TỘI PHẠM TIN HỌC VIỆT NAM DỄ BẮT, KHÓ XỬ

Toàn b

Toàn bộ các cuộc tấn công trên mạng trong năm 2006 đều được làm rõ, nhưng thủ phạm chỉ bị xử lý hành chính với mức tiền phạt 10-20 triệu đồng. Các cơ quan chức năng "phàn nàn" rằng hạn chế của luật pháp khiến họ khó khăn trong việc bảo vệ trật tự kỷ cương trong không gian Internet.

Tại cuộc hội thảo về các hành vi vi phạm, tội phạm trong thương mại điện tử (TMĐT) do Bộ Thương mại tổ chức ngày 10/11 ở Hà Nội, đại diện đơn vị chống tội phạm công nghệ cao của C15 (Bộ Công an) cho biết Luật Hình sự ban hành năm 1999 có 3 điều khoản (224, 225 và 226) điều chỉnh những hành vi trên Internet nhưng hầu hết đã lỗi thời. Các công cụ pháp lý khác cũng chỉ dừng lại ở mức độ xử lý hành chính. Sự phát triển của Internet trong thời gian qua đòi hỏi những quy định mới.

Thiếu luật, cơ quan chức năng như bị "trói tay" khi đảm bảo an ninh cho TMĐT. Ảnh: Hưng Hải.

"Quy định hiện hành rất khó truy cứu trách nhiệm hình sự đối với tin tặc", ông Trần Ngọc Hoà, Trưởng phòng chống tội phạm công nghệ cao thuộc C15 nói. "Luật quy định việc phá hoại gây 'hậu quả nghiêm trọng', hoặc từng bị kỷ luật, xử lý hành chính rồi mà tái phạm mới bị truy cứu trách nhiệm hình sự. Nhưng trên môi trường Internet yếu tố này rất khó xác định vì sự quan trọng của thông tin chứa trong máy tính hoặc mạng máy tính khó có thể đo đếm được". Ông Hoà cho biết nhiều nước quy định nếu truy cập trái phép vào máy tính người khác là đã có thể bị xử lý hình sự, bất kể việc đó đã gây ra thiệt hại gì cho chủ nhân hay chưa. Nhưng Việt Nam vẫn còn thiếu cả những quy định đến việc bảo vệ hệ thống thông tin quan trọng của chính phủ, quân đội, an ninh,

bưu điện…

Theo ông Đỗ Ngọc Duy Trác, Trưởng phòng nghiệp vụ Trung tâm ứng cứu sự cố máy tính quốc gia (VNCERT), môi trường Internet tại Việt Nam hiện nay có nhiều yếu tố gây mất an toàn. Tại đây không có cơ chế định danh người dùng, khó kiểm soát các giao tiếp và thiếu sự phối hợp, giám sát giữa các tổ chức quản lý Internet. Ở Việt Nam có một kỹ thuật giả mạo địa chỉ mạng (fake IP) suốt 20 năm qua vẫn không giải quyết được. Mặt khác, an ninh thông tin là một vấn đề mới đối với đa số người dùng. Chia sẻ vấn đề này, ông Vũ Ngọc Sơn, Trưởng phòng virus Trung tâm an ninh mạng Bách Khoa (BKIS), cho biết thậm chí có những đơn vị lập trình website cũng chưa ý thức đầy đủ về vấn đề bảo mật. Tại những công ty nước ngoài, mỗi lập trình viên sau khi tuyển dụng sẽ được tham gia một khoá đào tạo lập trình đặc biệt về an ninh mạng. Tìm được công ty thiết kế website ở Việt Nam làm được điều này rất khó. Việc đầu tư thời gian và công sức vào bảo mật có thể làm chậm tiến độ triển khai dự án, hiệu quả lại khó kiểm chứng.

Vì còn nhiều "lỗ hổng" nên tính giáo dục, răn đe của luật pháp bị giảm nhẹ, tội phạm tin học có chiều hướng gia tăng và đe doạ sự phát triển của TMĐT. Thống kê của VNCERT cho thấy hành vi nổi cộm nhất hiện nay là việc tấn công deface hoặc DDoS để "bảo kê trực tuyến". Trong tháng 3/2006, website của công ty Việt Cơ bị tấn công nặng nề, tất cả các dịch vụ bị đình trệ mất 1 tháng. Tháng 7/2006, hơn 300 website thuê máy chủ của công ty Nhân Hoà bị "đánh tơi tả" bởi một sinh viên trường ĐH Sư phạm Thái Nguyên. Thủ phạm sau đó bị phạt 10 triệu đồng, số tiền người bị hại bỏ ra để tự khắc phục hậu quả lớn hơn gấp nhiều lần. Sau các doanh nghiệp, cơ sở dữ liệu của Sở Kế hoạch Đầu tư TP HCM cũng bị hacker "hỏi thăm". Trong 3 ngày 8, 9, 10/7, giám đốc một công ty TNHH đã lợi dụng lỗ hổng bảo mật của website thay đổi mật khẩu 38 hồ sơ doanh nghiệp khác để "trả thù" vì họ không sử dụng dịch vụ công ty cung cấp. Nhiều hình thức tấn công khác như phát tán virus, chiếm đoạt tên miền, đột nhập thay đổi thông tin… khiến môi trường TMĐT Việt Nam gần như không có luật pháp. Giám đốc công ty Việt Cơ chua chát khi phát biểu với báo chí về việc website công ty bị tấn công: "Nhiều lúc tôi cảm giác làm TMĐT giống như đang sống ở miền Tây hoang dã nước Mỹ cách đây hàng thế kỷ. Phải sống theo luật tự bảo vệ lấy mình, mạnh được yếu thua".

Theo đánh giá của cơ quan điều tra, trình độ hacker Việt Nam chưa cao. Kẻ phạm tội sử dụng công cụ và kỹ thuật "thô sơ" và tất cả đều bị đưa ra ánh sáng. Nguyễn Quang Huy, người bị cáo buộc tấn công Chợ ĐiệnTử gần đây, vốn được giới "khoét vách online" coi là số một cũng bị bắt với những lỗi "rất sơ đẳng và chủ quan" như dùng máy tính tại nhà, không xoá log file khi chiếm quyền điều khiển máy chủ… Những công cụ đặc biệt và nghiệp vụ của cơ quan điều tra có thể khôi phục dữ liệu đã xoá trên ổ cứng, kể cả khi đã bị huỷ bằng các thao tác thông thường như định dạng lại (format), tái phân vùng (fdisk) hoặc ghi đè nội dung (over-write) một số lần nhất định. "Theo nguyên tắc chung, đã phạm tội thì phải có dấu vết dù nhiều hay ít. Cách duy nhất để không để lại gì là không phạm tội", một cán bộ điều tra của C15 khẳng định. "Hầu hết các hacker Việt Nam đều quá trẻ và chưa lường hết được hậu quả".

Để ngăn chặn tình trạng hỗn loạn hiện nay, giải pháp lâu dài được các chuyên gia đề xuất chủ yếu là hoàn thiện hành lang pháp lý và trang bị thêm công cụ cho cơ quan chức năng. Cụ thể, bổ sung các hành vi liên quan đến vi phạm, tội phạm trong lĩnh vực TMĐT vào Luật Hình sự. Đồng

thời, bổ sung tính pháp lý của chứng cứ điện tử trong Luật Tố tụng Hình sự và ban hành các nghị định hướng dẫn Luật Giao dịch điện tử và Luật CNTT. Tuy nhiên, việc xây dựng hành lang pháp lý không thể hoàn tất trong một sớm một chiều. Trước mắt, những việc có thể làm được là bắt tay xây dựng hệ thống điều phối cấp quốc gia về CNTT, phát triển các tiêu chuẩn và khuyến cáo an toàn dành cho doanh nghiệp. Nâng cao nhận thức của cộng đồng cư dân mạng về môi trường TMĐT trong sạch và cạnh tranh lành mạnh đặc biệt quan trọng.

Hưng Hải