyšska a českých serverů) k dosažení svých politických záměrů. Některé kybernetické útoky (viz příklad z období konfliktu Gruzie s Ruskem o Jižní Osetii), mohou být prováděny civilisty, čímž se charakter kybernetického konfliktu komplikuje," uvedl mj. ve své přednášce Machník.

Podle něj už pět mocností aktivně rozvíjí své schopnosti pro boj v případě kybernetické války. Patří k nim Spojené státy, Rusko, Francie, Čína a Izrael. Další státy jsou do těchto aktivit zapojeny částečně, přičemž jednotlivé národy vedou v kybernetickém zbrojení konkurenční boj. Jsou také ochotné kybernetické zbraně použít, což vede k politickému nepřátelství.

„Kybernetická válka je ovlivňována mnoha způsoby i aktéry natolik, že jejich řešení a určení viníků bývá

velice složitou a někdy i neřešitelnou otázkou. Agrese ve formě kybernetického útoku se stále ještě nepovažují za napadení v pravém slova smyslu. Klasický vojenský útok by vyvolal mezinárodní skandál a byl pravděpodobně příčinou odvety, elektronický útok by mohl zapadnout do ztracena, už proto, že státní účast na něm lze snadno popřít a prokázat ji je obtížné. A na vyšetření podobné události nemusí mít dotyčný stát dostupné prostředky," konstatoval Machník.

Kybernetická válka není snadno definovatelná - odborníci vyhodnocují její čtyři klíčové atributy: zdroj útoku, následek, motivace, sofistikovanost. Podle Machníka lze dnes z tohoto zorného úhlu pohledu spolehlivě určit některé klasické případy. Například do této oblasti patřila „Operace Aurora“, kdy došlo k útokům čínských hackerů na internetový vyhledávač Google a jeho službu Gmail. Obdobně „Titan Rain“ byl útokem čínských hackerů, zaměřeným na získání informací ze zdrojů americké armády. V době bojů s Gruzií o Jižní Osetii útok vedený z území Ruské federace, zlikvidoval řadu důležitých gruzínských vládních serverů.

Proto je podle něj nebezpečný i tzv. defacement, kdy

je měněn obsah oficiálních stránek firem či státu, což může v některých případech vyvolat paniku u obyvatelstva.
Vojenské konflikty tak mohou ztratit svůj konvenční rozměr a stanou se nekonvenčními válkami, v nichž ani nebude nutné, aby jedna či druhá strana použila klasických „horkých“ zbraní. Naopak: K likvidaci protivníkova státu bude stačit poměrně malá, vysoce specializovaná skupina, která provede několik útoků na kritickou informační strukturu daného státu (banky, pojišťovny, komunikační sítě, informační systémy národní působnosti, informační systémy státní správy, databáze (např. obyvatelstva), systémy řízení podniků, systémy dodávky energií, rozvodné sítě apod.). Výsledek? Destabilizace a případná likvidace státu zevnitř. Někdy by k vyvolání chaosu stačilo vyvolat zmatek např. v dopravě.
Ostatně, není to tak dlouho (r. 2010), co byl podniknut útok na řídicí systém dálnic v Německu, či energetickou síť města New Orleans.

## Hackeři a diplomatické konflikty

Hackeři stále častěji zasahují do ozbrojených a diplomatických konfliktů, které se týkají jejich národa. Vrátíme-li se opět k Rusku, stojí za zmínku třeba případ z roku 2002, kdy tamní FSB (Federalnaya Sluzhba Bezopasnosti) zaznamenala aktivitu jisté skupiny z Tomska, která vedla soukromou elektronickou válku proti rebelům v Čečensku. O případech „Gruzie“ a „Estonsko“ jsme se už opakovaně zmínili.

Během loňských leteckých útoků NATO proti Kadáfího režimu v Libii prý USA uvažovaly o napadení kybersystémů libyjské protivzdušné obrany. Akce se ale nekonala z obavy, aby nevznikl precedent a podobně pak nezačaly otevřeně postupovat i jiné země (Rusko, Čína). Nikdo si také nebyl jistý, zda má prezident Spojených států pravomoc kybernetické útoky nařídit bez toho, aby o svém postupu informoval Kongres.

Při likvidaci superteroristy Bin Ladina se mj. uvažovalo o „menší akci,“ která by zaslepila pákistánské radary. Protentokrát bylo od tohoto postupu proti nespolehlivému „spojenci“ upuštěno, ale i díky tomu se v USA začalo otevřeně diskutovat o tom, nakolik má být kybernetický útok pokládán za

válečný akt. (Zdroj: New York Times)
Na druhé straně hrozí jakési útoky proti zbraňovým systémům takříkajíc zevnitř. Jde o případ malware, který pronikl do počítačů USAF, které mají na starosti řízení bezpilotních letounů Predator a Reaper, stále častěji nasazovaných v Afganistánu. Přes veškerou snahu se údajně ony škodlivé kódy nepodařilo zcela vyhubit, přičemž už tyto letouny opět létají do akcí. (Nedivme se pak, že jeden z letounů, nepoškozený, získal Írán.)
Spekuluje se proto, že malware byl přítomen už na nějakém pevném disku nebo jiné komponentě, možná už během „výroby“, později připojené do vojenské sítě. V této souvislosti se nyní diskutují (konenčně) i obecná rizika pro vojenské systémy, používající součástky (vč. čipů) vyrobené v cizích zemích (Zdroj: The Register 10.10. 2011), především firmami z východní Asie a Číny (což se kupodivu týká právě zbraňových systémů USA, do kterých byly např. zakoupeny – v rámci úspor – repasované čipy z Číny).
Obětí útočníků na pomezí válečného kyberútoku se stala i další firma pracující s citlivými informacemi – japonský armádní dodavatel Mitsubishi Heavy

Industries. Vytěženy byly např. počítače a servery v závodě na výrobu ponorek nebo raketových motorů. Armádní dodavatelé jsou pro zloděje dat přirozeně lákavým cílem, loni v květnu se obětí staly např. i americké firmy Lockheed Martin a L-3 Communications. (Zdroj: CNet, říjen 2011)

## Cyber Commandos

Spojené státy jsou však už velmi blízko tomu, aby kybernetické útoky podobného druhu klasifikovaly stejně, jako klasické válečné činy. Právě útok na Lockheed Martin, jednoho z největších dodavatelů letadel a raketových střel pro americkou armádu a letectvo, byl možná posledním podnětem k rozhodnutí reagovat na podobné akce buď ekonomickými sankcemi, nebo přímo odvetným vojenským útokem.
Do budoucna mají být podobné útoky na americké vládní systémy či zbrojovky hodnoceny jednoznačně jako válečný akt.
Podle zprávy ČTK ze dne 22. června (2011) by jako útok proti Spojeným státům mohly být hodnoceny i

nejzávažnější formy kyberútoku, které by ohrozily americké civilisty, například odpojením dodávek energie. Zatím ale není jasné, jakým způsobem by USA reagovaly, pokud by původcem útoku byla například skupina teroristů a nikoliv konkrétní stát (zas ta nejistota). Navíc otázka zní – stála by za to „horká“ válka s Ruskem či Čínou?

Nicméně je Obamův výnos (viz vložený text) vyvrcholením dvouletého úsilí amerického ministerstva obrany vnést pořádek do využívání kybernetické "munice". Přichází zároveň v době, kdy USA začínají pracovat se svými spojenci na globálních pravidlech vedení kybernetických válek. Podle agentury AP jsou regule blízké pravidlům, která platí pro klasickou válečnou munici - od nasazení jaderných bomb až po elektronické sledování nepřítele.

Pentagon chce také mnohem aktivněji chránit počítačové sítě výrobců zbraní, kteří disponují citlivými údaji o amerických zbrojních zakázkách. Ministerstvo obrany už pokusně sdílí s několika firmami citlivá data o možném ohrožení, aby jim umožnilo bránit se případným útokům. Partnery Pentagonu mohou v budoucnu být i elektrárny,

rozvodné sítě nebo finanční instituce.
Americká armáda, která je v současnosti na technologické špičce, loni založila zvláštní jednotku, tzv. United States Cyber Command (USCYBERCOM) a intenzivně se zabývá možnostmi elektronického vedení boje. Formálně spadá pod ministerstvo obrany, ale zřejmě má „klíč“ od použití prezident, podobně jako existuje „atomový“ kufřík. Cílem Cyber Command je především ochrana americké vojenské počítačové sítě a v případě potřeby i útoky na nepřátelské systémy. Spojené státy v tom ale nezůstávají osamoceny.
Rovněž Velká Británie už má svoji vlastní kyberpolicii spadající pod Národní bezpečnostní agenturu a týmy na způsob Cyber Command.
Na nové formy boje se připravuje i Německo. Bundeswehr disponuje jednotkami, které se místo pořadových cvičení učí „klikat“ myší a zadávat správné povely do klávesnice. Loni bylo v novém programu vyčleněno 76 absolventů tamních univerzit, kteří se pod vedením brigádního generála Fredericka Williama Kriesela zapojí do elektronického boje v kyberprostoru proti pirátům, kteří by mohli ohrozit německou infrastrukturu

podobným způsobem, jako se to před lety stalo v případě Estonska a nedávno Lotyšska.
U nás sice před dvěma lety vzniknul při ministerstvu vnitra odbor kybernetické bezpečnosti, ale po odchodu jeho prvního ředitele, ing. Aleš Špidly, o něm či o jeho činnosti není ani slyšet.

## Simulovaná kyberválka

Ano, i Evropa se snaží. Např. v listopadu 2011 prodělala simulovanou kyberválku.
Jejím cílem bylo prověřit důvěryhodnost a bezpečnost on-line služeb v Evropě. Země sedmadvacítky společně s Islandem, Norskem a Švýcarskem podnikly toto cvičení v prvním listopadovém týdnu (2011). Na cvičení mají navázat v budoucnu podobné akce, které by měly být ještě složitější.
"Toto cvičení, které mělo prověřit připravenost Evropy v případě kybernetických hrozeb, představuje první významný krok ke spolupráci při boji proti potenciálnímu on-line ohrožení," komentovala cvičení komisařka Evropské komise odpovědná za digitální

agendu Neelie Kroesová (ČTK). Osobně ovšem pochybuji, že tato sedmdesátiletá dáma opravdu ví, o co jde.
Během této celoevropské simulace kybernetického útoku totiž měli odborníci z celé Evropy za úkol reagovat na pokusy o napadení nejdůležitějších on-line služeb v několika státech EU. Jak doplnil pro ČTK český bezpečnostní expert Radek Smolík, „… hlavním předmětem zájmu bylo simulování postupného výpadku infrastruktury internetu v komunikaci mezi státy a uvnitř některých států ve vztahu ke klíčovým sítím."

**Virtuální realita a právo**

Ano, útoky blížící se svou destrukcí reálné horké bojové akci se v kyberprostoru stávají – bohužel – realitou, stejně tak jako se jí stal kyberprostor, realitou, se kterou a ve které se musíme naučit žít. Bohužel jí ale chybí právní rámec. Právě proto je cyberwar nebezpečím pro budoucnost civilizace. Podle Václava Jirovského (Dopravní fakulta ČVUT, Ústav bezpečnostních technologií a inženýrství; viz

CYTER 2011) jsou globální závody ve zbrojení v kyberprostoru realitou. A právní odpovědnost je v zásadě velice proměnlivá, diskutabilní a leckdy i zcela neúčinná. Společným jmenovatelem uvedených negativ je globální povaha internetu (kyberprostoru) a jeho právně těžce regulované prostředí.
Je paradoxem moderních technologií, že nejcitlivějšími místy pro úder jsou technologicky nejvíce rozvinuté země. Nemylme se – v oblasti internetové infrastruktury mezi ně patří i ČR.
Mezi cíle, které jsou na pořadu zájmu potenciálního protivníka patří např.:

- armádní sítě
- vládní systémy a webové stránky vládních úřadů a agentur
- elektronické obchodování a finanční instituce
- telekomunikační firmy.

Proto se aktuální hrozby cyberwar 21. století soustředí na:

- řídící systémy (SCADA) a databáze – útoky na

nejnižší vrstvy (energetika, doprava ... smart grids, zdravotnické systémy .... cloud computing, psychologicky propracované útoky, zero-day útoky)
- útoky proti mobilním zařízením
- rozvoj specifických útoků ze strany států podporujících terorismus
- kreativní sociální inženýrství (virtuální osoby, umělá inteligence, zahlcení kyberprostoru).

Největší překážkou kybernetické obrany jsou váhání a nekompetentní rozhodnutí – kyberkutilství, vliv politických lobby. To vše může ohrozit další vývoj, a tím i kybernetickou bezpečnost.
Kyberprostor už sice nevyčistíme od lidského „smogu“, stejně jako jej nevyženeme z ovzduší. Kyberkriminalitě a kyberválkám, hraným na pozadí sítě sítí, zřejmě také nezabráníme. Je zde jen jedna – zdá se rozumná – cesta: vychovávat lidi k bezpečnému jednání na internetu.

## Právní mantinely

Otázkou bohužel je, kdo a kdy postaví nějaké právní

mantinely.
Renomovaný specialista na IT právo, JUDr. Martin Maisner, mi při odpovědi na otázku, kde lze hledat hranice mezi kybernetickou kriminalitou a kybernetickou válkou, po chvilce váhání mj. řekl: „Snad bychom se měli vrátit ke Clausewitzovi – když mluvíme o válce. Ale platí to – válka je pokračování politiky násilnými prostředky, byť jde o kyberprostor. Podle mne se kyberkriminalita a tzv. kybernetická válka (cyberwar) liší především tím, zda je nějak statutárně organizována, pokud za tím stojí politický záměr. Například – když USA vypnou třeba Maledivám v souvislosti s diplomatickým tlakem komunikační sítě včetně internetu, protože tam došlo k převratu, tak bych to nazval kybernetickou válkou. Jestliže se jedná o útok jednotlivce, aniž by to mělo nějaký mezinárodně právní, nebo organizační rámec, pak je to buď kyberkriminalita nebo kyberterorismus. Existují motivy různé, včetně duševní choroby.
Ale kyberterorismus, stejně jako terorismus klasický, vždy páchá násilí za nějakým politickým účelem, když chce něčeho dosáhnout – např. propuštění politických vězňů. V případě útoků, majících za cíl např. rozbití státního zřízení až po získání území a

podobně, pak lze hovořit o cyberwar…“
Jistě, definice zcela jasné, zda a kdy kybernetický terorismus dělá mezní krok do kybernetické války, se zatím nedopátráme. Záleží doposud na rozsahu jednotlivých útoků a v jejich chápání. Záleží na tom, který stát, která osobnost poprvé usoudí, že jde o válečný akt a vytvoří obranný precedens. Nebo budeme čekat, až se světem přežene přílivová vlna kolapsu sítě sítí? Zkuste si představit, co by se stalo, kdo a co všechno je dnes provázáno v kyberprostoru. Zhroutila by se naše vyspělá civilizace, tak, jak ji známe?
Nezbývá, než dát za pravdu James Lewisovi, kybernetickému expertu amerického Střediska pro strategická a mezinárodní studia. "Je to jiný svět, bomby už nepotřebujeme," řekl agentuře AP.

---

Loni v červnu podepsal prezident Spojených států Barack Obama výnos upravující pravidla kybernetických válek, které může americká armáda a tajné služby vést v zahraničí. Prezidentský dekret mj. stanoví, které operace musejí mít souhlas Bílého domu a které ne a jakými pravidly se mají řídit.

# Rozhovor: Aktuální trendy v oblasti bezpečnosti IT

Jaké jsou aktuální trendy v oblasti bezpečnosti IT? Mění se v poslední době nějak preference zákazníků - ať už v souvislosti s ekonomickou situací, nebo v návaznosti na technologický vývoj? I o tom je následující rozhovor s Alešem Pikorou, ředitelem divize DataGuard společnosti PCS.

**Jaké je postavení divize Dataguard v rámci společnosti PCS?**

DataGuard se na rozdíl od ostatních divizí věnuje především softwarové bezpečnosti dat a službám s tím souvisejícím – což je analýza bezpečnostního prostředí, návrhy řešení, implementace, komplexní podpora zákazníka. Mimo to poskytujeme interně správu ICT prostředků všem ostatním divizím i firmám PCS.

**Pozorujete ze strany zákazníků v poslední době nějakou výraznější změnu preferencí v oblasti zabezpečení IT?**

Většina zákazníků mnohem pečlivěji zvažuje každou

investici do IT, což se dotýká i oblasti bezpečnosti. Firmy v současné době často zvažují konsolidaci svých bezpečnostních řešení. Mnohem častěji také zaznamenáváme dotazy na cloudové služby a virtualizaci. Již delší dobu také cítíme tlak na zabezpečení mobilních zařízení, jako jsou smartphony a tablety, které v současné době zaznamenávají velký nárůst.

**Můžete nějak upřesnit, jaký podíl na obratu DataGuard představuje prodej produktů a jaký vlastní služby - a které konkrétně?**

V posledních dvou letech dosáhl podíl vlastních služeb na více než 20 % celkového obratu divize.

**Vašimi zákazníky jsou výlučně firmy, nebo i koncoví uživatelé?**

Některé produkty v našem portfoliu jsou vhodné i pro domácnosti, a proto se část zákazníků nachází i v této části trhu. Většina produktů a především služeb je však určena pro firemní zákazníky jakékoli velikosti od malých firem, přes SMB, až po Enterprise sektor.

**Jaké produkty/značky distribuujete "tradičně", o jaké jste rozšířili své portfolio v poslední**

**době?**

Nejdelší tradici v našem portfoliu mají produkty výrobců McAfee, Kaspersky a Eset. Naopak naprostou novinkou jsou produkty Fortinet, které jsme nedávno zařadili do svého portfolia, a především vlastní nový produkt DataGuard MailFilter. Služby, jako přidanou hodnotu k prodeji produktů, jsme našim zákazníkům nabízeli od samého vzniku DataGuardu, tedy od roku 1992. Naší strategií je budovat si pozici dodavatele služeb, jež jsou postaveny na spolehlivých technologických řešeních a nabídnout zákazníkům prvotřídní servis.

**Projevují vaši zákazníci zvýšený zájem o zabezpečení mobilních zařízení?**

Určitě ano, spolu se zvyšující se penetrací firemního prostředí těmito zařízeními stoupá i požadavek na jejich zabezpečení. Mnozí si začínají uvědomovat, že komfort mobilní kanceláře musí také následovat její odpovídající zabezpečení.

**Nejsou podle vás související rizika v současnosti trochu přeceňována?**

Nemyslím, že by tady bylo nějaké přeceňování bezpečnostní situace. Naopak se stále setkáváme s opačným problémem, tedy s podceňováním rizik – a

to právě v relativně nových oblastech, jako je třeba mobilní technologie.

**Dochází k nějakému posunu v útocích na mobilní zařízení/smartphony?**

V roce 2011 bylo dle dostupných údajů zaznamenáno zvýšení zranitelností o 93 %. Vzrostl i počet hrozeb cílených na stále populárnější systém Android. Tvůrci malwaru stále zdokonalují malware pro mobilní zařízení a zároveň vytváří i speciální škodlivé kódy.

**Jak se podle vašeho názoru firmy mají vypořádat s trendem BYOD (používání soukromých zařízení pro pracovní potřeby)? A jaká je v této oblasti prozatím realita?**

Realita je zatím taková, že většina firem nepřipouští použití soukromých prostředků pro pracovní potřeby, a to právě na základě bezpečnostních směrnic. Nalézt kompromisní řešení, uspokojující obě strany, je zatím velmi těžké a tak o jeho hledání raději většina ustoupí. Na druhou stranu tyto trendy sílí a mnohé firmy si jejich výhody uvědomují. Dle mého názoru však nelze ustoupit od nezbytných bezpečnostních zásad a pravidel na úkor pohodlí uživatele.

**Když se vrátíme k vašemu nejnovějšímu přírůstku. Co vás vedlo ke kroku zařadit do vašeho portfolia nabízených služeb právě cloudové řešení?**

Ať se na cloudové řešení díváte z jakéhokoli úhlu, tak vždycky nějakou výhodu najdete. Samozřejmě najdete i nevýhody, v našem případě je to především jistá nedůvěra v dostatečné zabezpečení komunikace. Je jen otázkou času, kdy budou technologie dokonalejší a zákazníci přesvědčenější, a systémy vzdálených poskytování služeb, dat, produktů, atd. bude běžnou součástí IT struktur. Chtěli jsme tento trend následovat, a v jistém ohledu tak získat výhodu před konkurencí, protože jsme nyní schopni uspokojit i tyto požadavky zákazníka.

**Na co by si firmy měly dávat pozor? Můžete stručně vysvětlit výhody či nevýhody cloud řešení?**

Firmám bych doporučil pečlivý výběr dodavatele i technologie. Na vlně popularity cloudu se chtějí svézt i mnozí méně kvalitní výrobci, což může celé myšlence cloudu jen uškodit. Proto předem otestujte nabízené řešení, seznamte se s úrovní podpory

dodavatele a využijte referenčních kontaktů.

**Co přináší Vaše řešení DataGuard MailFilter?**

DataGuard MailFilter je řešení pro firemní e-mailovou komunikaci. Jedná se o produkt nabízený formou služby. Jeho nasazení je velmi rychlé, veškerá komunikace probíhá přes bezpečnostní brány a je zašifrována. Navíc toto řešení nabízí oproti konkurenčním řešením vyšší stupeň zabezpečení, protože využívá několik antivirových a antispamových skenerů, ne pouze jeden. Zákazníci ani nemusí mít strach o své e-maily. V případě, že nasadí DataGuard MailFilter nejsou mail servery veřejně dostupné, takže nedojde k napadnutí z internetu. Navíc jsou veškerá data zálohována na několika serverech v různých zemích. Nemluvě o finančních úsporách.

*(Partnerský příspěvek.)*