

MẠNG KHÔNG DÂY CÓ BẢO MẬT?

Thanh toán tín dụng trên ĐTDD, tính cơ động vượt trội và những cuộc gọi wi-fi là viễn cảnh tươi sáng của Internet không dây. Nhưng hiện có nhiều nguy cơ mới nảy sinh gắn liền với đột phá này. Một thế giới vô tuyến đang hình thành và tất nhiên

Thanh toán tín dụng trên ĐTDD, tính cơ động vượt trội và những cuộc gọi wi-fi là viễn cảnh tươi sáng của Internet không dây. Nhưng hiện có nhiều nguy cơ mới nảy sinh gắn liền với đột phá này. Một thế giới vô tuyến đang hình thành và tất nhiên hãy còn chưa ổn định. Khi chúng ta tăng tốc các cuộc liên lạc trong những ngày cao điểm, bạn và tôi chắc chắn khó tránh khỏi sự tấn công của các dịch vụ quảng cáo và thương mại trên mạng không dây. Nguy cơ Trước hết đó là nguy cơ về những hacker kỹ thuật số. Mặc dù vấn đề này đã không ngừng gia tăng trong suốt thập kỷ qua khi mà ngày càng nhiều thông tin cá nhân được lưu trữ trên các thiết bị di động và kết nối Internet hữu tuyến. Và hiện nay, mạng Internet không dây đã cộng thêm nhiều phức tạp vào mớ hỗn độn này. Hôm 26-10 vừa qua, sân bay quốc tế Hartsfield-Jackson ở Atlanta, Mỹ đã khai trương dịch vụ Wi-Fi (wireless fidelity), khiến nơi đây trở thành điểm truy cập Internet di động lớn nhất tại Mỹ. Bất cứ ai có một laptop (máy tính xách tay) cũng có thể kết nối liên lạc dễ dàng với mạng Internet toàn cầu. Mặc dù chuyên gia Kirsten Tagami cho biết người sử dụng có thể an tâm khi truy cập vì đã có những bức tường lửa (firewall) và các hỗ trợ an ninh bổ sung, song các rủi ro lại rất cao, đặc biệt khi những đối tượng sử dụng kết nối liên lạc thương mại thường biết rất ít về các thao tác và kỹ xảo phần mềm này. Tại bất cứ điểm truy cập Internet không dây nào, người sử dụng cũng có thể bị "phơi nhiễm" với các nguy cơ an ninh. Đó cũng là nguyên nhân hồi đầu năm, Công ty An ninh mạng nội hạt AirDefence có kế hoạch tập trung vào điểm yếu này bằng việc kiểm tra những lỗ hổng dễ tổn thương của các điểm truy cập không dây. Trong chiến dịch củng cố an ninh mạng, các chuyên gia của AirDefence có thể log on dễ dàng vào mạng không dây của một khách sạn hay công ty và có thể khai thác các thông số khi có cuộc trao đổi qua mail. Họ cũng đột nhập vào bất cứ hệ thống liên lạc nội bộ nào khi có đối tượng truy cập. Giữ liên lạc liên tục là thế mạnh của thời đại công nghệ thông tin, và chiếc ĐTDD không chỉ đơn thuần là phương tiện để bạn trao đổi thông tin, mà thậm chí đã trở thành người bạn tri kỷ của nhiều người. Nó lưu giữ nhiều thông tin của chủ nhân và các đối tượng giao lưu, từ số thẻ tín dụng, tài khoản ngân hàng cho đến các thông tin cá nhân của bạn bè, người thân. Thế nhưng, các hacker có thể đột nhập dễ dàng và lấy cắp các thông tin này. Và giải pháp Câu trả lời gói gọn trong 3 từ: thiết kế (design), điều chỉnh (regulate) và giáo dục (educate). Các biện pháp an ninh mà khách hàng có thể dễ dàng thao tác nên được thiết kế kỹ lưỡng và cần có sẵn trong bất cứ thiết bị kết nối không dây nào. Điều này cực kỳ quan trọng đối với những nhà thiết kế giải pháp an ninh mạng. Chẳng hạn như Công ty BellSouth mới đây đã khai trương một số dịch vụ không dây ở những điểm truy cập có chọn lựa thuộc bang Georgia (Mỹ). Dự án Internet không dây tốc độ cao cũng đang được họ nhắm đến khu vực New Orleans, nơi hạ tầng cơ sở thực sự khó khăn cho mạng Internet hữu tuyến sau cơn bão Katrina. Đặc biệt, BellSouth đang nhắm đến vấn đề an ninh cao nhất theo những cách khác nhau, như ứng dụng công nghệ tiên tiến để truyền thông số trực tiếp từ máy tính của khách hàng đến các trạm quản lý chính của BellSouth, sử dụng mã số nhận diện duy nhất của đối tượng đăng ký truy cập và sản xuất các trang thiết bị được thiết kế chuyên dụng chỉ thích hợp duy nhất cho mạng BellSouth. Cuối cùng, điều không kém phần quan trọng khác là khuyến cáo các nhà cung cấp mạng không dây và khách hàng về nguy cơ này. Và, người ta cũng kỳ vọng nhiều vào kế hoạch hành động nhằm kiểm soát các nguy cơ an ninh cho mạng Internet không dây khi hội nghị thượng

đỉnh về an ninh mạng vô tuyến sẽ diễn ra tại Trung tâm An ninh công nghệ thông tin Georgia vào ngày 15-11 tới đây... Đ.Nguyên Hùng