EVROPSKÉ HODNOTY
Názory i souvislosti

Odborný podklad think-tanku Evropské hodnoty
2016-02-13

Kyberbezpečnost a veřejná politika

Vladimír Bízik

Spolupracovník Analytického týmu think-tanku Evropské hodnoty

Think-tank Evropské hodnoty je nevládní odborná instituce bránící liberální demokracii.

V současnosti se nacházíme v situaci, kdy se kyberbezpečnost stala neoddělitelnou součástí veřejné diskuse – ve sféře akademické to platí bezpochyby již delší dobu a nyní také v oblasti veřejné státní politiky. Kyberprostor je ve svém nejširším pojetí ideálním terčem pro hackery, zločince, teroristy i státní aktéry. Složky veřejné moci i větší soukromé společnosti prakticky nepřetržitě čelí pokusům o krádež citlivých dat, kybervandalismu či DDoS útokům (viz níže). Jako kyberprostor však nemůžeme chápat pouze počítače a internet v užším smyslu, jak se nám intuitivně obvykle vybaví, ale například i elektrickou síť konkrétního státu, bankovní systémy, systémy řízení letového provozu, telefonní komunikační sítě – takovéto systémy jsou často, ne však nevyhnutelně, s počítači v běžném pojetí propojené.

Bezpečnost v kyberprostoru začala být přirozeně relevantním pojmem v momentě, kdy kyberprostor vznikl. Pokud se jedná o internet, který je jako takový v „ostrém“ veřejném provozu asi dvě desetiletí, už od samotného počátku bylo očekávatelné, že se stane to, co se v historii stalo již mnohokrát: lidská civilizace dosáhla nových obzorů a její stinné stránky na sebe nenechaly dlouho čekat. Zpočátku byly tyto hrozby zanedbatelné a byly spíše tématem sci-fi. Například knižní série Net Force, jejímž duchovním otcem byl vlivný americký spisovatel Tom Clancy a která začala vycházet koncem devadesátých let, správně předpověděla, že velká část lidské činnosti se bude v blízké budoucnosti odehrávat v kyberprostoru, a tudíž se tam přesune i odpovídající část kriminality; na to i v Clancyho fiktivním světě musely reagovat vlády industrializovaných zemí a zřídit nejen veřejné kontrolní orgány bdící nad internetovou bezpečností, ale státy byly také nuceny přehodnotit společenské normy, mnohdy staletí staré. Co se týče první části, v současnosti se dá tvrdit, že na institucionální úrovni existují v relevantních státech kompetentní orgány, které kyberútokům dokáží čelit. Normativní realita je však, jak tomu v historii typicky bývá, v defenzivě a pouze s nešťastným opožděním reaguje na změněné podmínky světové reality. Namísto formulace nových pravidel pro nová odvětví lidské činnosti jsme pořád nuceni vystačit si s analogiemi situací, které zná právo jednotlivých zemí či ustálená zvyková pravidla mezinárodního společenství.

Nyní již závislost států, korporací a jednotlivců v industrializovaném světě na počítačích a internetu dosáhla a mnohdy předčila fiktivní světy umělců. Až přibližně v poslední dekádě tedy můžeme jasně sledovat trendy, které přivedly kyberbezpečnost do popředí pozornosti tvůrců politiky kupříkladu i do té míry, že je to dnes již téma, s nímž politici vstupují do kampaní (téma kyberbezpečnosti bylo probíráno například v předvolebním souboji Mitta Romneyho a Baracka Obamy ucházejícího se o křeslo podruhé). Některé státy (nutno zvlášť podtrhnout Estonsko) definují kyberbezpečnost jako dominantní prvek své velké strategie a přijímají za tímto účelem veškerá dostupná opatření. Ještě stále jsme však teprve v začátcích.

Než se dostaneme k popisu aktuálních trendů, dilemat a pokroků v kyberbezpečnosti, musíme si vymezit několik pojmů, se kterými budeme po zbytek textu rutinně operovat. Tento výčet nebude v žádném případě vyčerpávající, představí především ty koncepty, které laický čtenář nemusí znát, které je ale vzhledem k jejich významu důležité znát pro základní orientaci v v dané problematice.

Prvním důležitým pojmem je samotný **kyberprostor**. Ten je těžké definovat, protože existují nejrůznější oficiální definice či slovníková vymezení. Oxfordský slovník anglického jazyka definuje kyberprostor jako „prostor virtuální reality, pomyslný prostor, v jehož rámci probíhá elektronická

komunikace (zejména přes internet)“.[1] V každém případě však hovoříme o kyberprostoru, v případě, žese nejedná o fyzickou lokalitu – i když mnohé jeho aspekty mají fyzickou podstatu a hmotu (počítače, kabely, atd.). Kyberprostor zahrnuje také, nikoli však výlučně, internet – součástí kyberprostoru jsou i počítače a data v nich uložená a jiné počítačové sítě, které mohou, ale nemusí být s internetem spojené. Konečně, kyberprostor obsahuje nehmotné statky – informace, software, systémy propojení, atp. Kyberprostor tedy můžeme charakterizovat jako soubor předmětů založených nebo závislých na počítačích a komunikačních technologiích; informace, které tyto předměty používají, ukládají, zacházejí s nimi či zpracovávají; a propojení mezi těmito různými elementy.[2]

Pojmem, který se ke kyberprostoru úzce vážce, je pak samotná **kyberbezpečnost**. Ta vychází ze tří předpokladů. Za prvé: žijeme ve světě, který s námi sdílí aktéři chovající se nepřátelsky či nespolečensky – mohou nám ublížit nebo nás připravit o peníze, myšlenky či soukromí. Za druhé: spoléháme na informační technologie, které plní stále více funkcí ve společnosti. Za třetí: informační systémy, ať jsou zkonstruovány jakkoliv dobře (a mnohé vzhledem ke stavu vývoje technologií dobře zkonstruovány nejsou), mají zranitelná místa, která mohou potenciální útočníci zneužít. Bezpečnost v kyberprostoru (neboli kyberbezpečnost) můžeme tedy definovat jako veličinu týkající se technologií, procesů a opatření, které pomáhají předejít a/nebo minimalizovat negativní dopady událostí v kyberprostoru záměrně zapříčiněných aktéry se škodlivými úmysly.[3] Pojmy jako „škodlivý“, „útočník“ jsou však samy o sobě problematické a užíváme jich s tímto vědomím. Záleží na společenském kontextu a úhlu pohledu, kdo je útočníkem a kdo obětí. Podobně je to například u situací, kdy dochází k narušení soukromí. Žádné právo není absolutní a to platí i pro právo na soukromí. Jasné vnímání toho, kdo je útočníkem a kdo obětí, rozvrátila zejména kauza kolem Edwarda Snowdena a informací, které vynesl z americké NSA v roce 2013. Ty odstartovaly širokou (nikoli však dostatečně) společenskou diskusi o rovnováze mezi bezpečností a právem na soukromí a také o tom, že ne každý, kdo narušuje soukromí uživatelů internetu je útočníkem (nebo na druhé straně ne každý orgán veřejné moci je automaticky chráněn od označení škodlivého aktéra). Jako poslední poznámku je potřeba uvést, že kyberbezpečnost se nemusí nutně spojovat pouze s technologií. Jak uvidíme dále, kyberbezpečnost je propojená i s netechnologickými otázkami, jako je např. legislativa, bezpečnost, obrana a podobně.

Kyberkriminalitu nebo **kyberzločin** můžeme široce definovat jako použití internetu a informačních technologií pro krádež cenných statků. Zahrnuje mnoho činností jako například online podvody (krádež čísla kreditní karty, ať už prolomením bezpečnostních systémů, nebo oklamáním naivního uživatele internetu, tzv. phishing), kybernetická šikana (zneužití online anonymity pro pohrůžky či šikanu oběti), kybernetický vandalismus (prolomení přístupu k webovým stránkám a jejich změna, obvykle nelichotivá pro vlastníka webu), krádež identity (získání přihlašovacích údajů uživatele k webovým stránkám či službám, například bankovním, ať už prolomením databáze hesel, uhodnutím hesla nebo phishingem; krádež identity je mnohem větším problémem ve Spojených státech než u nás, protože v USA neexistují občanské průkazy jako unikátní a celoplošná forma identifikace obyvatele, proto získáním důvěryhodné identifikace může v zámoří pachatel vystupovat jako oběť i mimo kyberprostor; v ČR tomu pomáhá předcházet právě kontrola občanského průkazu a evidence obyvatel).[4]

Tímto se již dostáváme k definici nejčastějších metod kybernetické kriminality. Již zmiňovaný phishing je psychologickou metodou, jak od uživatelů počítačů vylákat citlivá data bez toho, aby byl

útočník nucen prolamovat bezpečnost počítačových systémů. Předmětem phishingu mohou být přihlašovací jména, hesla, čísla kreditních karet a jiné údaje (ve Spojených státech to mohou být například čísla bankovních účtů, která jsou tam na rozdíl od ČR považována za citlivý osobní údaj). Slovo phishing je anglický neologismus vycházející ze slova fishing, tedy rybaření – útočník používá návnadu, aby zmátl a podmanil si svou oběť. Touto návnadou je často například email, který se snaží vzbudit dojem, že je od správce systému žádajícího citlivé údaje pro ověření identity uživatele. Pachatel žádá o zaslání údajů buď přímo emailem, nebo nabízí odkaz na webové stránky, které jsou kopií legitimních stránek, která je od nich v některých případech téměř nerozeznatelná. Provozovatelé phishingu užívají nejrůznější psychologické taktiky, aby uživatele úspěšně nalákali a odfiltrovali ty, kteří jsou příliš pozorní (například frekvencí gramatických chyb – méně inteligentní či pozorní uživatelé si chyb nevšimnou a nevzbudí u nich podezření o legitimitě emailu; dá se očekávat, že si nevšimnou ani podvodného záměru odesílatele). Stránky, na něž podvodné zprávy odkazují, pak mohou obsahovat nejrůznější **malware** (škodlivý software), který může v konečném důsledku například zapojit napadený počítač do **botnetu** (viz níže). Jak software pro ochranu počítačů před internetovými hrozbami, tak i moderní verze operačních systémů a internetových prohlížečů mají již zpravidla integrovaný jistý druh detekce a upozorňování na phishing a falešné weby. Nejlepší obranou je však informovanost uživatelů internetu, kteří dokáží intuitivně odhalit zjevně falešné emaily, všímají si adres, na které jsou přesměrováni a zajímají se například o to, jestli internetový prohlížeč hlásí, že bankovní web, který navštívili, má platný a aktuální **bezpečnostní certifikát.** Uživatelská informovanost je spojena s počítačovou gramotností, která musí být ve společnosti kultivována systematicky a dlouhodobě. Cílem je, aby běžní uživatelé počítačů (kteří mohou být zároveň zaměstnanci veřejné správy, a tudíž pracují s citlivými údaji přesahujícími jejich osobní sféru) dokázali odlišit čestné jednání od nečestného v prostoru virtuální reality stejně jako v každodenním životě.

Jakýmsi protipólem phishingu jsou pak **brute force** útoky, čili útoky hrubou silou. Ty jsou charakterizovány mechanickým zkoušením všech možných matematických kombinací znaků. Lze si je představit jako výrobu všech možných tvarů klíčů, všech kombinací zoubků a tvarů – když takových klíčů vyrobíme dostatečné množství, jeden bude do zámku určitě pasovat. V reálném světě bychom pro takovýto pokus patrně neměli dostatek kovářů, a i kdybychom zaměstnali celou populaci Země, pro výrobu klíčů by na planetě nebyl ani dostatek kovů. Ve světě virtuálním nám však stačí výpočetní síla počítače, která narůstá s jeho výkonem. Počítač, který se snaží zjistit přístupové heslo, systematicky zkouší všechny matematické kombinace znaků. Čím je heslo delší, tím déle samozřejmě trvá jeho uhodnutí, přičemž tato délka nenarůstá lineárně, nýbrž exponenciálně (počet možných hesel není násoben, ale umocňován každým dalším znakem). Počet kombinací se dále může násobit, je-li potřeba uhodnout nejen heslo, ale i přístupové jméno. Data jsou pak často šifrována takzvanými **šifrovacími klíči**. To je sled znaků, který musí počítač znát, aby získal přístup k zašifrovaným datům, jinak budou nesrozumitelná. Šifrovací klíč je většinou charakterizován počtem **bitů**. Za tím se neskrývá nic složitého – bit je zkrátka znak a můžeme si to zjednodušeně představit tak, že kolik znaků klíč obsahuje, tolik o něm říkáme, že má bitů. Tradiční bezpečnostní standard ze 70. let pracuje se 64 bitovými klíči, které však již dnes běžné současné počítače dokáží brute force metodou prolomit do 24 hodin. Proto se dnes používají bezpečnostní klíče o 128 nebo 256 bitech. Pro ilustraci: pokud bychom zapojili do práce takový počet superpočítačů, že by za jedinou vteřinu dokázaly vyzkoušet 10^{18} kombinací znaků, rozlousknutí 256 bitového klíče by jim

trvalo až 3×10^{51} let, pokud by neměli obrovské štěstí. Pro všechny praktické účely můžeme říci, že prolomení takového klíče by trvalo nekonečně dlouhou dobu, je to tedy nemožné. Kvalitní kryptografický klíč je tedy jednou z dobrých metod ochrany dat.

Součástí programů, které jsou určeny pro brute force techniky přístupu, může být i databáze jednoduchých hesel, které často používají počítačově méně gramotní uživatelé (qwerty, 12345, své jméno či přihlašovací jméno, název organizace, atd.). Dále takové programy mohou obsahovat databáze hesel ukradené z jiných zdrojů. To se děje často a píše se o tom i v médiích: hackerům se občas podaří proniknout do informačních systémů velkých poskytovatelů internetových služeb, odkud získají přihlašovací jména a hesla uživatelů, ale často i jejich osobní údaje nebo dokonce čísla kreditních karet. V nedávné době se to prokazatelně stalo v případě společností Sony (PlayStation Network) či eBay. Tyto seznamy si útočníci ponechají pro vlastní „potřebu“, ale ještě častěji je nabídnou zájemcům na černém trhu. Co je pro útočníky na takovýchto databázích „nejcennější“, je skutečnost, která opět pramení z nedostatečné počítačové gramotnosti uživatelů. I když totiž mají hesla dlouhá a složitá používají je pro více různých internetových služeb. Když tak dojde k úniku dat a uživatel si změní heslo pouze na napadených stránkách, lze se dostat do všech ostatních služeb, kde použil heslo stejné. Útočníci s tímto počítají a přizpůsobují tomu i svůj software.

Z pohledu provozovatele webu existují různé techniky obrany proti brute force útokům. Systém může přijmout pouze určitý počet hesel v jistém čase, nebo data zamaskovat tak, aby útočící algoritmus nepoznal, že data jsou již odemčená a pokračoval tak ve zkoušení dalších kombinací. Co se týče pohledu uživatele a ochrany jeho účtů s citlivými daty, řešení jsou nasnadě. Důležité je používat dlouhá a komplikovaná hesla, nejlépe kombinaci malých a velkých znaků a číslic. Skvělou alternativou je jako heslo použít nějakou delší českou větu. Škodlivé programy češtinu neumí analyzovat, nepočítají s ní, a i když je teoreticky možné, že moderní brute force prolamovací programy mají databáze anglických slov a typických vět, s češtinou mohou počítat jen stěží – je pro ně pouze náhodným shlukem znaků. Takovéto „zaklínadlo“ pak stačí u každého webu mírně obměnit. Druhou metodou je používat správce hesel – což je software (například 1Password, vestavěné správce hesel mají i aktuální verze některých prohlížečů a operačních systémů), který generuje dlouhá jedinečná hesla a pak si je pamatuje a automaticky vkládá – uživateli pak stačí jedno heslo pro odemknutí (to samo by mělo splňovat podmínky kvalitního hesla a být obměňováno). Jelikož je bezpečnostní klíč obvykle uložen na počítači uživatele a nikoli na internetu, je používání správce hesel relativně bezpečné, podmíněné především fyzickou bezpečností počítače.

Webové služby často používají bezpečnostní opatření, jakými jsou například bezpečnostní otázky, když uživatel ke službě přistupuje z neznámého počítače. To je však problematické zejména v současnosti, ve věku sociálních sítí a všudypřítomných informací. Když se bezpečnostní otázka ptá uživatele, jak se jmenuje jeho pes a jeho profil na Facebooku je plný fotografií z procházek s Azorem, odpověď na takovou otázku není příliš tajná. Ještě horší je to v případě celebrit a známých osobností, kdy snad ani neexistuje taková informace, na kterou by se web mohl zeptat, aby o ní nevěděla i veřejnost. Ostatně právě to bylo podstatou medializované kauzy[5], kdy reportér magazínu Wired, Matt Honan, přišel o přístup ke svým internetovým účtům kvůli tomu, že potřebné osobní informace si útočník mohl snadno dohledat. V roce 2014 zde byla podobná kauza, kdy se útočník dostal k účtům několika celebrit u Apple.[6] Nejednalo se o brute force útok, ani o přístup zadními dvířky (viz níže), jak bylo zpočátku medializováno. Bylo zkrátka jednoduché uhodnout bezpečnostní otázky sloužící

k obnově hesla po jeho ztrátě.

Proti takovým útokům je nasnadě jedna metoda, a to tzv. **dvou-faktorové** neboli **dvou-krokové** ověření. To spočívá v tom, že po zadání hesla přijde uživateli ještě SMS zpráva na jeho telefonní číslo. V ní obdrží kód, po jehož zadání teprve získá přístup ke svému osobnímu účtu. Kromě SMS zprávy lze také využít generátor unikátních kódů, který nevyžaduje komunikaci s mobilní sítí ani internetem, stačí pouze generátor nainstalovat na mobilní telefon a mít jej po ruce. Bezpečnost je takto exponenciálně zvýšena, protože i kdyby útočník získal heslo uživatele, nemá jeho mobilní telefon a naopak. Dvou-krokové ověřování nabízí již velká část poskytovatelů internetových služeb a další přibývají, jelikož se jedná dnes již o závažný problém, jehož vnímání bylo díky mnoha medializovaným únikům hesel znásobeno.

Jedním z nejčastějších metod útoků proti počítačovým sítím, serverům[1] či webovým službám je tzv. **denial of service (DoS)** útok. Takový útok má za cíl daný systém či síť vyřadit z provozu, a to přehlcením serveru – výsledek se poté projeví tak, že webová služba, síť či server prostě nefunguje, nepovede se načíst požadovaný soubor, neodešle se email atd. Z teoretického hlediska není snadné bez dalšího odlišit zahlcenost serveru způsobenou nadprůměrně velkým zájmem od záměrného útoku. Tradiční DoS útok pošle na server velké množství falešných požadavků. Takovému útoku lze předejít poměrně snadno – software zablokuje větší množství požadavků přicházejících ze stejného počítače. Problematičtější je obrana vůči variantě nazývané **distributed denial of service** útok **(DDoS)**. Jak název napovídá, zde jsou požadavky distribuovány mezi různými počítači, které se často nacházejí na celém světě. Tomuto útoku je nelehké zamezit, protože napadený server nedokáže jednoduše odlišit škodlivý nápor od velkého množství legitimních připojení. Základem ochrany každého počítačového systému je tzv. **firewall**. Je to hardware nebo software, který filtruje komunikaci počítače s vnějším prostředím a umožňuje připojení pouze těm vnějším počítačům, které splňují stanovené podmínky.

DDoS útoky jsou prováděny buď velkou koordinovanou armádou hackerů s armádou počítačů, ale ještě častěji těmto útokům pomáhají tzv. **botnety.** Botnet je síť napadených počítačů často nic netušících uživatelů, kteří buď nedbalostí a online naivitou, nebo používáním neaktuálního, a tudíž zranitelného softwaru svůj počítač infikovali škodlivým softwarem. Útočník se také třeba může „nabourat“ do internetového routeru a všechny počítače přistupující k internetu přes něj se stanou součástí botnetu. Stačí, aby router nebyl zabezpečen kvalitním heslem nebo obsahoval objevenou bezpečnostní „díru". Pokud uživatel získá software na černém trhu, existuje nebezpečí, že je tento software infikován už předem. Proto se velká část počítačů v botnetech nachází například v Číně – počítačové pirátství je zde standardem; rozhodně však v tomto kontextu nemůžeme mluvit pouze o Číně. Ekonomika botnetů je v tmavých zákoutích internetu vysoce rozvinuta a v současnosti není problém si na online černém trhu DDoS útok vůči zvolenému webu objednat za nevelkou sumu. Po anonymní platbě kryptoměnou (například BitCoin) dá poskytovatel této služby signál armádě infikovaných počítačů, které práci automaticky odvedou. Útok vůči estonským vládním, mediálním a bankovním webům v dubnu 2007 byl DDoS útokem a jako takový zvýšil o této hrozbě povědomí mezi širší veřejností. Botnety pocházely z nejrůznějších míst: ze Spojených států, celé Evropy, Kanady,

[1] Lidová terminologie často ztotožňuje pojem „server“ s pojmem „webová stránka“, je to však velice nepřesné – server je počítač, který „servíruje“ data, tedy k němuž se cizí počítač připojuje. Těmito daty mohou být třeba webové stránky. Mnohé weby se nacházejí na mnoha serverech, často tzv. serverových farmách a naopak, jeden server může obsahovat mnoho webových stránek.

Brazílie, Vietnamu atd. Jednotlivé útoky mohly trvat minutu, ale i několik hodin –některé byly i desetihodinové. Je důležité poznamenat, že bylo mimo moc Estonska tyto útoky zastavit – přestaly samy. Vyšetřování odhalila téměř určité propojení útoků s veřejnými orgány Ruské federace, ta ale pochopitelně dodnes jakoukoli roli popírá.[7]

Škodlivý software, který zapojí počítač do botnetu, je v současnosti jeden z nejrozšířenějších a nejnebezpečnějších typů **malwaru**. Klasické počítačové viry či trojské koně jsou nyní již hrozbami spíše rudimentárními – smazání dat na napadeném počítači hackerům nestačí, dnes je pro ně atraktivní tato data získat (phishing), využít výpočetního výkonu počítače (botnet), či vydělat (ransomware). **Ransomware**, čili software požadující výkupné, je jedním z nejnovějších malwarových trendů. Je zaměřen na jednotlivce a zpravidla neusiluje o krádež informací, jeho cílem je finanční zisk. Takový škodlivý software se do počítače dostane tradičními cestami přes napadené soubory nezachycené antivirovým softwarem, falešné weby a v poslední době také přes typicky klamavé reklamy: často lze na webu nalézt odkazy, které tvrdí, že je daný počítač napaden viry nebo že je nutná jeho údržba. Důvěřivý uživatel tak v dojmu, že nabízený software počítači pomůže, dobrovolně stáhne a nainstaluje software škodlivý. Ten může mít samozřejmě různou povahu, může pouze smazat uživatelova data jako klasický virus, může ukrást choulostivé údaje, zapojit počítač do botnetu nebo dlouhodobě tajně odesílat vše, co uživatel napíše na klávesnici (obzvlášť rozšířený malware, tzv. **keylogger**).

Také se může odhalit jako zmiňovaný ransomware: ten zpravidla zablokuje počítač a veškerá data zakóduje a odemčení přislíbí teprve po provedení platby na účet útočníka. Ransomware může v tuto chvíli „odhalit svou pravou tvář“ a oznámit uživateli, jakého podvodu se stal obětí, nebo se může nadále tvářit legitimně: útočník například vystupuje jako FBI a tvrdí, že počítač je podroben vyšetřování a po platbě může být z vyšetřování vyňat; nebo jako výrobce počítače požadující licenční platbu za nepřetržité využívání služeb. Je vhodné zmínit, že oběťmi ransomware útoků se nově nestávají pouze počítače s nejrozšířenějším, a tudíž pro útočníky nejatraktívnějším operačním systémem Windows, či přenosná zařízení s otevřeným systémem Android, ale také počítače Apple s operačním systémem OS X.[8] Velmi specifickým druhem hrozby je také tzv. **logická bomba**. To je software, který uvnitř počítače po nějaký čas „spí“ a aktivuje se až po splnění určitých podmínek, například po uplynutí jisté doby. Může se jednat o malware, ale může jít i o součást legitimního softwaru, kterou jeden z autorů do kódu „propašuje“. Příkladem může být program, který zabuduje pracovník do účetního systému velké společnosti a který po delší době – typicky poté, co pracovníka propustí ze zaměstnání – způsobí zhroucení celého systému. Logické bomby je velice obtížné detekovat, protože ve „spícím“ stavu obecně nevykazují žádnou zjevně škodlivou aktivitu; velice obtížné bývá rovněž dohledat strůjce útoku.

Výše jsme si představili nejběžnější útoky, které jsou namířeny zejména proti uživatelům-jednotlivcům, ačkoli některé z nich jsou přímo propojeny s útoky na větší organizace, veřejné úřady atd. Nejlepší obranou proti individuálním útokům je obrana psychologická a nejvíce nezbytnou zbraní je osvěta a bezpečné praktiky užívaní internetu. Situace je však mnohem složitější, pokud jde o útoky vedené vůči organizacím a veřejnoprávním korporacím, mající za účel krádež citlivých dat, fyzickou destrukci, destabilizaci společenských procesů, nebo přímo (hybridně) vojenské cíle. Takové útoky jsou mnohem sofistikovanější, promyšlenější a využívají nezměnitelné inherentní vlastnosti počítačových systémů: neschopnosti odlišit přístup škodícího útočníka od legitimního přístupu

uživatele. Typickým, nejčastějším, ale ani zdaleka ne jediným druhem takového útoku je DDoS útok. Server je ve své podstatě přístupný všem připojeným počítačům splňujícím dané podmínky; při zvýšené zátěži tak tedy činí, dokud na to stačí jeho kapacity. Že se jedná o DDoS útok si lze všimnout zpravidla, až když k němu dojde.

Nejsofistikovanější informační systémy vládních agentur či velkých obchodních společností používají velké množství obranných systémů k ochraně proti únikům informací a proti útokům obecně – od používání sofistikovaných firewallů přes aktivní monitoring pohybů na sítí a jejich anomálií až po tvorbu klamných systémů, které mají útočníkovi podsunout mylné informace a nejlépe odhalit i jeho identitu. Takový systém se nazývá **honeypot** (hrnec medu, který má navnadit „medvěda“), celá infrastruktura honeypotů je pak **honeynet**. Pokud napadený získá informace o počítači, z něhož byl útok veden, například za pomoci honeypotu, může zahájit kybernetický protiútok, neboli **hacking back**, aby odhalil útočníkovu fyzickou identitu nebo zničil jeho systémy. O legitimitě takového protiútoku si ještě řekneme víc níže, důležité však je, že mnohé dotčené strany si již uvědomují nutnost nikoli pouze pasivních opatření, ale především aktivní kybernetické obrany, jejíž komplexnost musí narůstat úměrně s komplexností útoků.

Obrana vůči kyberútokům je obecně ve své podstatě mnohem složitější než kyberútoky samotné. Kvůli komplexnosti počítačových systémů stačí útočníkovi využít pouze jediné zranitelnosti v celém řetězci na sebe navazujících subsystémů. Jedná-li se i o tak triviální úkol, jakým je zobrazení webové stránky, podílejí se na něm přinejmenším tito aktéři: výrobce hardwaru a operačního systému, doručovací služba, která přepraví počítač od výrobce či distributora ke koncovému uživateli, poskytovatel internetového připojení, vývojář webového prohlížeče, tvůrce tzv. pluginů (zásuvných modulů) ve webovém prohlížeči, tvůrce nástrojů pro tvorbu webových stránek, správce serveru, na němž je webová stránka umístěna, výrobce softwaru, který běží na serveru, zadavatel případné reklamy běžící na webové stránce, DNS[2] registrátor, který zaregistroval webovou adresu, na které lze web nalézt, poskytovatel DNS služby, která převede jméno webové stránky na unikátní číselnou hodnotu, poskytovatel certifikátu, který stvrzuje, že správce webu je tím, za něhož se skutečně vydává a v neposlední řadě také všichni poskytovatelé internetového připojení, přes které se signál postupně dostal až k cílovému uživateli.[9] Stačí selhání jediného z těchto subjektů a data uživatele mohou být přístupná třetím stranám, zničena, či jinak zneužita.

To, že na bezpečnost počítačových systémů mají vliv i tak triviální okolnosti jako totožnost přepravce počítače k zákazníkovi dokazuje kromě jiného i jednoduchost, s jakou se dostal do „oběhu“ dnes již proslulý virus Stuxnet. Ten se v roce 2010 rozšířil na počítačích vládních orgánů v Íránu a způsobil nezanedbatelnou fyzickou škodu – infikoval zařízení na obohacování uranu a dle všeho v nich zničil až tisíc centrifug. Po celou dobu dokonce tyto centrifugy hlásily zcela běžný provoz. Do té doby se jednalo bezpochyby o nejsofistikovanější počítačový virus, který měl velice složitý kód a způsob fungování a který způsobil hmatatelnou nezanedbatelnou fyzickou škodu srovnatelnou s aktem válečné agrese. Podle všech indicií zdrojového kódu i podle informací uniklých z důvěrných kanálů lze předpokládat, že virus vznikl za spolupráce izraelských a amerických tajných služeb. Na íránské počítače se však dostal způsobem zcela jednoduchým – na USB flash disku. Sympatizant íránské

[2] DNS si můžeme představit jako jakýsi telefonní seznam. Přiřazuje snadno zapamatovatelné webové adresy na číselné IP adresy, které hierarchicky spojí uživatele s požadovaným serverem a webem. Více o doménách, adresách, atp. lze nalézt kupříkladu na webu cz.nic, provozovatele domén s koncovkou .cz.

opozice (a dle všeho izraelský agent) pouze vložil infikovanou USB klíčenku do vládního počítače a virus se pak začal šířit sám. Přitom nelze říci, že íránské autority neaplikovaly rozumné bezpečnostní principy. Počítače průmyslových řídicích systémů nebyly připojené k internetu, nebyly tedy vystavené přímým útokům. Na počítačích byl nainstalován operační systém Windows, který bylo potřeba z nějakého důvodu aktualizovat. Pracovníci tedy aktualizaci, dbajíce bezpečnosti, přinesli na USB disku – infikovaném Stuxnetem.[10]

V současné době je nejčastějším způsobem, který „otevře" počítač útočníkům, tzv. **zero-day** útok. Operační systémy a software, který na nich běží, jsou velmi komplexní programy. Jejich kód a způsob fungování je složitý, je často výsledkem desítek let práce. Stejně složitý a komplexní je ale i vnější svět, se kterým tento software přichází do styku – zejména když je neustále připojen k internetu. Software obsahuje mnoho tzv. zranitelností, které mají různý původ – někdy se jedná o programátorskou chybu, někdy o tzv. zadní vrátka (**backdoor** – umožňují autorovi softwaru jistý druh servisního přístupu, deklarovaného či utajeného), jindy jsou součástí základní funkce programu, jejíž zneužitelnost se ukáže až časem. Různorodá technologická povaha zranitelností není tak důležitá jako spíše fakt, že dávají potenciálnímu útočníkovi možnost neoprávněného přístupu do systému a také možnost data uživatele zničit, modifikovat či ukrást. Samotný pojem „zero-day" znamená, že od opravy chyby uběhlo doslova „nula dnů" – vývojář programu o chybě buď ještě neví, nebo zatím nevydal bezpečnostní aktualizaci. Uživatel softwaru je tedy stále vystaven potenciálnímu nebezpečí. Příkladem může být právě virus Stuxnet, který využil několika zero-day chyb operačního systému Windows (využití či zneužití zero-day je známo jako **exploit**).

Díry v operačních systémech či programech objevují jak jejich výrobci, tak různé nezávislé společnosti, agentury nebo i věřené orgány. Kolem objevování zero-day zranitelností se vytvořil jakýsi etický kodex a je zvykem, že ten, kdo je objeví, o tom neprodleně informuje autora softwaru a chyba je publikována až se zveřejněním bezpečnostní opravy. Tento systém má ale několik technických nedostatků. Výrobci softwaru obvykle zveřejňují bezpečnostní záplaty s prodlením (co se operačních systémů týče, Microsoft tak dělá pravidelně každý měsíc, Apple bezpečnostní záplaty obvykle přibaluje k obecným aktualizacím svých systémů, vývojáři webových prohlížečů, které nejsou součástí systémů, jsou většinou flexibilnější) a nějakou dobu trvá, než si tyto opravy uživatel nainstaluje. Běžní uživatelé obecně stále nerozumějí důležitosti bezpečnostních záplat, aktualizace softwaru je spíše otravují a odkládají je, dokud je k tomu systém přímo nepřinutí. Běžného uživatele se však alespoň netýkají adresní útoky, ale pouze ty obecné, které jsou nasměrované proti jakémukoli počítači. Co se týče společností či vládních agentur, jejich IT oddělení si většinou důležitost bezpečnosti systémů uvědomuje. Kvůli vnitropodnikové byrokracii a nezbytnosti aktualizace provádět opatrně, aby nebyl ohrožen chod systémů, vzniká mnohdy mezi dostupností záplaty a její aplikací dlouhá prodleva. Dalším dnes hodně diskutovaným problémem je objevování zero-day zranitelností subjekty, které si tato zjištění nechávají pro sebe. Mohou pak kdykoli v budoucnosti této chyby využít ve svůj vlastní prospěch, pokud je ovšem někdo nepředběhne a chyba není „předčasně" opravena.

Bohatá diskuse se vede na téma, že podle všech dostupných informací zero-day exploitů využívají nikoli pouze temná zákoutí internetu, ale i složky veřejné moci. Zdaleka největší (dle ročního rozpočtu) federální zpravodajská služba USA, National Security Agency (NSA), zakládá velkou část své práce na sběru informací z internetu, sledování počítačů osob podezřelých z terorismu a útocích

vůči těmto počítačům. K tomu často užívá metody, které nejsou od metod kyberzločinců rozeznatelné. Existují důvodná podezření, že NSA využívá velkého počtu zero-day zranitelností,[11] o kterých ví jen ona, ke sledování a útokům proti počítačům nepřátelských subjektů. Je sice možné, že existují tajné dohody mezi technologickými společnostmi a agenturami jako je NSA, které dávají vládě zadní vrátka do svých systémů, toto tvrzení však zůstává i nadále pouhou konspirační teorií, kterou se dosud nepodařilo dokázat, ale ani vyvrátit. Odhalování a shromažďování zero-day zranitelností softwaru je beztak silnou zbraní a organizaci s obdobnými prostředky dává samo o sobě do rukou neuvěřitelnou moc. Jsme v situaci, kdy se nám definice kyberútoku, jak jsme o něm hovořili na začátku textu, mírně znejasňuje – některé veřejné orgány pro naplnění svých cílů používají metody, které jsou prakticky shodné s metodami nelegitimních aktérů. Zároveň se tím dostáváme k jednomu z klíčových dilemat současného kyberprostoru: **soukromí versus bezpečnost**.

V posledních několika letech je dominantním tématem diskusí o kybernetické bezpečnosti aféra kolem programu NSA známého jako PRISM, o kterém útržkovité informace vynesl na světlo Edward Snowden. PRISM je systém, který údajně shromažďuje velké množství informací, které po sobě lidé na internetu dobrovolně či neúmyslně zanechávají a odhaluje tak především teroristy a jejich plánované útoky. V dnešní době musí být každému jasné, kolik dat po sobě na internetu zanechává a že k těmto datům mají přístup i autority. Diskuse tak rozvířilo spíše zjištění, že někdo z těchto informací vytváří komplexní profily osob a následně je vyhodnocuje. Navíc se to týká jak amerických občanů, tak i občanů evropských. Většina datových center poskytovatelů internetových služeb se však nachází na území USA a tito poskytovatelé samotní zde mají většinou domicil. Skutečným problémem však je, jak se tyto informace dostaly na veřejnost a to, že o nich představitelé státních orgánů mimo NSA neměli tušení.[12] To je však spíše otázka, kterou na národní úrovni musí řešit samotné USA. Je však patrné, že doba naprosté anonymity a soukromí na internetu již skončila, pokud někdy vůbec začala, a o soukromí a osobní data může uživatele připravit nejenom útočník, ale i legitimní státní aktér. Zbývá doufat, že tato ztráta soukromí skutečně vede ke zvýšení veřejné bezpečnosti. To, nakolik jsou kyberútoky a narušení soukromí ze strany agentur jako NSA přípustné, je již spíše otázkou politické teorie – ta musí dojít ke konsenzu o otázkách politické legitimity takovéto činnosti. Lze obecně předpokládat, že tak, jak politická teorie přiznává politickou legitimitu například státnímu monopolu násilí, dospěje také ke shledání, že je společensky legitimní narušovat soukromí ze strany veřejné moci, pokud tato moc ovšem nebude zneužívaná a bude aplikovaná proporcionálně ke svému účelu.

U kyberútoků je nezbytné rozlišovat mezi tím, jestli je útok blízký nebo vzdálený. **Vzdálený útok** se vyznačuje tím, že útočník využije internet, typicky jedním ze způsobů zmiňovaných výše, dále je to možné například prolomením ochrany bezdrátové sítě, ke které je napadený počítač připojen a v rámci níž uživatel sdílí svá data. **Blízký útok** předpokládá, že útočník získá fyzický kontakt s napadeným počítačem a „osobně“ nějakým způsobem modifikuje jeho hardware nebo software. Tento druh útoku je samozřejmě mnohem složitější. Je nákladnější, riskantnější, vyžaduje buď hluboké utajení útočníka, nebo širší konspiraci v rámci organizace, která s počítačem přichází do styku. Výsledky a následky útoku mohou však být závažnější. Provozování vzdálených útoků je pro útočníky bezpochyby více morálně ospravedlnitelné. Normativní a etická pravidla, která má v moderní společnosti většina jedinců zažitá, fungují tak, že pro psychicky zdravého člověka je problém závažně porušit společenské normy – například něco fyzicky ničit. Když se však jedná o útok

virtuální, jakkoli mohou být jeho výsledky hmatatelné, je to pro lidské svědomí jednodušší. Mezi činem a jeho následkem není jasně viditelné pojítko a to ho dělá pro značnou část populace přípustným, a pokud se s ním pojí třeba peněžní odměna, tak i přímo atraktivním. Pouze specifická část populace je schopna zlikvidovat centrifugy v zařízeních na obohacování uranu (nehledě na fyzické překážky), ale požádat někoho, aby pouze vložil USB klíčenku do počítače, je jednoduché. Člověk to udělá, i když je informován o následcích takového činu. Tento psychologický jev je také patrný například u stahování autorsky chráněných děl z internetových úložišť – člověk, který by nebyl schopen v kamenném obchodě ukrást zboží, považuje za eticky přípustné ukrást digitální ekvivalent stejného produktu na internetu. To je samozřejmě psychologicky odůvodnitelný rozpor – společenské normy slouží právě k tomu, aby biologicko-psychologické pochody zmírňovaly a modifikovaly. Proto se stejně jako pro oblast ochrany autorských práv pro kyberbezpečnost počítá s postupnou změnou norem – a to jak etických a morálních, tak norem právních. Pokud mluvíme o právních normách, musejí se internetovým hrozbám přizpůsobit jak na úrovni národní, což se v mnohých státech do značné míry postupně děje, tak i na úrovni práva mezinárodního.

Tím se dostáváme k druhému dilematu v kyberbezpečnosti, kterým je otázka **aplikovatelnosti mezinárodního práva** pro kyberprostor. Mezinárodní právo je z velké části tvořeno zvyky a obyčeji, je utvářeno dlouhá staletí a obecně lze říci, že je velice konzervativní – funguje jako jakýsi společný jmenovatel pro všechny státy. Proto je jeho modifikace obtížná a zdlouhavá. Diskuse o aplikaci mezinárodního práva na incidenty v kyberprostoru a o jeho případné modifikaci odstartovala po roce 2007, kdy došlo ke zmíněným událostem v Estonsku. V roce 2009 se sešla skupina desítek uznávaných světových expertů pod záštitou estonského kybernetického obranného centra excelence NATO CCD COE, aby formulovali pravidla, jak na kyberprostor mezinárodní právo aplikovat. Na tomto základě vznikl tzv. **Tallinnský manuál** aplikace mezinárodního práva na kybernetickou válku [13]publikovaný v roce 2013.

S výše řečeným je bytostně spjato i dilema, jestli jsme schopni stávající mezinárodní právo adaptovat pro kyberprostor, anebo jestli by nebylo lepší cestou formulování zcela nových norem pro tyto novodobé fenomény. Oba přístupy jsou legitimní a mají své podporovatele. Nikola Schmidt z Univerzity Karlovy[14] je toho názoru, že kybernetická bezpečnost je tak novým systémem, že je nutno k ní přistupovat z pozice „prázdnoty“ právních norem, které je třeba začít vyplňovat. Autor tohoto textu se naopak přiklání k názoru, že mezinárodně-právní obyčeje jsou odrazem jakéhosi meta -práva, které existuje bez ohledu na konkrétní společenské zřízení či technologický pokrok. Tyto meta -právní normy svým účelem chrání legitimní zájmy jedinců ve společnosti; právní systém, který na jejich základě vzniká, pak představuje již ochranu konkretizovanou. Když máme právní normu, která zakazuje zcizení nebo zničení soukromého majetku, pouze výkladem této normy můžeme dojít k tomu, že majetek může být i nehmotný, nacházející se v digitální podobě. Takovým způsobem pak stačí zrevidovat již existující mezinárodně-právní normy. Pakliže považujeme za válečný akt ohrožení územní celistvosti cizího státu, stačí, když na stejnou úroveň položíme celistvost kyberprostoru kontrolovaného danou zemí. Tento argument vychází z předpokladu, že mezilidské vztahy vždy byly a jsou řízené stejnými mechanismy a se společenským a technologickým vývojem se mění pouze jejich vnější podoba. Tak či onak musí proběhnout široká diskuse na toto téma, protože ať již zvítězí formulace nových norem, nebo reinterpretace norem stávajících, nestane se to ze dne na den.

V dalších publikacích navážeme na tato témata a budeme se zabývat mimo jiné tím, jak Tallinnský

manuál mezinárodní právo vykládá a jak je lze na kyberválku aplikovat. Posléze se dostaneme k institucionálnímu zakotvení kyberbezpečnosti na úrovni orgánů NATO, Evropské unie a představíme aktuální právní stav v České republice, tedy to, jak je zatím kyberprostor normativně zabezpečen na úrovni vnitrostátní.

[1] Cyberspace – What is it? RAJNOVIC, Damir. Cisco Blogs [online]. [cit. 2015-05-28]. Dostupné z: https://blogs.cisco.com/security/cyberspace-what-is-it

[2] CLARK, David, BERSON, Thomas a LIN, Herbert. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, D.C.: The National Academies Press, 2014, 133 s. ISBN 03-093-0318-4. s. 8-9.

[3] tamtéž, s. 9.

[4] tamtéž, s. 13.

[5] How Apple and Amazon Security Flaws Led to My Epic Hacking. Wired [online]. [cit. 2015-05-28]. Dostupné z: http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

[6] Apple to tighten iCloud security after celebrity leaks. BBC News [online]. [cit. 2015-05-28]. Dostupné z: http://www.bbc.com/news/technology-29076899

[7] CLARK, David, BERSON, Thomas a LIN, Herbert. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, D.C.: The National Academies Press, 2014, 133 s. ISBN 03-093-0318-4. s. 13.

[8] FBI Ransomware Now Targeting Apple's Mac OS X Users. SEGURA, Jérôme. Malwarebytes Unpackded [online]. [cit. 2015-05-28]. Dostupné z: https://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/

[9] CLARK, David, BERSON, Thomas a LIN, Herbert. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, D.C.: The National Academies Press, 2014, 133 s. ISBN 03-093-0318-4. s. 37-40.

[10] The Real Story of Stuxnet. KUSHNER, David. IEEE Spectrum [online]. [cit. 2015-05-28]. Dostupné z: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet#

[11] NSA saves zero-day exploits for high-value targets. GOODIN, Dan. Ars Technica [online]. [cit. 2015-05-28]. Dostupné z: http://arstechnica.com/security/2013/10/nsa-saves-zero-day-exploits-for-high-value-targets/

[12] S americkým sledováním se musíme smířit. REZEK, Tomáš. Asociace pro mezinárodní otázky [online]. [cit. 2015-05-28]. Dostupné z: http://www.amo.cz/publikace/s-americkym-sledovanim-sa-musime-zmierit.html#.VWZee2A_uX3

[13] Tallinn Manual on the International Law Applicable to Cyber Warfare. NATO Cooperative Cyber Defence Centre of Excellence [online]. [cit. 2015-05-28]. Dostupné z: https://ccdcoe.org/tallinn-manual.html

[14] Kyberprostor bude strategickým místem budoucnosti. SCHMIDT, Nikola. Natoaktual.cz [online]. [cit. 2015-05-28]. Dostupné z: http://www.natoaktual.cz/kyberprostor-bude-strategickym-mistem-budoucnosti-fyl-/na_analyzy.aspx?c=A140630_135804_na_analyzy_m02

Think-tank Evropské hodnoty je nevládní odborná instituce bránící liberální demokracii.

Politikům předkládáme odborná doporučení a systematicky sledujeme a hodnotíme jejich práci. Za základní prvky vysoké politické kultury považujeme aktivní občany, zodpovědné politiky a soudržnou společnost, která sdílí hodnoty svobody a demokracie.

Od roku 2005 se jako nevládní nezisková organizace, která není spojena s žádnou politickou stranou, věnujeme výzkumné a vzdělávací činnosti. Vedle vydávání odborných publikací a komentářů pro média, pořádáme konference, semináře a školení pro odbornou i širší veřejnost. Na svých akcích zprostředkováváme dialog mezi politiky, odborníky, novináři, podnikateli i studenty.

POLITICKÁ KULTURA • ČESKO V EVROPSKÉ UNII • VNITŘNÍ BEZPEČNOST

THINK-TANK EVROPSKÉ HODNOTY

Vlkova 36, 130 00 Praha 3

info@evropskehodnoty.cz

www.evropskehodnoty.cz

facebook.com/Evropskehodnoty