STANOVISKO SAŽP

k výpadku služieb webového sídla www.obnovdom.sk dňa 9. októbra po 9:00 hod

Slovenská agentúra životného prostredia (SAŽP) v pondelok, 9. októbra zaznamenala výrazný výpadok funkčnosti webu www.obnovdom.sk, čo narušilo plynulosť generovania elektronických formulárov pre Výzvu č. 4. na predkladanie žiadostí o poskytnutie prostriedkov mechanizmu na obnovu rodinných domov. Máme za to, že výpadok bol spôsobený externým zásahom (útokom v štádiu zmarenia).

Od 7:00 začal vysoký nárast premávky (trafficu) takmer na 98% kapacity (viď graf nižšie). Keďže hrozila nedostupnosť všetkých našich služieb, pristúpili sme k obmedzeniu rýchlosti na FW na 800 Mbps pre dopytované webové sídlo. Zahltenie linky spôsobilo mimoriadny počet požiadaviek na video na webe. Približný počet požiadaviek: 300 000, v niektorých momentoch tvorili požiadavky na video cca 30% celkového počtu požiadaviek. Piatok po zverejnení videa bol počet požiadaviek 20 000 až 50 000.

Disponujeme kapacitou 1GB firewallu - a pri dosiahnutí tejto kapacity začal systém spomaľovať. Na jeden zo serverov bola okamžitá záťaž (load) 300%, pričom ostatne boli vyťažené na cca 15%. Dá sa teda predpokladať, že tento server bol pridelený zdroju incidentu, ktorý vyrábal cielenú premávku (traffic) na video, čím linku blokoval. Ďalšie dva servery však plne fungovali. Po identifikácií problému bolo video z webu odstránené a po resete servera sa dostupnosť služieb znovu obnovila.

V rámci prípravy prebehlo testovanie záťaže serverov cez simulované http požiadavky (requesty) a to v niekoľkých sériách – jedna séria po 500 dávok po 20 súčasných požiadaviek (concurrent requests). Na servery to nebola takmer žiadna záťaž. V ďalšom kroku sme preto vykonali simulovaný test dopytov (vygenerované dáta cez http „post request“, realizovaný náhodne v intervale 1-5 sekúnd), ktorý sme spustili v nedeľu ráno. Takto sme odoslali približne 4 000 žiadostí za 90 minút, servery boli vyťažené na max. 15% CPU s dostatkom voľných slotov. Považovali sme preto zvolené nastavenie za dostatočné.

Vzniknutá situácia spôsobila zahltenie a obmedzenie jedného servera, napriek tomu ďalšie

dva servery žiadosti prijímali a spracovávali ich. Do 9.25 máme uložených 544 žiadosti v databáze. Po identifikácii problému a prijatí opatrení sme začali od cca 9:30 prijímať žiadosti oveľa rýchlejšie a postupne to rástlo na úroveň 10-15 žiadostí za sekundu.

Uvedenú udalosť sme zároveň hlásili na MIRRI a NBÚ ako bezpečnostný incident.

1 Objem prenesených dát v čase