# Jak fungují útoky DoS

S útoky typu DoS (Denial of Service – odepření služby) se lze v kybernetickém světě setkat stále častěji. O co při nich jde, jak probíhají, jak se jim bránit, jaké jsou jejich důsledky?

Útoky DoS jsou prováděny tak, že dochází k zahlcení nějaké služby či prostředku velkým množstvím požadavků. Speciálním případem jsou pak DDoS útoky (Distributed DoS), kdy dochází k napadení jednoho cíle z několika směrů. Proti takovýmto incidentům je pak nesmírně obtížná obrana – v případě jednosměrného útoku je snadné agresora „odstřihnout“, ale v případě stovek či tisíců útočníků už je to prakticky nemožné. Jedinou účinnou obranou je v takové chvíli odpojení napadeného stroje, což je ale právě stav, jehož chtěl útočník dosáhnout. DoS útoky přitom stojí komerční firmy každoročně nemalé finanční prostředky. Důvod finančního úniku je přitom dvojí. Jednak jsou to ztráty způsobené samotným útokem (ztráta dostupnosti služeb, a tím ztráta příjmů). Jednak je to nutnost analýzy vzniklých problémů a potřeba je řešit. Cílem DoS útoků jsou zpravidla velké servery jako Yahoo!, Amazon, eBay, ZDNet či CNN. Tedy servery, které jsou na trvalém připojení k internetu bytostně závislé a pro které představuje každá odstávka značné problémy.

Tyto útoky přitom nejsou vedeny snahou něco získat (finanční či jiný prospěch apod.), ale úmyslem někoho poškodit. Motivačním faktorem zde tedy není prospěch vlastní, ale neprospěch cizí. Není to však neměnným pravidlem. Ve výjimečných případech se stává, že útočník může DoS útok použít k tomu, aby donutil administrátora systém restartovat. Tím mj. může provést spuštění nějakého ovladače nebo služby. Typickým příkladem je instalace backdoor programu na servery NT/2k. Jakmile takový program chcete spustit, musíte provést jeho restart. To sice můžete provést okamžitě, ale tím na sebe také okamžitě upozorníte. Mnohem elegantnější metoda je použití útoku DoS k tomu, aby se server stal nefunkčním. První věcí, kterou potom administrátor serveru udělá, je jeho restart. Málokdy přitom pátrá, proč služba přestala odpovídat – na restarty serverů je zkrátka zvyklý.

Mezi samotnými hackery jsou DoS útoky považovány za „špinavé“ a opravdu schopní programátoři se jim jakožto podřadným vyhýbají. Narušit činnost sítě nebo znepřístupnit službu je zpravidla výrazně jednodušší, než do systému vniknout. Protokoly TCP/IP, které se dnes všeobecně po internetu používají, totiž vznikaly v době, kdy se o bezpečnosti vůbec neuvažovalo a vše bylo postaveno na vztahu důvěryhodnosti. Operační systémy, programy a služby procházely od doby svého vzniku vývojem, který toto postupně zohledňoval, a dnes již všechny programy obsahují alespoň základní bezpečnostní prvky, naproti tomu se ale právě skupina protokolů TCP/IP téměř nezměnila. Jistě existuje již verze 6, která bezpečnostní aspekty zohledňuje, ale v současné době není mnoho pádných důvodu, proč ustupovat od platného modelu IPv4, který bohužel na bezpečnost důraz příliš neklade.

Velice sofistikovaným způsobem byl proveden DDoS útok v červenci 2001 pomocí internetového červa CodeRed. Ten se šířil na serverech s instalovaným IIS (Internet Information Server). Přestože šlo o známou bezpečnostní chybu, kvůli laxnosti administrátorů zůstala nezáplatována a během velmi krátké doby dokázal CodeRed napadnout přes tři sta tisíc strojů! Mezi 20. a 27. každého měsíce se CodeRed pokoušel z napadených serverů (tedy z několika set tisíc míst!) „útočit“ na webovskou stránku www.whitehouse.gov (oficiální doména americké vlády – pozor, nezaměňovat s doménou com, což je pornografická stránka!). V daném případě bylo nutno změnit IP adresu příslušného webu, jinak by se stránka stala dlouhodobě nedostupnou.

*TOMÁŠ PŘIBYL*, AEC