

Kyberterorismus: Terorismus a internet

Internet je velmi silné médium. A díky tomu také velmi zranitelné. Je paradoxem, že na jedné straně je celosvětový, univerzální a ze svého principu „nalezení cesty k připojenému počítači“ téměř nezničitelný, na druhou stranu však je ve věku pokročilé digitalizace velmi zranitelný a není bezpečný. V kontextu s terorismem se tedy pojem internetová bezpečnost začal v posledních letech skloňovat ve všech pádech. Kde je však kámen úrazu?

Tvůrci ARPANETu, vojenské sítě, která dala filozoficky i reálně vznik internetu, nikdy nepočítali s tím, že by na dané síti pracoval člověk, který by měl zájem danou síť zničit, popř. poškodit. ARPANET byl interní záležitostí a jako k takovému se k němu přistupovalo (paradoxně si tak tvůrci nebyly ochotní připustit, že by snad mohlo dojít k sabotážím přímo na jednotlivých zařízeních ARPANETu přímo na území USA, což je bohužel americký trend do dnešních dní – válku na svém území zcela rezolutně vylučují).

Bohužel, rozšířením internetu mezi „prostý lid“ začíná éra postupného zabezpečování síťových protokolů a vychytávání chybiček a nepřesností v počítačové komunikaci.

Vzniká tím internet nebo dnes také vznešeně řečeno „kyberprostor“ (první definice z roku 1984), který zprostředkovává tzv. sdílené služby (e-mail, prezentace dat a informací, znalosti, přístupy, apod.). A člověk opět hledá cestu, jak dané věci zneužít ve svůj prospěch. A tak vznikl hacker – odborník-narušitel.

Filozoficky se internetový terorismus dá dělit na dva směry:

první směr je čistě propagandistický až informativní a tudíž spíše inklinuje k jakési negativní či odmítavé reakci na aktuální stavy mezinárodní či národní politické situace (propagace jednotlivých teroristických skupin, propagace ideologií, apod.).

druhý směr, který realizuje přímá napadení konkrétních počítačových sítí a likviduje služby, je výrazně nebezpečnější, neboť ve svém rozletu útočník paradoxně zničením sítě nebo její části zlikviduje i svůj operační prostor, což je z hlediska taktického jakési Pyrrhovo vítězství, ovšem z hlediska hackera je to maximální výhra (hacker v tomto směru funguje dosti podobně jako některé druhy plísni, které svou činností likvidují „sobě-ideální“ prostředí, v němž žijí a tak se zároveň fakticky zabíjejí).

Z hlediska tradičnosti se při počítačovém terorismu jedná o neletální formu útoků (nejedná se primárně o ztráty na životech, i když vyřazením důležitých systémů to není nemožné), která inklinuje spíše k nekonvenčním metodám terorismu.

Paradoxně vysokí vládní představitelé nehodlají za akty kyberterorismus přijmout nic jiného, než-li útoky vedené na infrastrukturu státu, což je z hlediska definování kyberterorismu poněkud zavádějící, neboť typické útoky jsou vedeny i na běžné uživatele internetu nebo přímo na služby, nikoliv na konkrétní firmy a podniky (i když i takový druh útoku samozřejmě také není vyloučen – viz útoky na služby update serveru Microsoft Update v roce 2005).

Podívejme se teďka na možné dělení podle potenciálních druhů útoků v rámci počítačové sítě:

přímý útok na lokální technologie – útoky vedené na infrastrukturu kritických systémů a tzv. sémantické útoky (např. defacement stránek, likvidace poštovních serverů, apod.).

souběžný útok – narušení či fyzický útok probíhající proti shodnému cíli v několika souběžných kanálech (např. narušením telekomunikační (fax, telefon, apod.) a informační struktury (internet, počítačová síť).

řízení teroristické skupiny – zneužití technologie k řízení a koordinaci činností teroristické skupiny (email, steganografie, apod.).

Samozřejmě, největším problémem při kybernetickém útoku na infrastrukturu služeb, je především finanční ztráta způsobená výpadkem a nedostupností jednotlivých služeb systémů.

Podívejme se na dělení jednotlivých metod, které jsou pro napadení v rámci kyberterorismu nejčastěji používány:

útoky na klíčové uzly počítačové sítě (internetu) – útoky na DNS servery, routery či další důležité aktivní uzlové prvky počítačové sítě.

spuštění útoků typu DoS a DoA – narušení služeb cílového systému a přebrání kontroly nad nimi (např. defacement stránek, apod.).

útok na síťové protokoly – využití slabín v síťových protokolech

fyzické napadení – umístění softwarového či hardwarového odposlechového zařízení / softwaru (malware) na cílovou stanici (do cílové sítě).

Podle analýz je možné říci, že nejčastější motivací pro kybernetické útoky je reakce na konkrétní politické situace mezinárodní nebo národní politiky. Podle dopadů lze říci, že na stabilitu a funkčnost počítačové sítě (myšleno internetu) má větší vliv právě kybernetický útok (např. šíření počítačového viru), než-li přímé destruktivní útoky (např. útok na ambasády či na WTC). Je to logické, protože kybernetický útok je z hlediska strategického použití spíše záležitostí vojenskou. Jeho ideální použití je jako souběžného útoku společně s přímou likvidací či jako přípravu pro přímou bojovou operaci (např. umlčení komunikační soustavy protivníka). Přesto i v době míru je kybernetický útok velmi nebezpečnou zbraní použitelnou k vydírání či likvidaci konkurence nebo oponenta neletální cestou (bez přímé konfrontace, nebojově). Uplatnění těchto metod a postupů je možné jak v rámci průmyslové špionáže (vytěžení informací), tak v konkurenčním boji či v rámci propagace teroristické ideologie. Nejhorší variantou je tzv. kybernetický chuligán, který je člověkem, který se snaží na svou pěst napadat informační systémy, aby tím získal slávu. Takový člověk sice nedisponuje technikou celých oddělení tajných služeb, ale zato jej žene touha po slávě, což z něho může činit nejzákeřnějšího a nejméně vyzpytaleného útočníka, protože nikdy člověk není, jaký je jeho hlavní cíl a zda použité metody nejsou pouze zástěrkou k učinění něčeho mnohem nebezpečnějšího nebo komplexnějšího.