TÌNH HÌNH AN NINH THÔNG TIN Ở VIỆT NAM VÀ SỰ TIẾP CẬN ISO/IEC 27001 - HỆ THỐNG QUẢN LÝ AN NINH THÔNG TIN (ISMS)

Bảo vệ thông tin và dữ liệu là một trong những vấn đề quan trọng nhất của các mạng thông tin trong thời đại Internet, đặc biệt với sự phát triển của công nghệ, ngày càng có nhiều cách kết nối, nhiều phương thức trao đổi từ xa sử dụng công nghệ di động và không dây. Yêu cầu quản lý và tuân thủ các nguyên tắc, công nghệ, giải pháp chuẩn đối với các mạng ngày càng phải chặt chẽ hơn. Có thể nói chưa bao giờ mức độ rủi ro liên quan đến an ninh thông tin trên các mạng lại trở thành vấn đề bức xúc như hiện nay.

Tại Việt Nam, theo số liệu thống kê của Trung tâm An ninh mạng BKIS (Bach Khoa Internetwork Security Center), trung tâm hàng đầu tại Việt Nam về nghiên cứu và triển khai các giải pháp về an ninh mạng, chỉ riêng trong năm 2007 số máy tính bị nhiễm vius là 33.646.000 máy; số dòng virus mới xuất hiện là 6.752; số website bị hacker (tin tặc) trong nước tấn công là 118 bị tin tặc nước ngoài tấn công là 224 (tổng cộng- 342 websites); số website được BKIS phát hiện có lỗ hổng là 140.

Con số này có xu hướng ngày càng tăng, chẳng hạn như: chỉ riêng tháng 6/2008 đã có 2.675 dòng virus mới; 5.462.000 máy tính bị nhiễm virus; 59 website bị tấn công; 30 website có lỗ hổng (chủ yếu là của các cơ quan viễn thông, ngân hàng, chứng khoán); đến tháng 7/2008 có 3.060 dòng virus mới và 5.183.000 máy tính bị nhiễm virus; 75 website bị tấn công (đa phần là của các cơ quan nhà nước).

Những nguyên nhân chủ yếu làm cho mạng bị xâm nhập là: 1) Nhận thức về an ninh thông tin chưa tốt trong đội ngũ cán bộ (từ quản lý đến thừa hành); 2) Thiếu đầu tư cho an ninh thông tin; 3) Hệ thống không được thiết kế tốt một cách tổng thể; 4) Thiếu các chính sách và biện pháp quản lý an ninh thông tin.

Những hình thức mà tin tặc thường sử dụng để xâm nhập mạng là: mất/lộ mật khẩu; lừa đảo trực tuyến; tấn công từ chối dịch vụ; thư rác; mã độc; lỗ hổng hệ thống.

Có nhiều giải pháp để đảm bảo an ninh mạng, trong đó việc áp dụng ISO/IEC 27001 - Hệ thống Quản lý an ninh thông tin (ISMS - Information Security Management System) là một giải pháp tổng thể, đã và đang được nhiều quốc gia đặc biệt chú trọng.

Những lợi ích khi áp dụng ISO/IEC 27001:

- Tiêu chuẩn được thế giới công nhận là có năng lực quản lý; là tiêu chí cơ bản cho kinh doanh thương mại điện tử; hệ thống có thể phục hồi nhanh sau thảm hoạ; là chuẩn so sánh của ngành/lĩnh vực;

- Xây dựng được cơ chế an ninh thông tin; quy trình thực hiện tốt nhất và chi phí có hiệu quả đối với hệ thống quản lý an ninh thông tin; nhấn mạnh việc đảm bảo chất lượng và chứng tỏ là một hệ thống quản lý an ninh thông tin thích hợp ở trình độ cao;

- Bằng chứng của việc quan tâm đến khách hàng/người dùng; tăng cường đáp ứng yêu cầu đối với từng cá nhân và tuân thủ luật bảo vệ bí mật đời tư; chú trọng yếu tố lòng tin và sự tin cậy bên trong và ngoài doanh nghiệp/tổ chức; đáp ứng yêu cầu tương lai của khách hàng, các bên và các đối tác, tức là đáp ứng các yêu cầu về an ninh của khách hàng/người dùng; thu hút khách hàng mới;

- Duy trì ấn tượng tốt về doanh nghiệp/tổ chức; duy trì được tính cạnh tranh.

10 bước áp dụng ISO/IEC 27001:

1. Xác định phạm vi của Hệ thống Quản lý an ninh thông tin (ISMS);

2. Xác định chính sách an ninh thông tin;

3. Phân loại tài sản thông tin;

4. Xác định phương pháp luận đánh giá rủi ro;

5. Tiến hành đánh giá rủi ro;

6. Xác định việc chấp nhận rủi ro dựa trên nguồn lực của tổ chức;

7. Xác định việc chấp nhận rủi ro và những điểm tồn tại;

8. Thực hiện và quản lý các điểm kiểm soát đã lựa chọn;

9. Hoàn chỉnh kế hoạch duy trì và phát triển;

10. Chuẩn bị tuyên bố về tính khả dụng.

10 yếu tố để áp dụng thành công:

1. Có chính sách an ninh thông tin, mục tiêu và các hoạt động phản ánh mục đích hoạt động/kinh doanh;

2. Xác lập xu hướng và khuôn khổ thực hiện, duy trì, kiểm soát và cải tiến an ninh thông tin phù hợp với văn hoá của tổ chức;

3. Hỗ trợ cụ thể và cam kết từ tất cả các cấp quản lý;

4. Thông hiểu các yêu cầu an ninh thông tin, đánh giá rủi ro và quản lý rủi ro;

5. Marketing có hiệu quả về an ninh thông tin tới tất cả các nhà quản lý, nhân viên các bên khác (để họ nhận thức được vấn đề);

6. Chỉ đạo chính sách và tiêu chuẩn về an ninh thông tin tới tất cả các nhà quản lý, nhân viên và các bên khác;

7. Cấp quỹ/kinh phí cho các hoạt động quản lý an ninh thông tin;

8. Cung cấp kiến thức, đào tạo và giáo dục thích hợp;

9. Xây dựng quy trình quản lý sự cố an ninh thông tin;

10. Xây dựng hệ thống đánh giá sát thực hoạt động.

Hiện tại, Nhật Bản là quốc gia đứng đầu trong việc áp dụng tiêu chuẩn ISO/IEC 27001 với 2668 cơ quan/tổ chức đã được cấp chứng nhận, tiếp đó là Ấn Độ- 381 và Anh- 347. Trung Quốc mới chỉ có 100 và Mỹ- 73 là những nước đang bắt đầu áp dụng mạnh mẽ IS0 này

Ở Việt Nam, đến nay mới chỉ có 4 đơn vị tư vấn và chứng nhận ISO/IEC 27001, đó là: BVC - Bureau Veritas Certification, TUV Rheinland Vietnam, TUV NORD và TUV SUD. Số đơn vị được chứng nhận cũng chưa đến 10, đó là: FCG Vietnam (CSC), FPT IS, CMC Soft Co., Ltd, GHP FarEAST, ISB Corporation Vietnam,... tức là các công ty hoạt động trong lĩnh vực công nghệ thông tin hoặc công ty có vốn đầu tư của nước ngoài. Ngoài ra, có 3 công ty đang trong quá trình thực hiện là: HTP Soft, Quantic, VietUnion và một số đơn vị đã áp dụng ISO 27001 nhưng không lấy chứng nhận.

Trong số nhiều lý do dẫn đến việc áp dụng ISO này còn rất hạn chế ở Việt Nam, có lý do chi phí cao, gấp tới 2 - 3 lần ISO 9000. Tuy nhiên, tới đây, chắc chắn số lượng các đơn vị tiếp cận và áp dụng ISO/IEC 27001 ở Việt Nam sẽ tăng, bởi vì:

- Yêu cầu bức thiết của vấn đề an ninh thông tin và mạng gắn chặt với hoạt động và lợi ích kinh doanh của mỗi cơ quan; Yêu cầu ngày càng cao về an ninh thông tin của đối tác, khách hàng/người dùng;

- Các cơ quan chính phủ như Bộ Khoa học và Công nghệ (Tổng cục Tiêu chuẩn Đo lường Chất lượng), Bộ Thông tin và Truyền thông đã chú trọng và khuyến nghị các doanh nghiệp/tổ chức thực hiện ISO/IEC 27001;

- Vấn đề tăng cường thương hiệu, sức cạnh tranh của các doanh nghiệp/tổ chức ngày càng trở nên mạnh mẽ.

ISO/IEC 27001 đang được kỳ vọng sẽ thu hút sự quan tâm của nhiều doanh nghiệp/tổ chức như với ISO 9000 trong thập niên 90 và sẽ mang lại hiệu quả thiết thực cho những đơn vị áp dụng, nhất là trong hoạt động và kinh doanh trên mạng INTERNET. Các cơ quan thông tin KH&CN, đặc biệt những nhà cung cấp dịch vụ Internet (ISP) và cung cấp nội dung thông tin (ICP), là nơi quản trị những mạng lớn với Ngân hàng dữ liệu gồm nhiều CSDL và nhiều nguồn tin điện tử quý giá, cần có những bước tiếp cận kịp thời đối với việc đảm bảo an ninh thông tin nói chung và áp dụng ISO/IEC 27001 nói riêng.

Nguyễn Tiến Đức

Tài liệu tham khảo

ISO Regional Seminar & Workshop on ISO/IEC 27001 - Information Security Management System (ISMS)., Hanoi, Vietnam, 25 August 2008.