ZaBEZPEČ si vedomosti:
Kybernetická bezpečnosť

Autor:
Rastislav Kačmár

Technologický pokrok a bezpečnosť

Stáročia spoločenského a technologického vývoja priniesli nové hrozby pre individuálnu aj globálnu bezpečnosť. Kým spoločenský vývoj spôsobil vznik hrozieb, akými sú ekonomická, potravinová či environmentálna bezpečnosť, technologický pokrok je dôvodom, prečo je čoraz aktuálnejšia aj kybernetická bezpečnosť. Dnešný svet sa spolieha na využívanie technológií a ľudia, azda len s výnimkou krajín tretieho sveta, denne používajú počítače a mobilné telefóny, platia platobnými kartami a prostredníctvom internet bankingu, a teda sú závislí od elektrickej energie a internetu.

Moderné technológie nám uľahčujú život, dnes si už život bez smartfónov, počítačov, internetu či navigačných systémov nedokážeme predstaviť. Úmerne s tým, ako nám technológie zjednodušujú každodenné úlohy, rastie aj naša závislosť na nich a frekvencia, s akou ich využívame. Skutočnosť, že technológie sa pomaly dostávajú do každej oblasti nášho života zvyšuje našu zraniteľnosť voči kybernetickým útokom a zdôrazňuje dôležitosť kybernetickej bezpečnosti. Hrozba kybernetických útokov sa pomerne jednoducho rozšírila zo striktne vymedzenej sféry, ktorá bola doménou technologických expertov, do všetkých oblastí spoločenského života, vrátane politických procesov a bezpečnostného plánovania na národnej, ale aj medzinárodnej úrovni.

Ešte v roku 1993 existovalo na celom svete len päťdesiat internetových stránok, na začiatku milénia to už bolo viac ako päť miliónov a v roku 2010 už samotná Čína dosiahla hranicu štyristo miliónov používateľov internetu. Medené telefónne káble používané v 80. rokoch 20. storočia boli schopné za jednu sekundu preniesť jednu stranu informácií, optické káble používané dnes zvládnu za sekundu deväťdesiattisíckrát viac. Podobne významné zmeny nastali aj v oblasti skladovania informácií. Kým v roku 1980 by gigabajt informácií obsadil celú miestnosť, dnes dokážeme niekoľkonásobok tohto množstva dát skladovať na kompaktných USB kľúčoch, ktoré sú menšie ako ľudská dlaň. Nízke náklady, anonymita a asymetrie v zraniteľnosti znamenajú, že aj menej významní aktéri môžu kybernetický priestor využiť na presadzovanie tvrdej a mäkkej moci, a to v oveľa väčšej miere, ako im to ich obmedzené kapacity umožňujú v tradičných sférach medzinárodnej politiky. Prekážky

pri vstupe do kybernetického priestoru sú zanedbateľné, takže neštátni aktéri môžu s využitím obmedzených zdrojov v tejto oblasti zaujať významnú pozíciu. Naopak, veľmoci nedokážu kybernetický priestor ovládať tak ako tradičné oblasti, či už ide o nadvládu na súši, mori alebo vo vzduchu.[1]

Ako sa kybernetická bezpečnosť dostala do centra pozornosti?

Kybernetická bezpečnosť sa objavila začiatkom deväťdesiatych rokov 20. storočia, v tomto období však bola takmer výlučne doménou počítačových expertov a informatikov. Klasické bezpečnostné prístupy sa kybernetickou bezpečnosťou nikdy nezaoberali a do popredia sa dostala až na konci 20. storočia. Prvá konferencia, ktorá kybernetickú bezpečnosť zaradila medzi dôležité bezpečnostné témy, sa uskutočnila až v roku 1999 v USA. [2] V tom čase už uplynulo osem rokov od vydania odbornej správy Computers at Risk: Safe Computing in the Information Age, v ktorej počítačoví experti upozorňovali na skutočnosť, že technologický pokrok sa stáva dôležitým činiteľom v oblasti bezpečnosti. Správa bola vydaná v roku 1991 a definovala kybernetickú bezpečnosť ako *„ochranu pred nechceným odhalením, modifikáciou alebo zničením údajov v systéme a takisto ako ochranu samotných systémov.“* [3] Národná akadémia vied už v tom čase tvrdila, že USA závisia na počítačoch, ktoré kontrolujú transport energií, komunikáciu, letectvo, finančné služby a mnoho ďalších oblastí.

Autori zároveň upozorňovali na hrozbu kybernetického terorizmu a systematických kybernetických útokov, ktoré by mali vážne následky pre infraštruktúru USA. Niektorí teoretici aj napriek tomu tvrdili, že kybernetickú bezpečnosť nie je potrebné vymedzovať ako samostatný sektor bezpečnosti, ale postačí, ak sa jej bude venovať dostatočná pozornosť v rámci iných, už existujúcich bezpečnostných sektorov, najmä v rámci vojenského, politického a ekonomického. Informačná revolúcia a globalizácia však spôsobili, že počítačoví odborníci čoraz viac upozorňovali, že ak sa digitálne technológie dostatočne nezabezpečia, môžu priniesť vážne hrozby pre

[1] Nye, J. (2010). *Cyber Power,* http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, online [cit. 1.10.2016]
[2] Schmitt, (2013). *International Law in Cyberspace: The Koh Speech and Talinn Manual Juxtaposed.*
[3] National Research Council. (1991). *Computers at Risk: Safe Computing in the Information Age.* Washington, D.C. : National Academy Press

spoločnosť. Postupne začali význam kybernetickej bezpečnosti chápať aj najvyšší politickí predstavitelia. Napríklad americkí politici vystríhali pred takzvaným elektronickým Pearl Harborom a George W. Bush v roku 2003 vydal Národnú stratégiu pre bezpečný kybernetický priestor. Dnes je kybernetická bezpečnosť už bežnou súčasťou bezpečnostnej agendy štátnych aj neštátnych aktérov.

Špecifiká kybernetickej bezpečnosti

Čím je kybernetická bezpečnosť špecifická, respektíve čím sa líši od tradičných alebo nových hrozieb, ktoré patria do takzvanej ľudskej bezpečnosti (human security)? Prvý faktor, ktorý spôsobuje naliehavosť tejto problematiky, je, že kybernetická bezpečnosť sa týka obrovského počtu ľudí. Hrozby sú omnoho bezprostrednejšie ako tradičné vojenské hrozby. Ľudia prípadnú nedostupnosť internet bankingu, internetu a e-mailu či telefónnej siete alebo útok na ich súkromné údaje, teda javy, ktoré sa môžu odohrať v priebehu niekoľkých sekúnd a spôsobiť jednotlivcovi značné škody, často vnímajú osobnejšie a citlivejšie ako občianske konflikty vo vzdialených regiónoch alebo environmentálne problémy, dôsledky ktorých sa prejavujú v dlhodobom horizonte. Kybernetická bezpečnosť sa tak jednoducho posúva zo sféry národnej bezpečnosti k bezpečnosti spoločenskej a individuálnej.

Útoky v kybernetickom priestore sú zároveň ľahšie uskutočniteľné – útočník k tomu, aby uskutočnil kybernetický útok, potrebuje zväčša len počítač, pripojenie na internet a svoje vlastné schopnosti. V tomto prípade sa nevyžaduje fyzický prístup k obeti. Povaha kybernetického priestoru umožňuje útočníkom nasadiť svoje ofenzívne kapacity prakticky kdekoľvek a kedykoľvek, a to v priebehu niekoľkých minút, navyše bez nutnosti fyzického presunu a prítomnosti jednotiek. Útoky tak majú potenciál ohroziť náš každodenný život a majú väčší dopad na bežných ľudí, ako hrozby, ktoré sú síce závažnejšie, no ich výskyt je menej častý a je obmedzenejší aj geograficky. Kybernetické útoky geografia neovplyvňuje a nezabránia im ani tradičné fyzické hranice. Na druhej strane, bežný človek sa pred útokmi dokáže brániť len do istej miery a nie všetci ľudia, ktorí používajú moderné technológie, môžu byť experti na

kybernetickú bezpečnosť. Často pozorujeme skôr opačný jav – bežní používatelia neovládajú ani základy informatickej bezpečnosti a nedodržiavajú jednoduché opatrenia a postupy, ktoré ich môžu ochrániť pred kybernetickým útokom, prípadne znížiť jeho pravdepodobnosť.

Ďalší problém je, že kybernetické hrozby sú mimoriadne sofistikované, a preto sa aj útočník ťažko stopuje. Pri väčšine kybernetických útokov môžeme len predpokladať a hádať, kto bol skutočným vinníkom a len veľmi zložito to vieme dokázať. Hackeri totiž pre svoje útoky využívajú napadnuté počítače nič netušiacich bežných užívateľov internetu alebo servery a IP adresy na iných miestach, než na tých, kde sa naozaj nachádzajú.

Problém z hľadiska bezpečnosti predstavuje aj skutočnosť, že technologický pokrok je nezastaviteľný. Vedci a vynálezcovia pravidelne prichádzajú s novými technologickými výdobytkami, čo zároveň zvyšuje riziko ohrozenia, požiadavky na bezpečnosť a zároveň aj mieru, do akej sa spoločnosť spolieha na technológie. Pokroky v oblasti umelej inteligencie ukazujú, že ľudstvo ešte ani zďaleka nie je za hranicami svojich možností. Avšak hľadanie spôsobov, ako zabezpečiť už existujúce technológie pred kybernetickými hrozbami, nehovoriac o tom, ako sa postarať o to, aby neboli zraniteľné aj nové a omnoho komplexnejšie technológie, spôsobuje vrásky na čele bezpečnostných expertov a ľudí zodpovedných za ochranu kritickej infraštruktúry po celom svete.

Práve kritická infraštruktúra je v prípade kybernetických hrozieb jedna z najviac ohrozených oblastí. Všetky jej zložky sú čoraz viac závislé na informačnej infraštruktúre pri správe informácií, komunikácií a kontrolných funkciách. Kombinácia počítačov a komunikačných systémov dnes slúžia ako základná infraštruktúra pre organizácie, priemysel a ekonomiku a sú aj hlavnou zložkou bezpečnostného prostredia. [4] Ako príklad môžeme použiť Spojené štáty americké, jeden z najvyspelejších štátov sveta - len samotné Ministerstvo obrany USA využíva 15 000 sietí a sedem miliónov kusov výpočtovej techniky, ktoré musia byť patrične zabezpečené a pravidelne kontrolované. Podľa amerického ministra obrany sú Spojené štáty americké pravidelne vystavované

[4] Cavelty – Krishna-Hensel – Mauer. (2007). *Power and Security in the Information Age. Investigating the Role of State in Cyberspace.* Hampshire : Ashgate Publishing Limited.

hrozbe kybernetického útoku od viac ako stovky zahraničných tajných služieb.[5] Samozrejme, hrozba presahuje ministerstvo obrany a jeho štruktúru, ktorá je len jednou z množstva súčastí vládnej administratívy. Na bezpečnosti kybernetických sietí sú závislé viaceré prvky kybernetickej infraštruktúry vrátane elektrární, dopravných a finančných systémov, ktoré sú riadené práve modernými technológiami.

Postupne tak vznikla predstava o kybernetických hrozbách, ktoré môžu ovplyvniť fungovanie elektrických sietí, potrubí a ropovodov, radarov a iných elektronických systémov, čo by viedlo k takzvaným kybernetickým katastrofám – problémom pri dodávkach energií, výpadkom telekomunikačných a finančných sietí alebo dopravným nehodám. Podľa niektorých analýz by rozsiahly DDoS útok namierený proti Spojeným štátom americkým, prípadne inému štátu podobných rozmerov a stupňa rozvoja, mal devastujúce následky. V prípade, že by došlo k prerušeniu distribúcie energií a iných služieb na dobu troch mesiacov, následky kybernetického útoku by boli porovnateľné so škodami spôsobenými štyridsiatimi hurikánmi.[6]

Špecifikom bezpečnostných hrozieb je aj skutočnosť, že ich vznik môže zapríčiniť nielen vedomé konanie, ale aj systémová chyba. Kybernetické hrozby často vyplývajú z nedostatkov, takzvaných zraniteľností, ktoré vo väčšine prípadov vznikajú neúmyselne už pri samotnom vývoji bežne používaného softvéru alebo pri zabezpečovaní kritickej infraštruktúry. Zraniteľnosť v systéme môže byť využitá potenciálnym útočníkom. Ideálny stav, teda existencia systémov a softvérov bez využiteľných zraniteľností, je v súčasnosti prakticky nedosiahnuteľná.

Typy hrozieb

Kybernetické bezpečnostné hrozby sú mimoriadne rôznorodé. Ciele útokov sa nenachádzajú len v štátnom aparáte a vojenskej sfére, ale aj v ekonomickom, environmentálnom a spoločenskom sektore. Kybernetická bezpečnosť má jednoznačné

[5] Murphy, T. (2010). Security Challenges in the 21 st Century Global Commons, http://files.redsafeworld.net/200000946-5458a54d26/Global%20Commons.pdf, online [cit. 4.10.2016]

[6] Cornish – Hughes – Livingstone. (2009). *Cyberspace and the National Security of the United Kingdom. Threats and Responses.* London : Royal Institute of International Affairs

vojenské implikácie a najmodernejšie technológie sú využívané práve ozbrojenými silami, ktoré sú na informačných a komunikačných technológiách závislé. Okrem priamych vojenských bezpečnostných hrozieb, ktoré vyplývajú z možnosti, že vojenské systémy, prípadne utajené informácie by sa dostali pod kontrolu nepriateľa, môžeme vymedziť aj nepriame a nevojenské kybernetické bezpečnostné hrozby. Tie sa týkajú už spomínaných nevojenských sektorov, najmä energetickej, finančnej a dopravnej infraštruktúry štátu.[7] Vo všeobecnosti kybernetické hrozby môžeme rozdeliť do štyroch domén:

- štátne a štátmi sponzorované útoky,
- ideologický a politický extrémizmus,
- organizovaný zločin,
- individuálny zločin.

Jednotlivé domény a ich obsah sa navzájom prelínajú. Napríklad hacking môže byť individuálnym zločinom a neorganizovanou aktivitou, no jeho využitie je časté aj v iných doménach a s oveľa väčšími následkami, ako pri útokoch individuálnych hackerov. Najväčšiu pozornosť si získavajú útoky realizované štátnymi aktérmi, prípadne inými aktérmi s podporou štátov, a to najmä preto, že v prípade preukázateľnosti pôvodcu útokov majú najväčší potenciál vyvolať konflikt aj v iných sférach.

Druhou doménou je ideologický a politický extrémizmus, ktorý prebieha v kybernetickom priestore. Z hrozieb, ktoré patria do tejto domény, je v súčasnosti najzávažnejšou terorizmus, respektíve činnosť teroristických organizácií v kybernetickom priestore. Kybernetické útoky však nenapĺňajú potenciálne obete takým strachom a nevyvolávajú podobný teror a emócie ako fyzické útoky. Sú ťažšie zapamätateľné a neprodukujú obrazový materiál, ktorý si obyvateľstvo môže s daným útokom asociovať. Teroristické organizácie preto aj naďalej viac využívajú klasickú formu útokov, samovražedné atentáty na civilné obyvateľstvo. Na druhej strane, internet svojou povahou poskytuje teroristickým organizáciám lacný a rýchly spôsob šírenia informácií na globálnej úrovni, uľahčuje komunikáciu medzi jednotlivými

[7] Cornish P. et al. (2010). *On Cyber Warfare.* London : Royal Institute of International Affairs

bunkami, pomáha získavať zdroje a nových členov. Prostredníctvom internetu sa cieľová skupina teroristických organizácií, ktoré sa predtým zameriavali najmä na nábor priamo v teréne rozšírila, omnoho väčší dopad majú aj videá a iné formy propagandy zverejňované na internete.

Najväčšie kybernetické útoky

- 2003 – výpadok prúdu na východnom pobreží USA – bez elektriny ostali niekoľko dní milióny ľudí, až v roku 2007 sa zistilo, že útok zapríčinil vírus Slammer worm.
- 2007 – Estónsko – DDos útok na estónsku štátnu správu. Estónci sa nevedeli elektronicky spojiť s orgánmi štátnej správy, realizovať platobné príkazy alebo získať dôveryhodné informácie o dianí v krajine. Za vinníka sa označuje Rusko.
- 2010 – Stuxnet - počítačový červ známy pod týmto názvom napadol iránske jadrové zariadenia a spôsobil ich kolaps, pričom ide o prvý známy prípad, kedy škodlivý počítačový softvér dokázal vyvolať fyzickú deštrukciu.
- 2014 – Sony – hackerom, ktorých pravdepodobne sponzorovala Severná Kórea, sa podarilo napadnúť produkčnú spoločnosť. Útok bol reakciou na film Interview, ktorý zosmiešňoval severokórejský režim a Kim Čong-una.
- 2015 – útok na OPM USA – hackeri napadli Osobný úrad federálnej vlády USA, získali osobne údaje viac ako 20 miliónov štátnych zamestnancov.
- Na Slovensku je najznámejším prípadom hacknutie Národného bezpečnostného úradu v roku 2006. NBÚ používal jednoduché heslo nbusr123, na čo chceli útočníci upozorniť.

Tretia doména, organizovaný zločin, sa v kybernetickom priestore prejavuje najmä hospodárskou špionážou. Jej cieľom je získanie prístupu k duševnému vlastníctvu a technologickým inováciám nadnárodných spoločností, ale aj štátnych inštitúcií. Kybernetickú špionáž však nevykonávajú len organizované skupiny zamerané na finančný zisk, ale aj štáty, ktoré sa takýmto spôsobom snažia získať utajené informácie, zväčša vojenského charakteru, iných štátov. Poslednou doménou je individuálny zločin, ktorého charakteristickým prejavom je hacking jednotlivcov, teda neautorizovaný prístup do cudzích počítačov, serverov alebo databáz. Motívy hackingu sú rôzne, môže

ísť o osobný prospech, snahu poukázať na bezpečnostné nedostatky alebo záujem o publicitu.

A čo Slovensko?

Slovensko po inštitucionálnej, no hlavne legislatívnej stránke, v oblasti kybernetickej bezpečnosti zaostáva. Aktuálna bezpečnostná stratégia pochádza ešte z roku 2005, a preto adekvátne nezohľadňuje zmeny bezpečnostného prostredia, vrátane kybernetickej bezpečnosti. Aj k schváleniu prvej samostatnej stratégie kybernetickej bezpečnosti došlo až v roku 2015 (Akčný plán ju doplnil v roku 2016), hoci NATO kybernetickú bezpečnosť zahrnulo do svojej agendy už na pražskom samite, ktorý sa konal v roku 2002. Vo svojej strategickej koncepcii z roku 2010 Severoatlantická aliancia uznáva, že *„moderné bezpečnostné prostredie obsahuje široký a meniaci sa súbor výziev voči bezpečnosti územia a obyvateľstva krajín NATO."*[8]

Na samite vo Varšave už NATO potvrdilo, že operácie v kybernetickom priestore budú rovnako dôležité ako vojenské akcie na zemi či vo vzduchu. Členské štáty vyhlásili kybernetický priestor za piaty operačný priestor, čím sa dostal na úroveň pozemných, leteckých, morských a vesmírnych operácií. NATO týmto krokom napodobnilo Spojené štáty. Najsilnejší štát Aliancie totiž kybernetický priestor uznal za operačnú doménu už v roku 2010. NATO po samite zverejnilo takzvaný Cyber Defence Pledge, teda záväzok pre oblasť kybernetickej bezpečnosti. V ňom vyhlasuje, že Aliancia musí držať krok s rýchlo sa meniacimi kybernetickými hrozbami a zaistiť, že členské štáty sa dokážu brániť aj v tomto priestore. Slovensko, samozrejme, ako členský štát Aliancie takisto na týchto rozhodnutiach participovalo a záväzky vyplývajúce zo samitu platia aj pre SR.

V roku 2016 kľúčový dokument prijala aj ďalšia medzinárodná organizácia, ktorej členom je aj Slovensko – EÚ schválila Smernicu pre sieťovú a informačnú bezpečnosť (NIS), ktorá by mala priniesť zvýšenie odolnosti dôležitých služieb voči online hrozbám. V súvislosti so zavedením smernice budú musieť zvýšiť úroveň zabezpečenia voči

[8] NATO. (2010). *Active Engagement, Modern Defence. Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/topics_82705.htm,* online [cit. 29.9.2016]

kybernetickým útokom poskytovatelia širokej škály základných služieb, a to v oblastiach energetiky, dopravy, bankovníctva či zdravotníctva, a digitálnych služieb, vrátane vyhľadávačov a cloudov.

Samotná slovenská stratégia kybernetickej bezpečnosti konštatuje, že *„najvážnejším problémom v oblasti kybernetickej bezpečnosti v podmienkach Slovenskej republiky je skutočnosť, že ochrana kybernetického priestoru, resp. kybernetická bezpečnosť Slovenskej republiky ešte nie sú výslovne a komplexne upravené v platnej legislatíve a existujúce kapacity a mechanizmy v oblasti bezpečnosti sietí a informácií už nepostačujú na to, aby držali krok s dynamicky sa meniacim prostredím hrozieb a aby vo všetkých oblastiach riadenia štátu a spoločenského života zabezpečovali dostatočne vysokú a najmä právne účinnú úroveň ochrany.“*[9] Kybernetické aj iné moderné hrozby budú určite zohľadnené aj v novej Bezpečnostnej stratégii, ktorá by mala byť dokončená v polovici roka 2017.

Na Slovensku pôsobí veľmi efektívny tím CSIRT.SK, špecializovaný útvar pre riešenie počítačových incidentov a slovenskí experti na kybernetickú bezpečnosť, vrátane tých vojenských, pravidelne participujú na medzinárodných tréningoch a súťažiach, kde obsadzujú popredné pozície – či už ide o cvičenia v rámci NATO (Cyber Coalition, Locked Shields – slovenský tím pod vedením Ministerstva obrany v roku 2016 toto najväčšie medzinárodné cvičenie zamerané na kybernetickú ochranu dokonca vyhral), v strednej Európe (CESP) alebo celoeurópske cvičenie Cyber Europe.[10]

To, že kybernetické hrozby sú aktuálne aj na Slovensku, dokazuje štatistika CSIRT-u, ktorý v roku 2015 prijal približne 1,5 milióna hlásení o možnom výskyte škodlivej aktivity z IP adries na území Slovenska. Najčastejšie ide o výskyt botov, ale mimoriadne populárny je ešte stále aj phishing, respektíve šírenie malvéru prostredníctvom podvodných e-mailov a falošných stránok.

[9] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 (Návrh), http://www.rokovania.sk/File.aspx/Index/Mater-Dokum-187874, online, [cit. 1.10.2016]
[10] CSIRT.SK Report 2015, https://www.csirt.gov.sk/doc/CSIRT-SK-Report-2015.pdf, online [cit. 2.10.2016]

SLOVAK SECURITY POLICY INSTITUTE
SLOVENSKÝ INŠTITÚT PRE BEZPEČNOSTNÚ POLITIKU
Na vŕšku 8
811 01 Bratislava
Slovenská republika
Tel.: (+421) (02) 4319 1592
Email: info@slovaksecurity.org
www.slovaksecurity.org

Vydal Slovak Security Policy Institute, október 2016.

Realizované s finančnou podporou Ministerstva zahraničných vecí a európskych záležitostí SR v rámci dotačného programu v oblasti medzinárodných vzťahov a zahraničnej politiky. Za obsah tohto dokumentu je výlučne zodpovedný Slovenský inštitút pre bezpečnostnú politiku.