BẢO MẬT THÔNG TIN TRONG CÁC DOANH NGHIỆP VIỆT NAM: NHIỀU LỖ HỔNG DỄ BỊ XÂM NHẬP

Ông Nguyễn Thế Đông - GĐ Trung tâm Phản ứng nhanh sự cố máy tính Athena tại TPHCM - cho biết: Cách đây chưa lâu, một tập đoàn của Bắc Âu đầu tư tại miền Đông Nam Bộ đã phải dừng hẳn guồng máy sản xuất suốt 2 ngày liền vì hệ thống máy tính

Ông Nguyễn Thế Đông - GĐ Trung tâm Phản ứng nhanh sự cố máy tính Athena tại TPHCM - cho biết: Cách đây chưa lâu, một tập đoàn của Bắc Âu đầu tư tại miền Đông Nam Bộ đã phải dừng hẳn guồng máy sản xuất suốt 2 ngày liền vì hệ thống máy tính bị nhiễm trojan - một loại virus ăn cắp thông tin và có thể làm tê liệt hệ thống máy tính. Hệ thống mạng lỏng lẻo DN Bắc Âu kể trên, dù hệ thống máy tính đã được đầu tư bài bản, nhưng còn gặp phải sự cố gây thiệt hại không nhỏ. Đối với nhiều DN vừa và nhỏ trong nước, hậu quả chắc chắn sẽ còn khó lường hơn một khi hệ thống mạng không được chăm sóc kỹ càng. Theo một khảo sát trên 415 DN tại TPHCM, Đồng Nai, Bình Dương do Athena và Thời báo Vi tính Sài Gòn tiến hành, thì rất nhiều DN trong số này còn ít sử dụng cơ sở dữ liệu chung, thông tin phân tán, dễ thất lạc và không được cập nhật đồng bộ. Nhiều DN vẫn chưa có hệ thống và chính sách sao chép lại dữ liệu (backup) phòng khi xảy ra sự cố. Dù có tới 87% số DN được khảo sát có phân công người chuyên trách quản lý hệ thống mạng, nhưng trong đó chỉ có 36% số người học chuyên ngành CNTT. Số người có các bằng cấp quốc tế về quản trị mạng còn ít hơn-chỉ chiếm 18%. Chính vì nguồn nhân lực về quản trị mạng mỏng và thiếu chuyên môn như thế, cho nên tại nhiều DN, các chính sách, quy định về bảo mật cũng thiếu chặt chẽ. Cụ thể như, ít có qui định rõ ràng đối với nhân viên sử dụng Internet và các thiết bị CNTT trong đơn vị, hoặc giả có nhưng thực hiện không nghiêm, lơi lỏng. Kết quả khảo sát cũng cho thấy, chỉ có 25% DN có phân quyền, phân nhóm người dùng, tạo thư mục, ổ đĩa mạng dùng chung. Song số DN có thiết bị lưu trữ thông tin trên server và thực hiện định kỳ việc phòng ngừa rủi ro là rất ít, chỉ có 15%. Dù hệ thống máy tính của 100% DN đều có cài đặt các phần mềm chống virus, nhưng chỉ 19% DN sử dụng chế độ tự động kiểm tra phiên bản phần mềm chống virus khi người dùng đăng nhập hệ thống mạng. Tình trạng sử dụng các phần mềm chống virus cũ, không được cập nhật, thiếu các giải pháp căn cơ về chống virus, sâu máy tính, phần mềm gián điệp, thư rác, lọc web... đang khá phổ biến tại các DN hiện nay. 8% DN sử dụng hệ thống firewall, 14% DN sử dụng các công cụ giám sát hệ thống mạng nhưng phần lớn sử dụng không thường xuyên và thiếu hiệu quả, đã nói lên sự thiếu hiểu biết, ít quan tâm từ phía DN. Đang bùng nổ sự xâm nhập của virus Ông Phạm Trọng Điểm - chuyên gia về bảo mật của Cty Nam Trường Sơn - cho rằng, hiện nay trên thế giới đang bùng nổ sự tấn công của virus. Thống kê từ tháng 1-10.2005, trên toàn cầu đã xuất hiện gần 2,6 triệu "con" virus, tính ra cứ mỗi ngày có 11.500 "con", và cứ mỗi 7 giây các hệ thống máy tính trên toàn cầu phải đối mặt với sự xâm nhập của 1 "con" virus. Thư rác cùng với phương thức tấn công bằng virus qua email cũng đang phổ biến. Năm 2005, mật độ thư có virus đã tăng lên tỉ lệ 1/75. Các cuộc tấn công của tin tặc đã gia tăng gấp 10 lần so với 10 năm trước. Chính vì thế, theo ông Điểm, các DN cần phải biểu đồ hóa sự bùng nổ của virus để xây dựng kế hoạch phòng chống cho hệ thống máy tính của đơn vị mình. Còn tại VN, trong khuôn khổ cuộc khảo sát nêu trên, có đến 91% số DN bị virus, trojan nhiễm vào hệ thống máy tính, dạng virus tấn công qua email còn trầm trọng hơn - diễn ra đối với hệ thống máy tính của 97% số DN. Ngoài ra, các DN cũng thường xuyên gặp những sự cố về phần cứng, phần mềm, cơ sở dữ liệu, web và Internet v.v... Theo ông Nguyễn Thế Đông, thực trạng qua đợt khảo sát cho thấy các DN còn đầu tư ít, hoặc cầm chừng đối với công tác bảo mật hệ thống máy

tính, vì chưa đánh giá hết các nguy cơ và hậu quả khi xảy ra sự cố. Ông Phạm Trọng Điểm cho biết, các hình thức tấn công của virus ngày càng đa dạng và tinh vi, vì thế, nếu công tác bảo mật thông tin mạng máy tính tại DN không được chuyên nghiệp hoá và thường xuyên nâng cấp thì sẽ khó tránh được các cuộc tấn công gây thiệt hại.