# CÔNG NGHỆ BẢO MẬT THUA XA KỸ THUẬT HACK

5 lĩnh vực bảo mật chính cần giải quyết là nạn botnet, tấn công Web 2.0, tin nhắn có mục đích lừa đảo, tấn công mạng viễn thông và RFID.

Công nghệ hacking hiện đã vượt qua sự phát triển của ngành công nghiệp bảo mật. Các bộ phận CNTT cần hợp tác

5 lĩnh vực bảo mật chính cần giải quyết là nạn botnet, tấn công Web 2.0, tin nhắn có mục đích lừa đảo, tấn công mạng viễn thông và RFID.

Công nghệ hacking hiện đã vượt qua sự phát triển của ngành công nghiệp bảo mật. Các bộ phận CNTT cần hợp tác cùng nhau chặt chẽ hơn nữa để xóa bỏ khoảng cách này, báo cáo mới của Trung tâm Bảo mật CNTT Georgia (GTISC) cảnh báo.

GTISC viết tắt của Georgia Tech Information Security Center là một khoa trong trường đại học công nghệ Georgia, chuyên làm về các vấn đề bảo mật thông tin.

Trong báo cáo hàng năm về tình trạng an ninh trực tuyến của GTISC, các chuyên gia IT đã khuyến cáo hệ thống bảo mật hiện tại thua xa kỹ thuật tấn công (hack). Những kỹ thuật hack này đang ngày càng trở nên nổi tiếng và hiệu quả. GTISC thúc giục sự hợp tác giữa ngành công nghiệp bảo mật, các nhà cung cấp dịch vụ, các ISP, nhà phát triển ứng dụng và người dùng Internet.

Báo cáo cũng nói 5 lĩnh vực bảo mật chính cần giải quyết là nạn botnet, tấn công Web 2.0, tin nhắn có mục đích lừa đảo, tấn công mạng viễn thông và RFID (công nghệ nhận dạng tần số radio)

GTISC ước tính khoảng 10% máy tính trên thế giới hiện là một bộ phận của botnet, và tỷ lệ lây nhiễm đang tăng lên. Những mạng lưới như vậy được những kẻ lừa đảo tận dụng triệt để, báo cáo gợi ý các nhà cung cấp bảo mật cần làm nhiều hơn nữa để tích hợp các bức tường lửa trong hệ thống IP để kiểm tra sự lây lan của chúng.

Sự phát triển của Web 2.0 cũng đặt ra những mối đe dọa mới với người dùng Internet. Các nhà phát triển web cần có ý thức bảo mật hơn nữa, và có các công nghệ bảo mật cần thiết để nhận dạng tốt hơn các hành vi đáng ngờ và tẩy chay chúng.

Những cải tiến trong công nghệ chống spam đã khiến hacker sử dụng phương pháp lan truyền tin nhắn có mục đích để lấy cắp dữ liệu. Khi các trang lừa đảo phishing bị đóng lại, những tin nhắn này sẽ cố tình cài đặt malware vĩnh viễn trên máy tính người dùng để lấy cắp thông tin trực tiếp.

Sự hội tụ ngày càng cao của hệ thống truyền thông và hệ thống VoIP cũng tạo ra nhiều nguy hiểm mới. Và cuối cùng, tấn công RFID dự đoán sẽ tăng mạnh trong năm 2008. báo cáo gọi những bảo mật RFID hiện có "cực kỳ hạn chế" và cảnh báo hacking sẽ trở thành vấn đề lớn trong năm 2008.

"Trong giai đoạn đầu, chỉ có một kiểu tấn công khai thác các thiết bị WiFi, nhưng khi công nghệ

trở nên phổ biến và thành tiêu chuẩn, thế hệ các công cụ tấn công WiFi tự động đầu tiên sẽ tiến hóa và tinh vi hơn", báo cáo chỉ rõ. Trong tương lai gần, GTISC dự đoán các công cụ tấn công sẽ cho phép cả những hacker kém hiểu biết về công nghệ tấn công vào các công nghệ RFID.