NGUY CƠ "11-9 TRÊN MẠNG"

Ngành

Ngành an ninh mạng tại Mỹ vừa trải qua một cú sốc nặng. Mới đây, Bộ tư lệnh Chiến dịch phòng thủ mạng hải quân (NCDOC) tiết lộ: vào tháng 11-2006, tin tặc nước ngoài đã xâm nhập vào hệ thống mạng của Trường Hải quân (NWC), trung tâm nghiên cứu và phát triển chiến lược hải quân Mỹ tại Rhode Island.

Vụ tấn công làm hệ thống mạng của NWC bị tê liệt và không thể kết nối với Internet trong nhiều tuần.

NCDOC khẳng định nhiều khả năng bọn tin tặc thực hiện vụ tấn công nhằm moi trộm thông tin về các cuộc tập trận của hải quân Mỹ do NWC lên kế hoạch. Bọn tin tặc sử dụng kỹ thuật "spear phishing": gửi email có vẻ như bắt nguồn từ NWC cho các nhân viên của trường để lấy mật mã truy cập các thông tin mật. Ngoài ra, chúng còn sử dụng những phương pháp truyền thống hơn như virus và sâu mạng, tuy nhiên mức độ phức tạp hơn rất nhiều.

Theo Học viện An ninh mạng SANs, mạng NWC bị đột nhập bởi trường không được trang bị hệ thống phòng vệ trực tuyến tối tân. Vụ tấn công một lần nữa cho thấy sự mong manh trong hệ thống an ninh mạng của Mỹ, bởi đây không phải là lần đầu tiên một cơ quan chính phủ là mục tiêu của bọn tin tặc nước ngoài. Năm 2003, hàng loạt vụ tấn công có tổ chức đã nhắm vào Cơ quan Hàng không - vũ trụ Mỹ (NASA), Phòng thí nghiệm quốc gia Sandia (trung tâm nghiên cứu của Bộ Năng lượng), Redstone Arsenal (một cơ sở quân sự của lục quân) và Lockhead Martin (nhà thầu quân sự lớn nhất thế giới). Sự kiện này được chính quyền Mỹ đặt cho cái tên "Titan Rain", và chính thức công bố vào tháng 8-2005.

Theo Bộ Quốc phòng Mỹ, nhóm "Titan Rain", bao gồm khoảng 20 hacker, có thể hoạt động tại Quảng Đông (Trung Quốc). Nhóm này đã lấy đi một số bí mật quân sự của Mỹ như thông tin về hệ thống hoạch định hoạt động của trực thăng quân sự và phần mềm kiểm soát các chuyến bay của không quân và lục quân. Cho tới nay, nhóm này vẫn còn hoạt động. Tuy nhiên, Hải quân Mỹ vẫn chưa xác định được liệu "Titan Rain" có phải là tác giả của vụ tấn công mới đây hay không. Điều tra cho thấy có thể các hacker xâm nhập NWC cũng từ Trung Quốc.

Bản thân Bộ Quốc phòng Mỹ, điều hành hơn 5 triệu máy tính trên khắp thế giới, cũng là một mục tiêu ưa thích của bọn tin tặc. Năm 2004, có tới hơn 79.000 vụ tấn công vào các cơ quan Chính phủ Mỹ. Trong đó, bọn tin tặc đã hơn 1.300 lần xâm nhập một máy vi tính của Lầu Năm Góc. Các

chuyên gia nhận định với những vấn đề mà an ninh mạng Mỹ đang gặp phải, hoàn toàn có khả năng một vụ 11-9 trên Internet sẽ xảy ra.

Theo Tổ chức Nguy cơ mạng toàn cầu (CCR), chính quyền Mỹ cần đưa ra chính sách vạch rõ nhiệm vụ của các cơ quan công quyền và khu vực tư nhân nhằm ngăn chặn các vụ tấn công trên mạng. Đồng thời, các cơ quan chịu trách nhiệm "tấn công" trên mạng như Cơ quan An ninh quốc gia (NSA) cần hợp tác chặt chẽ với các tổ chức "phòng thủ" như Bộ tư lệnh Chiến tranh mạng hải quân (NNWC).

Hiếu Trung