Безпека маршрутизаторів для малого офісу та дому (SOHO)

Створено 07.2014 CERT-UA
Іван Соколов

Введення

Домашні маршрутизатори (SOHO) стали невід'ємною частиною сучасного суспільства також, як користування Інтернетом. Вони увійшли у бізнес, домашній побут, шкільне навчання, соціальні зв'язки, підприємства і фінансовий менеджмент. Провідні (wired) та безпровідні (wireless) маршрутизатори (router) тепер є майже у кожного вдома, забезпечуючи зв'язок. Інтернет-сервіс-провайдери (ISP) продають ці пристрої зазделегідь сконфігурованими та готовими до використання.

Користувачі, зазвичай, застосовують їх відразу ж після придбання, підключаючись до Інтернету без виконання попереднього (або будь-якого) налаштування. Вони можуть не знати, як виконати додаткову конфігурацію, оскільки вона здається занадто складною, або вони не можуть витратити занадто багато часу для “продвинутих” налаштувань.

На жаль, налаштування за замовчанням (default configuration) у більшості маршрутизаторів надають лише мінімальний рівень безпеки, який залишає домашні мережі незахищеними та вразливими до атак. Малий бізнес та організації, які економлять на інформаційно-комунікаційному забезпеченні своєї інфраструктури та службі підтримки, часто використовують такі ж самі домашні маршрутизатори для підключення до Інтернету. Ці організації також часто встановлюють маршрутизатори без виконання на них безпечних налаштувань і, таким чином, піддають себе ризикам атак.

Питання безпеки

Налаштування за замовчанням більшості маршрутизаторів менш безпечні. Домашні маршрутизатори, зазвичай, доступні напряму з Інтернету, легко знаходяться та вивчаються. Ці характеристики дозволяють потенційному зловмиснику реалізувати майже ідеальний вектор атаки. Бездротові (wireless) функції, які інтегровані у більшість таких пристроїв, також додатково надають ще декілька векторів атак.

Попередження

Кроки з попередження, наведені нижче, розроблені для підвищення безпеки домашніх маршрутизаторів та зниження вразливості внутрішніх мереж проти атак ззовні:

• **змініть налаштування за замовчанням (пароль, ім'я адміністратора, текст запрошення)**: виробники встановлюють однакові імена та паролі для однакових пристроїв при виробництві та початковому конфігуруванні. Ці логіни/паролі зазделегідь викладені в відомих для зловмисників публікаціях. Проте, їх можна швидко змінити у ході початкового налаштування маршрутизатора. Рекомендуємо використовувати пароль з більш ніж 16 символів (чим більше — тим краще!), які є комбінацією літер та цифр. Також, змінюйте паролі кожні 30-90 днів.

• **змініть SSIDза замовчанням - унікальне ім'я вашої бездротової мережи (WLAN).** Всі бездротові пристрої у WLAN повинні користовуватись одним і тим самим SSID для взаємодії один з одним. Виробники встановлюють SSID за замовчанням, який зазвичай типово ідентифікує виробника або певний пристрій. Атакуючий може використати якусь відому для цього пристрою вразливість. Іноді користувачі встановлюють SSID, який ідентифікує їхню організацію, місце розташування, власне ім'я, тощо. Це робить простішим для атакуючого ідентифікувати по SSID їх специфічне заняття, домашню мережу або прізвище. Наприклад, SSID, який усім повідомляє широкомовно (broadcasts) ім'я компанії — більш приваблива ціль, ніж та, коли маршрутизатор повідомляє “ABC123”. Коли обираєте SSID, слідуйте наступним порадам по забезпеченню парольної політики:

- мінімальна довжина SSID повинна бути біль ніж 8 символів.
- використовуйте змішані цифрові та літерні SSID.

- періодично змінюйте SSID (наприклад, шляхом повторів деякої частини) та виключіть використання попередніх паролів.

• **Оберіть алгоритм шифрування WPA2-AES для конфіденційності даних:** часто-густо за замовченням встановлюється інший алгоритм, Wireless Equivalent Privacy (WEP), який забезпечує певну конфіденційність (автентифікація та криптографічний захист) але має серйозні вразливості. WEP був презентований у стандарті 802.11 ще у 1997 році. Алгоритм Wi-Fi Protected Access (WPA) більш надійний. У 2004 році він отримав найновішу версію — WPA2 з алгоритмом шифрування AES. WPA та WPA2 надають більш стійку автентифікацію та криптографічний захист, використовуючи динамічно змінювані ключі. WPA та WPA2 мають персональну та корпоративну версії. Персональна, що також зветься WPA-PSK (Pre-Shared Key), була розроблена для домашнього та офісного вжитку, та підтримує попередньо розподілені ключі, без серверу автентифікації. Використовуючи WPA-PSK, встановіть довгий ключ (pre-shared key) та періодично змінюйте його. Корпоративна версія WPA-Enterprise потребує серверу автентифікації RADIUS, протокол розширюваної автентифікації Extensible Authentication Protocol (EAP), а також надає більший захист. Проте, таке рішення потребує залучення додаткового бюджету та технічних спеціалістів. WPA2 підтримує шифрування за протоколом AES 128-біт. Цей протокол дозволений для використання в державних установах США та деяких інших країн. WPA2 з AES являє собою найбільш безпечний з доступних у маршрутизаторах для дому і офісу варіант. Якщо WPA2 не доступний, кращим варіантом буде WPA.

Якщо ваш старий маршрутізатор підтримує лише WEP, обирайте у налаштуваннях 128-бітний ключ, та створить якомога довший пароль адміністратора роутера.

• **обмежте зону покриття WLAN:** LAN'и за своєю природою більш безпечні, ніж WLAN'и, оскільки підключення до них може відбутися лише у приміщенні, де вони розташовані. WLAN зазвичай розповсюджуються за периметр офісу та дому (контрольовану зону). Це дозволяє зловмиснику підслуховувати Вашу мережу ззовні, без вашого відома. Саме тому розташування антени, її тип та сила сигналу — важливі для вирішення

питання. Обмежте зону розповсюдження сигналу Вашого WLAN. Центрально розташована (рівновіддалена) антена — найбільш вдалий варіант у більшості випадків. Якщо це можливо, то зробіть направлену антену для певного WLAN з обмеженими силою та площею покриття за допомогою конусу з металевої фольги).

• **виключайте мережу, коли вона не використовується:** важливою опцією безпеки бездротових маршрутізаторів є виключення мережі, коли вона не використовується. Це значно ускладнює несанкціоноване втручання ззовні. Не обов'язково вмикати/вимикати пристрої часто, проте це доцільно робити у подорожах та під час тривалих періодів перебування у оффлайні.

• **вимкніть UPnP:** Universal Plug and Play (UPnP) — технологія, яка корисна при підключенні мережевих пристроїв до інших шляхом пошуку і встановлення з'єднання. Оскільки UPnP спрощує початкову мережу конфігурацію, вона також несе ризик безпеки. Наприклад, шкідливе програмне забезпечення в Вашій мережі може використати UPnP для відкриття “дірок” у файрволі Вашого маршрутизатору для надання можливості входження зловмисникам. Тому, відключайте UPnP, якщо не користуєтесь пристроями, які його підтримують.

• **оновлюйте програмне забезпечення:** також, як і у випадку з персональними комп'ютерами, програмне забезпечення маршрутизаторів (routers firmware) потребує оновлень та патчів (patch). Багато оновлень закривають вразливості безпеки, які можуть виникати у мережі.

• **використовуйте статичні IP-адреси або обмежуйте зарезервовані адреси DHCP серверів:** більшість маршрутизаторів зконфігуровано у режимі серверів Dynamic Host Configuration Protocol (DHCP). DHCP виконує конфігурацію клієнтських пристроїв шляхом простого конфігурування їх мережевих налаштувань (IP-адрес, шлюзів (gateway), DNS, тощо). Також, це дозволяє користувачам неконтрольовано отримувати IP-адреси з Вашої мережі. Відключення DHCP та конфігурування клієнтів вручну — найбільш безпечний варіант, але більш складний для великих мереж. Якщо використовуєте DHCP, обмежте

кількість IP-адрес у пулі DHCP. Це може обмежити кількість користувачів, включаючи потенційно неавторизованих користувачів, що можуть підключитись до Вашої мережі.

• **вимкніть віддалене управління:** вимкніть цю опцію для захисту від спроб встановлення з'єднання з маршрутизатором та його конфігурування через інтерфейс wide area network (WAN).

• **вимкніть віддалене оновлення:** ця можливість, якщо можлива, дозволяє маршрутизатору слухати на інтерфейсі WAN трафік TFTP, який може потенційно скомпрометувати його програмне забезпечення. Тому, краще вимкнути цю можливість.

• **вимкнути DMZ:** демілітарізовані зони (DMZ) створюють ізольовану мережу, яка відокремлена від Інтернету та дозволяє реалізувати окрему політику безпеки і надати доступ до Інтернету тим, хто його потребує (web-сервери, тощо.). Вимкніть цю опцію, якщо вона непотрібна. Користувачі або адміністратори іноді використовують її для проведення обслуговування та забувають вимкнути, залишаючи активною. Для цієї опції рекомендуємо використовувати файрвол.

• **вимкніть непотрібні сервіси:** як і в будь-якій комп'ютерній системі, вимкніть непотрібні сервіси для зниження загроз їх зламу.

• **вимкніть ping (увімкніть stealth mode):** ping — можливість зазвичай вимкнена за умовчанням. Коли ця опція активована, розпізнавання маршрутизатора ззовні стає простішим, оскільки він починає відповідати на ping-команди, надіслані з Інтернету. Проте, деактивація цієї можливості не унеможливить несанкціонований доступ, а тільки зробить його більш складним. Але краще все ж вимкніть.

• **включіть файрвол маршрутизатора:** більшість файрволів має таку можливість. Впевніться, що ця можливість активована і обережно налаштована для того, щоб дозволити тільки авторизований доступ користувачам та сервісам при доступі до мережі.

• **активуйте stateful packet inspection (SPI) на маршрутизаторі**, якщо ця функція доступна. SPI розширює можливості маршрутизатора інспектуванням пакетів даних для визначення легітимного та нелегітимного трафіку. Інша можливість домашніх маршрутизаторів — створення білих та чорних списків контролю доступу (whitelists/blacklists) для дозволу/блокування списків веб-сайтів/сервісів/тортів/т.і. Зауважте, що вбудований у маршрутизатор фаервол, не перешкоджає користувачам, які знаходяться у зоні покриття Вашого маршрутизатора, намагатись приєднуватись до Вашої wifi-мережі.

• **журналювання:** активуйте журналювання та періодично переглядайте журнали, шукаючи важливі події, що стосуються втручань, спроб, атак, тощо. Навіть якщо Ви не розумієте логів, вони допоможуть технічним спеціалістам вирішити Ваші проблеми.

• **відстежуйте wireless трафік:** слідкуйте та ідентифікуйте будь-яке неавторизоване використання Вашої мережі шляхом перегляду журналів пристроїв, які підключались до маршрутизатора. Якщо ідентифіковано невідомий пристрій, треба налаштувати для нього фільтрацію по MAC-адресах або правила фільтрації файрволу. Для більш детальної інформації використовуйте документацію маршрутизатора (вона, зазвичай, постачається разом з пристроєм, або є на сайті виробника).

• **увімкніть фільтрацію за MAC-адресою:** дозвольте використання бездротової мережі лише обраним переліком приладів з унікальними ідентифікаторами активного мережевого обладнання - MAC-адресами. Для формування такого переліку увімкніть всі прилади, знайдіть їх у переліку підключенного обладнання у налаштуваннях роутеру, перепишіть їх MAC-адреси, та додайте їх у перелік виключно дозволених у відповідному меню налаштувань роутера.

• **робочі станції адміністраторів:** будьте впевнені, що робоча станція адміністратора маршрутизатора знаходиться у довіреному сегменті мережі і неможливі спроби розвідки (sniffing) керуючих даних та збору інформації про мережу.

• **відключіть bridging та використовуйте network address translation (NAT):** домашні маршрутизатори відділяють внутрішню мережу від Інтернету за допомогою трансляції мережевих адрес (NAT). NAT забезпечує приватні IP-адреси для всієї Вашої мережі і ніхто, маючи адресу з публічного діапазону IP-адрес (наприклад, з Інтернету), не зможе напряму підключитись до локальної мережі або сканувати її. IP-адреса зовнішнього інтерфейсу маршрутизатора приховує внутрішні IP-адреси локальної мережі, розташовані під нею, і це — додатковий захист.

• **деякі маршрутизатори мають можливість роботи у режимі моста (bridge) між двома мережами.** Ця можливість також може бути використана для під'єднання сегментів або пристроїв у одній внутрішній мережі (intranet) до Інтернету, використовуючи зовнішню IP-адресу маршрутизатору. Відключіть цю опцію, якщо вона не потрібна, щоб знизити спектр атак на маршрутизатор.

Майте на увазі, що це тільки рекомендовані кроки, які дозволять потенційно допомогти у захисті офісних та домашніх маршрутизаторів. Виконання цих кроків може бути неможливим для Вашої мережі або у Ваших умовах. Якщо необхідна додаткова допомога, звертайтесь до виробника Вашого маршрутизатора або до довідкових матеріалів у Інтернеті за тегами:

- Securing WLAN's using 802.11i
- Using Wireless Technology Securely
- Home Wireless Security

Приклади корисної літератури:

1. https://education.alberta.ca/media/822010/wirelessbestpracticesguid.pdf
2. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Wireless_80211i_Rec_Practice.pdf