AN NINH THÔNG TIN – VẤN ĐỀ THỜI SỰ CỦA XÃ HỘI THÔNG TIN

Các số liệu thống kê trong những năm gần đây về sự xuất hiện các dòng virus mới, số máy tính bị nhiễm virus và các trang web liên tục bị tin tặc tấn công (xem bài "Tình hình an ninh thông tin ở Việt Nam và sự tiếp cận ISO/IEC 27001" cũng được đăng trong số này của Tạp chí Thông tin và Tư liệu) cho thấy, an ninh thông tin đã trở thành sự thách thức và là mối quan tâm hàng đầu của các doanh nghiệp, các tổ chức nhà nước. Để hiểu rõ hơn tính cấp bách cũng như sự nhạy cảm của vấn đề này, Ban biên tập "Tạp chí Thông tin và Tư liệu" đã tiến hành phỏng vấn ông Lê Anh Tuấn, cán bộ kỹ thuật của công ty Beepack. Dưới đây là toàn bộ nội dung cuộc phỏng vấn nói trên.

BBT*: Tuy chưa định nghĩa được thông tin một cách chính xác, nhưng khi nói đến an ninh thông tin, theo ông thuật ngữ thông tin ở đây nên được hiểu như thế nào?*

Ông Tuấn: Thông tin trong cụm từ "an ninh thông tin" trước hết phải được coi là tài sản. Giống như bất kỳ loại tài sản nào khác của một tổ chức, thông tin có giá trị của nó, và nghĩa là, phải được bảo vệ một cách thích hợp. Thông tin có thể tồn tại dưới nhiều hình thức. Nó có thể là những gì được viết ra hoặc in ra trên giấy, được tàng trữ dưới dạng điện tử, được truyền đi bằng các phương tiện điện tử hoặc gửi qua bưu điện, được chiếu trên phim ảnh hoặc, rất đơn giản, được nói ra khi người ta trao đổi với nhau.

BBT*: Với cách hiểu như vậy, đối với một cơ quan hoặc doanh nghiệp, thông tin sẽ có thể bao gồm những thành phần gì?*

Ông Tuấn: Dưới góc độ an ninh, thông tin cần được bảo vệ hàm chứa các thành phần sau:

- Phần hữu hình: các loại CSDL, các hợp đồng, các quy trình quy phạm, thủ tục,…

- Phần vô hình: danh tiếng, uy tín của công ty; sự tín nhiệm hay lòng tin của khách hàng; …

- Phần mềm tin học: các phần mềm hệ thống, các phần mềm ứng dụng,…

- Phần thực thể: máy tính, máy in, máy fax, điện thoại, điện thoại di động, …

BBT: *Với khả năng kỹ thuật hiện nay trên thế giới, các thành phần được nêu trên của thông tin sẽ phải chịu những nguy cơ gì?*

Ông Tuấn: Nguy cơ có rất nhiều, nhưng thông thường người ta hay đề cập đến những trường hợp sau:

- IP bị nhân viên đã thôi việc tiết lộ ra hoặc gián điệp thương mại lấy cắp mất;
- Đối thủ cạnh tranh mở ra dịch vụ mới sớm hơn và rẻ hơn;
- Virus máy tính làm gián đoạn hoạt động kinh doanh;
- Các số liệu về khách hàng, về giá cả,… trong các CSDL bị sửa sai lệch;
- Sổ y bạ của người bệnh bị tiết lộ cho báo chí;
- Kế hoạch nguồn lực bị tìm thấy trên mạng Internet;
- Đăng ký sở hữu bất động sản bị sửa đổi;

BBT: *Trong những bối cảnh nào thì các nguy cơ nói trên có thể xảy ra?*

Ông Tuấn: Rất đáng tiếc nhưng sự thật là, tất cả mọi cái đều có thể xảy ra vào bất cứ lúc nào. Chẳng hạn:

- Nhân viên cố tình gây hại;
- Có người đột nhập (trong thực tế hoặc về logic);
- Thiết lập chế độ an ninh mạng không đúng (tường lửa, mật khẩu, kết nối từ xa, …);
- Để lại trên mặt bàn những thông tin nhạy cảm;
- Ảnh hưởng của mã độc;

- Tin tặc tấn công;
- Thông tin bị tiết lộ thông qua các nhà cung cấp bên ngoài;
- Động đất, hỏa hoạn, lũ lụt, đình công, mất điện,…

Nhìn chung, nếu thông tin của một cơ quan hay doanh nghiệp không được bảo vệ tốt, chúng sẽ vô hình chung giúp cho người khác có thể biết được toàn bộ hoặc một phần các dữ kiện; được những người quan tâm thu thập dần và biến thành tri thức, tức là sức mạnh trong cạnh tranh của họ. Chính vì lẽ đó mà an ninh thông tin đang trở thành mối quan tâm hàng đầu của mọi lĩnh vực, mọi cấp quản lý.

BBT: *Ông có thể cho một thí dụ gần đây về vấn đề an ninh thông tin được thế giới nói đến không?*

Ông Tuấn: Ngày 10 tháng 9 vừa qua, giới khoa học toàn thế giới đã chứng kiến sự kiện trọng đại được mong đợi từ lâu: Máy gia tốc hạt cực lớn (Large Hadron Collider LHC) đã được đưa vào vận hành tại Trung tâm nghiên cứu hạt nhân châu Âu (CERN). Theo đánh giá sơ bộ, mỗi năm LHC sẽ cung cấp 15 triệu Gb thông tin (nếu ghi trên DVD kép sẽ cần đến 1,7 triệu đĩa). Thế mà chỉ 2 hôm sau, một nhóm tự xưng là an ninh mạng người Hy Lạp "Greek Security Team" đã đột nhập thành công vào một máy tính kết nối tới hệ thống máy tính LHC. Tin tặc đã để lại một thông điệp trên trang web của cơ quan này. Không có bất kỳ một sự phá hoại nào, nhưng đó là một hồi chuông cảnh báo về vấn đề an ninh cho hệ thống máy tính LHC. Chúng ta đều biết, những thí nghiệm đang được CERN tiến hành có liên quan đến hơn 10000 nhà khoa học của trên 500 trường đại học từ hơn 80 nước trên thế giới. Sự kiện trên cho thấy, vấn đề an ninh thông tin của cả hệ thống phải được đặt lên hàng đầu.

BBT: *Vấn đề an ninh thông tin nên được giải quyết như thế nào trong bối cảnh nước ta đang hòa nhập vào nền kinh tế thế giới, sự cạnh tranh ngày càng gay gắt?*

Ông Tuấn: Để bảo vệ thông tin khỏi rất nhiều mối đe dọa các cơ quan và doanh nghiệp nên thiết lập hệ thống quản lý an ninh thông tin (ISMS). Trong cuộc Hội thảo về vấn đề này do Tổng cục Tiêu chuẩn Đo lường Chất lượng

phối hợp với Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) tổ chức tháng 8 năm nay tại Hà Nội, ISMS được cho là hữu hiệu trên cơ sở áp dụng tiêu chuẩn ISO/IEC 27001.

BBT: *Để kết thúc, xin ông cho biết đôi nét về năng lực của chúng ta trong việc giải quyết các vấn đề liên quan đến an ninh thông tin.*

Ông Tuấn: Thay vì đưa ra những nhận xét chủ quan, tôi xin cung cấp thông tin sau. Đầu tháng 9 vừa qua, Việt Nam lần đầu tiên ghi dấu ấn quốc tế trong lĩnh vực an ninh mạng. Trung tâm An ninh mạng BKIS (ĐH Bách khoa Hà Nội) đã phát hiện ra các lỗ hổng bảo mật trong sản phẩm của Microsoft và Google. Trình duyệt Chrome mới của Google đã bị dính các lỗi bảo mật và phải đưa ra bản vá. Trong số 4 lỗ hổng được các chuyên gia an ninh mạng toàn cầu phát hiện ra, thì lỗ hổng do BKIS phát hiện, được Google thừa nhận là nghiêm trọng nhất.

Microsoft cũng đã chính thức xác nhận và đưa ra bản vá cho lỗ hổng của phần mềm Windows Media Encoder được BKIS phát hiện ra. Lỗ hổng này, theo đánh giá của Microsoft, có mức độ nguy hiểm cao nhất vì tin tặc có thể lợi dụng để thực thi mã độc từ xa, chiếm toàn quyền kiểm soát máy tính của nạn nhân.

BBT: *Xin chân thành cám ơn Ông.*

Người thực hiện: ***BTV Lê Trọng Hiển***