

- globální servery
- lokální nebo distribuované servery
- firmy a organizace



NASA Ames Research Center
Mountain View, Kalifornie
1 globální server

U.S. DoD Network Information Center
Columbus, Ohio
1 globální server

NIC.CZ
Praha
servery nižší úrovně obsluhující ČR

WIDE Project
Osaka
1 globální server

- Server A VeriSign, Inc. 2 globální
- Server B Information Sciences Institute 1 globální
- Server C Cogent Communications 6 distribuovaných
- Server D University of Maryland 1 globální
- Server E NASA Ames Research Center 1 globální
- Server F Internet Systems Consortium, Inc. 2 globální, 46 lokálních
- Server G U.S. DOD Network Information Center 1 globální
- Server H U.S. Army Research Lab 1 globální
- Server I Autonomica 31 distribuovaných
- Server J VeriSign, Inc. 52 distribuovaných
- Server K RIPE NCC 5 globálních, 12 lokálních
- Server L ICANN 2 globální
- Server M WIDE Project 5 globálních, 1 lokální

Zranitelné body sítě

Při zadání webové adresy do prohlížeče prochází váš požadavek skrz systém DNS serverů. Ty mají za úkol vyhledat patřičnou adresu v síti. Úplně na vrcholku pyramidy DNS serverů stojí třináct kořenových serverů, označených písmeny A až M. Ty jsou kritické pro fungování internetu. Jejich odstavením by padla celá síť.

Právě třináct kořenových serverů tvoří páteř naší mapy. Některé z nich stojí na jediném obrovském počítači, některé se skládají z většího množství serverů na stejné úrovni. Existuje i kompromisní varianta – globální servery, podporované svými lokálními kopiemi. Tyto rozdíly reflektuje i naše mapa – globální servery značí velká, lokální a decentralizované

malá kolečka. Obecně platí, že samostatné globální servery jsou zranitelnější než decentralizované (distribuované) sítě. Posledním prvkem, který můžete na mapě najít, jsou černé čtverečky s odkazem na doménu známé firmy nebo organizace. Jde také o DNS servery, ale nižší úrovně. Na rozdíl od kořenových serverů neobstarávají celý internet, ale pouze

jeho část, navázanou na danou firmu. Úspěšný útok na všechny DNS servery, spravující danou doménu (některé firmy jich mají víc) tedy odstaví danou doménu, zbytek internetu se o útoku ani nemusí dozvědět. Při hackerském útoku na DNS server v Moskvě tak přestane fungovat doména kremlin.ru, zatímco stránky piratebay.org zůstanou nepoznáné. ■