

Nevhodnosť ponechania predvolených nastavení na aktívnych sieťových prvkoch

Najväčším problémom vznikajúcim pri ponechaní predvolených nastavení je triviálna možnosť zmeny nastavení pre ľubovoľného útočníka už pripojeného do siete. Tento útok by sa nemal podceňovať pretože na Internete sa nachádzajú bežne databázy s informáciami o predvolených nastaveniach jednotlivých routerov. Po chvíli vyhľadávania bude teda útočník schopný pripojiť sa na náš router a meniť ľubovoľné nastavenia. Vďaka tomu sa môžu napríklad zamestnanci dostať na nepovolené stránky, povoliť prístup k do siete útočníkom alebo stať sa členom *Botnetu*.

Napríklad *Botnet Chucka Norrisa*¹ mohol byť uskutočnený práve vďaka nedôsledným administrátorom. Tento botnet vznikol pomocou útoku využívajúceho jednoduchý slovník zostrojený z databázy predvolených prihlasovacích mien a hesiel pre všetky routery. Botnet posielal na vybrané IP adresy prostredníctvom protokolu telnet žiadosť o prihlásenie. Po úspešnom prihlásení sa na infikovanom zariadení stiahla aktuálna verzia vírusu, zakázala vzdialená konfigurácia a spustí škodlivý kód, ktorý sa pripojí na IRC server kde získava informácie o ďalšej koordinácii. Najväčšie nebezpečenstvo takéhoto útoku spočíva v tom, že v súčasnosti neexistujú efektívne spôsoby detekcie napadnutých routerov, keďže všetka škodlivá činnosť sa odohráva na sieťovom prvku. Botnet sa potom dá použiť na útok typu *Distributed Denial of Service*² alebo *DNS Spoofing*³. Začiatkom tohto roku bola odhalená ďalšia veľká sieť vo veľkosti zhruba 300 000 zariadení, ktoré boli už prekonfigurované na útočníkmi ovládané DNS servery.

Nevhodné sa ukázalo aj ponechanie predvolených *SSID*⁴ kde sú známe útoky špecifické pre niektoré typy routerov umožňujúce prevzatie kontroly bez znalosti hesla. Napríklad router s označením Netgear N600 Wireless Dual-Band Gigabit Router (WNDR3700v4) dovoľí po návšteve stránky s adresou `http://<router_address>/BRS_02_genieHelp.html` prístup do administrácie bez prihlásenia.

Pre úplnosť uvádzam zoznam opatrení, ktorých dodržiavaním môžeme znížiť pravdepodobnosť úspešného útoku:

¹ Jeho názov je podľa komentára v zdrojovom kóde, ktorý po preklade z taliančiny znamená: „V mene Chucka Norrisa“. Tento botnet bol objavený práve na našej Univerzite viď odkaz http://www.muni.cz/ics/research/projects/4622/web/chuck_norris_botnet

² *DDoS* je technika útoku na internetové služby, pri ktorej dochádza k zahlteniu siete alebo nefunkčnosti či nedostupnosti služby pre ostatných užívateľov.

³ *DNS Spoofing* je technika útoku pri ktorej sa zamení IP adresa pre doménu (napríklad namiesto stránky našej banky nám útočník podvrhne ním vyrobený klon).

⁴ *Service Set Identifier* je jedinečný identifikátor každej bezdrôtovej počítačovej siete.

1. zmeniť SSID na ľubovoľné slovo mimo identifikácie typu routru,
2. zmeniť predvolené heslo na nejaké silné heslo (ideálne aj mena ak to router umožňuje),
3. zakázať vzdialenú konfiguráciu,
4. nepoužívať predvolený rozsah IP adries,
5. okamžite sa odhlásiť z administrácie po ukončení konfigurovania ⁵.
6. udržiavať aktuálny firmware v routri,
7. pravidelná kontrola nastavení DNS v routri.

Slavomír Krupa

⁵ Znižuje pravdepodobnosť útoku *Cross-site request forgery*.