HACKER BỊ TRUY NÃ... DẠY CÁCH BẢO MẬT

Một hacker Anh sắp bị dẫn độ sang Mỹ do tội xâm nhập vào mạng máy tính quân sự của Mỹ tuyên bố : các nhà quản trị đã hoàn toàn thất bại trong việc phát hiện những vụ đột nhập ngoài ý muốn. Thành tích "bất hảo"

Một hacker Anh sắp bị dẫn độ sang Mỹ do tội xâm nhập vào mạng máy tính quân sự của Mỹ tuyên bố : các nhà quản trị đã hoàn toàn thất bại trong việc phát hiện những vụ đột nhập ngoài ý muốn. Thành tích "bất hảo"

Nguồn: AFP

Gary McKinnon, phát biểu trong hội thảo Infosec Europe 2006, đã sơ sẩy khi tấn công vào một trong những mục tiêu quan trọng, dẫn tới một cuộc điều tra trên quy mô toàn cầu. "Tôi bị túm vì đã sử dụng một công cụ điều khiển từ xa bằng đồ hình và quên mất múi giờ của mình. Ai đó đã ở trong văn phòng và nhìn thấy con trỏ chuột di động trên màn hình", Gary nhún vai. Vụ việc bắt đầu bị điều tra sau khi người ta phát hiện thấy nhân viên đã về hết mà máy tính vẫn bật và vận hành. "Nếu tắt máy tính vào ban đêm thì sẽ giảm thiểu nguy cơ (bị tóm) hơn", McKinnon cho biết. Vào ngày 10/5 tới đây, tòa án London sẽ quyết định có đáp ứng yêu cầu dẫn độ từ phía Mỹ hay không. McKinnon, một hacker rất có hứng thú với UFO, có thể sẽ bị kết án vì tội xâm nhập trái phép vào mạng máy tính của Lầu năm góc, quân đội, Hải quân, Không quân Mỹ và NASA, cài đặt các công cụ quản trị từ xa và truy cập nhiều file bí mật trong cơ sở dữ liệu. McKinnon (đang trong thời gian bảo lãnh tại ngoại) đã đến tham dự Hội thảo cùng Robert Schifreen, một cựu hacker có tên tuổi khác của Anh. Schifreen và bạn là hai hacker đầu tiên trên thế giới phải ra hầu tòa vị tội hack máy tính, sau khi xam nhập vào mạng của tập đoàn BT Group hồi giữa thập niên 80. Tuy nhiên, theo Schifreen, hacking chỉ là một trong rất nhiều nguy cơ mà ngành bảo mật máy tính phải đối mặt, bên cạnh thư rác, phishing và lừa đảo thẻ tín dụng. "Bất chấp những lời có cánh Microsoft quảng cáo về Vista, tội phạm mạng, hacking và lừa đảo vẫn sẽ tiếp diễn. Không có một sản phẩm đơn độc nào có thể đuổi chúng đi được".

Người dùng là mắt xích yếu nhất Người dùng chính là mắt xích yếu nhất, Schifreen nói. Ai cũng

sơ hở và có khả năng bị sập bẫy social engineering (kỹ năng tán gẫu, à ơi của các hacker) và không có bất cứ sản phẩm bảo mật nào có thể bảo vệ được họ khỏi nguy cơ này. USB cũng ngày càng trở thành mối hoạ tiềm tàng, khi mà các nhân viên xấu bụng có thể copy lại cơ sở dữ liệu vào một USB dung lượng lớn kiểu như ổ cứng của iPod và tuồn ra ngoài. Tuy nhiên, các nhà quản trị mạng cũng có thể thực hiện một số biện pháp đã giảm bớt nguy cơ. McKinnon, người thường xuyên chỉnh sửa các tệp tin sổ ghi (log file) bên trong những máy tính mà anh ta đã đột nhập, cho biết tốt nhất, log file nên được lưu trong máy chủ offsite. Ngoài ra, cơ chế thẩm quyền truy cập vào file này cũng phải cực kỳ chặt chẽ. Tuy nhiên, các tệp tin sổ ghi chỉ hiển thị được những gì xảy ra sau vụ đột nhập, khi mà đã quá muộn để hành động, Bob Ayers, cựu giám đốc chương trình Nâng cao bảo mật của Bộ Quốc phòng Mỹ nhận định. Ngoài người dùng, mật khẩu cũng là một mắt xích yếu thường trực. McKinnon có thể dễ dàng vượt qua những mật khẩu không có cơ chế bảo vệ tốt do các nhà quản trị đã làm không tròn phận sự khi định cấu hình. Theo McKinnon, hàng rào phòng thủ đầu tiên chính là hệ điều hành. Với Windows, điều này có nghĩa là bạn phải kích hoạt các phần mềm diệt virus và tường lửa, cũng như tắt máy chủ Register. Ayers thì nói rằng bảo mật dựa vào con người nhiều hơn là công nghệ. "Hãy thuê và giữ chân nhà quản trị hệ thống giỏi nhất mà anh tìm được bằng mọi cách", ông nói. Thiên Ý