

NÂNG CẤP BẢO MẬT MẠNG KHÔNG DÂY

Bạn có nghĩ rằng mạng không dây (wireless network) mà mình đang sử dụng thật sự an toàn không? Tốt hơn hết bạn nên xem xét lại vấn đề này. Chuẩn bảo mật Wi-Fi mới nhất, có tên là Wireless Protected Access 2 (WPA2), bổ sung khả năng mã hóa dữ liệu ở m

Bạn có nghĩ rằng mạng không dây (wireless network) mà mình đang sử dụng thật sự an toàn không? Tốt hơn hết bạn nên xem xét lại vấn đề này. Chuẩn bảo mật Wi-Fi mới nhất, có tên là Wireless Protected Access 2 (WPA2), bổ sung khả năng mã hóa dữ liệu ở mức chuyên nghiệp, đã xuất hiện cách đây hơn 1 năm nhưng hầu hết người dùng vẫn không sử dụng chuẩn này. Thực tế cho thấy WPA2 đáng để cài đặt vì chuẩn bảo mật WPA trước đây có thể dễ dàng bị "bẻ khóa", trừ khi bạn sử dụng một mật khẩu với độ dài hơn 20 ký tự và không được ghép lại từ những từ có thể dễ đoán. Trong khi người anh của WPA là chuẩn bảo mật Wired Equivalent Privacy (WEP) vẫn còn được sử dụng, dù chỉ an toàn hơn chút ít so với khi không sử dụng một biện pháp bảo mật nào. WEP có thể bị bẻ khóa chỉ trong vòng vài giây bất kể độ phức tạp của khóa (key) mà bạn đặt ra. Nếu mục tiêu bảo mật của bạn chỉ là ngăn chặn người dùng khác kết nối vào mạng thì WEP đáp ứng được yêu cầu đó. Tuy nhiên, nếu muốn bảo vệ nghiêm ngặt dữ liệu cá nhân của mình, tốt nhất bạn nên áp dụng WPA2. Trước khi bổ sung khả năng bảo mật WPA2 vào mạng, bạn phải tải về và cài đặt hotfix nâng cấp WPA2 cho Windows XP. Ngoài ra, bạn cũng cần cài đặt phiên bản mới nhất cho trình điều khiển thiết bị (driver) của card mạng không dây từ website của hãng sản xuất. Website Windows Update của Microsoft thường liệt kê những cập nhật trong mục "Hardware, Optional". Lưu ý, bạn chỉ thấy được tùy chọn này khi sử dụng Windows có bản quyền. Tiếp đến, tải về và cập nhật firmware mới nhất cho bộ định tuyến không dây (router) từ website của hãng sản xuất (tham khảo danh sách sản phẩm hỗ trợ WPA2 tại đây). Nếu router đang sử dụng quá cũ để cập nhật WPA2/WPA thì tốt nhất bạn nên thay mới vì thiết bị mới có giá khá rẻ, khoảng 35 USD. Sau khi chuẩn bị đầy đủ, bạn hãy sử dụng một trình duyệt để vào trang web quản trị của router (xem tài liệu hướng dẫn đi kèm thiết bị để biết chính xác cách thực hiện) và thay đổi chế độ bảo mật mặc định sang WPA2 Personal: chọn thuật toán WPA là TKIP+AGES và nhập vào mật khẩu ở mục WPA Shared Key (Hình 1). Mật khẩu có thể gồm các ký tự chữ cái và số, với chiều dài tối đa là 63 ký tự. Ở các lần đăng nhập sau, hệ thống sẽ nhắc nhở bạn cần nhập mật khẩu WPA Shared Key.

Hình 1: Thiết lập tính năng bảo mật WPA2 cho router/gateway.

BẢO MẬT TỰ ĐỘNG Mặc dù Windows 2000 và các phiên bản Windows trước đây không hỗ trợ tính năng bảo mật WPA2 nhưng bạn vẫn có thể bảo vệ an toàn mạng không dây của mình với sự trợ giúp từ một số công cụ hữu ích.

Hình 2: Bảo vệ mạng không dây an toàn với tiện ích Wireless Home Network Security của McAfee. McAfee Wireless Home Network Security (80 USD) là phần mềm có thể cấu hình bảo mật Wi-Fi cho nhiều gateway không dây và hỗ trợ đến 3 mạng máy (Hình 2). Hãng này liệt kê danh sách thiết bị mà chương trình này hỗ trợ tại địa chỉ www.mcafee.com/router. Dù chưa hỗ trợ WPA2 nhưng phần mềm này có thể khắc phục một số nhược điểm của chuẩn WPA (chẳng hạn sử dụng khóa tĩnh nên dễ bị bẻ khóa hơn). Chương trình tự động tạo ra và xoay vòng qua các khóa mới trên bất kỳ máy tính nào trong mạng và trên chính gateway. Ngoài ra, một cách khác để kiểm tra tính bảo mật của mạng không dây là sử dụng tiện ích miễn phí Netstumbler của Marius Milner. Netstumbler không chỉ giúp bạn xác định được những "lỗ hổng" bảo mật trên mạng mà còn phát hiện nguồn gốc của hiện tượng nhiễu sóng cũng như nhận biết những khu vực có tín hiệu sóng

