УДК 004.7.056.53

Р. Козак
(Тернопільський національний технічний університет імені Івана Пулюя)

БЕЗПЕКА БЕЗПРОВІДНОГО ПЕРИМЕТРА КОМП'ЮТЕРНОЇ МЕРЕЖІ

Діяльність більшості бізнес-компаній безперечно залежить від доступності мережних інформаційних ресурсів, доступ до яких все частіше реалізують з допомогою безпровідних технологій, незважаючи на пов'язані з цим додаткові загрози інформаційній безпеці (ІБ).

У технології бездротових мереж нині застосовують три механізми захисту: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) і WPA2. У свою чергу WPA і WPA2 можуть використовуватися із закритим ключем Pre-Shared Key (WPA-PSK) та з аутентифікацією 802.1 X. У 2004 році WEP було визнано застарілим та таким, що не рекомендується для використання навіть у домашніх мережах, однак і надалі стає причиною проникнення в периметр бездротових корпоративних мереж.

Під час атак на з'єднання WPA та WPA2 використовують практично однакові алгоритми, які відрізняються лише окремими елементами на різних стадіях виконання. Проте WPA містить декілька архітектурних вразливостей, що суттєво знижують його надійність у порівнянні з WPA2 та дають змогу виконувати деякі типи атак, результат яких не залежить від довжини та складності загального ключа PSK. У той же час для WPA2 відомою є лише одна архітектурна вразливість, виявлена у 2010 році – Hole 196. Вразливість отримала назву «інсайдерська» оскільки для її використання зловмисник і жертва мають бути автентифіковані в одній бездротовій мережі, а тому Hole 196 не може бути використана для підключення до мережі.

Надійність захисту від несанкціонованого підключення в сукупності із загальним закритим ключем (WPA2-PSK) прямо пропорційна складності й довжині вибраного ключа та імені мережі (SSID). У такому випадку зловмиснику потрібно дочекатися моменту підключення клієнта до бездротової мережі й перехопити дані аутентифікації, а саме так зване «рукостискання» (handshake), яке містить результат необоротного криптографічного перетворення SSID й PSK. Далі залишається здійснити атаку перебору по словнику.

Найчастіше рекомендують такі заходи щодо зниження ризиків проникнення в корпоративну мережу через її безпровідний периметр:

- використання унікального SSID;
- використання складних ключів, довжиною не менше 10 символів (в ідеальному випадку – випадковий набір символів, що містить заголовкові й прописні літери, цифри і розділові знаки, виключення клавіатурних послідовностей);
- регулярна заміна ключів;
- проведення періодичних тестів на проникнення;
- використання WPA-Enterprise у комплексі з WIDS та процесами моніторингу подій ІБ й реагування на інциденти ІБ.

Усі існуючі нині технології захисту безпровідних мереж піддаються певним типам мережних атак. Для ефективного зниження ризику проникнення в корпоративну мережу через безпровідний периметр недостатньо застосовувати лише технічні механізми захисту. Для їх підтримки важливо організовувати процеси моніторингу подій ІБ та реагування на інциденти ІБ, що має стати частиною комплексної системи управління інформаційною безпекою компанії.