1. Các chuẩn quản lý an toàn thông tin

1.1 Giới thiệu

Trong các chuẩn quản lý an toàn thông tin, bộ chuẩn NIST SP 800 của Viện tiêu chuẩn và công nghệ Mỹ và bộ chuẩn quốc tế ISO/IEC 27000 được tham chiếu và sử dụng rộng rãi nhất. Nhiều quốc gia, trong đó có Việt Nam đã dịch và chấp thuận nguyên vẹn một số chuẩn trong bộ chuẩn quốc tế ISO/IEC 27000 làm chuẩn quản lý an toàn thông tin quốc gia. Trong phạm vi của môn học, mục này giới thiệu khái quát về bộ chuẩn quản lý an toàn thông tin ISO/IEC 27000. Chi tiết về bộ chuẩn ISO/IEC 27000 và các bộ chuẩn khác được đề cập trong môn học Quản lý an toàn thông tin.

Chuẩn ISO/IEC 27000: 2009 giới thiệu khái quát về bộ chuẩn ISO/IEC 27000 và định nghĩa các thuật ngữ và từ vựng sử dụng cho toàn bộ các chuẩn con trong bộ chuẩn ISO/IEC 27000.

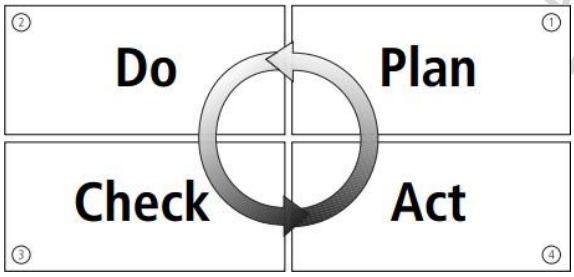
Chuẩn ISO/IEC 17799 được soạn thảo năm 2000 bởi International Organization for Standardization (ISO) và International Electrotechnical Commission (IEC) là tiền thân của ISO 27000. Năm 2005, ISO 17799 được chỉnh sửa và trở thành ISO 17799:2005. Năm 2007, ISO 17799:2005 được đổi tên thành ISO 27002 song hành với ISO 27001.

Chuẩn ISO/IEC 27001:2005 chuyên về hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS). Chuẩn này cung cấp các thông tin để thực thi các yêu cầu của ISO/IEC 27002 và cài đặt một hệ thống quản lý an toàn thông tin. Trong việc xây dựng hệ thống ISMS, chuẩn cung cấp các chi tiết cho thực hiện chu kỳ Lập kế hoạch – Thực hiện – Giám sát – Hành động (Plan-Do-Check-Act). Một điểm cần lưu ý là ISO/IEC 27001 chỉ tập trung vào các phần việc phải thực hiện mà không chỉ dẫn cách thức thực hiện.

Chuẩn ISO/IEC 27002 gồm 127 điều, cung cấp cái nhìn tổng quan về nhiều lĩnh vực trong an toàn thông tin. Nó đề ra các khuyến nghị về quản lý an toàn thông tin cho những người thực hiện việc khởi tạo, thực hiện và duy trì an ninh an toàn trong tổ chức của họ. Chuẩn này được thiết kế để cung cấp nền tảng cơ sở giúp đề ra các chuẩn an toàn thông tin cho tổ chức và các thực tế quản lý an toàn thông tin một cách hiệu quả.

Chuẩn ISO/IEC 27005: 2009 chuyên về quản lý rủi ro cho hệ thống quản lý an toàn thông tin. Chuẩn này hỗ trợ ISO/IEC 27001, nhưng nó không đề cập đến phương pháp kiểm soát rủi ro cụ thể.

1.2 Chu trình Plan-Do-Check-Act



Hình 5.3. Chu trình Plan-Do-Check-Act của ISO/IEC 27001:2005

Chuẩn ISO/IEC 27001:2005 chuyên về hệ thống quản lý an toàn thông tin cung cấp các chi tiết cho thực hiện chu kỳ Plan-Do-Check-Act gồm 4 pha: Plan - Lập kế hoạch, Do – Thực hiện kế hoạch, Check – Giám sát việc thực hiện và Act – Thực hiện các cải tiến, hiệu chỉnh. Phần tiếp theo là nội dung chi tiết của các pha này.

Pha ***Plan*** gồm các nội dung:

- Đề ra phạm vi của ISMS;
- Đề ra chính sách của ISMS;
- Đề ra hướng tiếp cận đánh giá rủi ro;
- Nhận dạng các rủi ro;
- Đánh giá rủi ro;
- Nhận dạng và đánh giá các lựa chọn phương pháp xử lý rủi ro;
- Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát;
- Chuẩn bị tuyến bố, báo cáo áp dụng.

Pha Do gồm các nội dung:

- Xây dựng kế hoạch xử lý rủi ro;
- Thực thi kế hoạch xử lý rủi ro;
- Thực thi các kiểm soát;
- Thực thi các chương trình đào tạo chuyên môn và giáo dục ý thức;
- Quản lý các hoạt động;
- Quản lý các tài nguyên;
- Thực thi các thủ tục phát hiện và phản ứng lại các sự cố an ninh.

Pha ***Check*** gồm các nội dung:

- Thực thi các thủ tục giám sát;
- Thực thi việc đánh giá thường xuyên tính hiệu quả của ISMS;
- Thực hiện việc kiểm toán (audits) nội bộ với ISMS;
- Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý;

- Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS.

Pha ***Act*** gồm các nội dung:

- Thực hiện các cải tiến đã được nhận dạng;
- Thực hiện các hành động sửa chữa và ngăn chặn;
- Áp dụng các bài đã được học;
- Thảo luận kết quả với các bên quan tâm;
- Đảm bảo các cải tiến đạt được các mục tiêu.

2. Pháp luật và chính sách an toàn thông tin

2.1 Giới thiệu về pháp luật và chính sách an toàn thông tin

Các chính sách và pháp luật an toàn thông tin có vai trò rất quan trọng trong việc đảm bảo an toàn cho thông tin, hệ thống và mạng. Trong đó, vai trò của nhân viên đảm bảo an toàn thông tin là rất quan trọng trong việc giảm thiểu rủi ro, đảm bảo an toàn cho thông tin, hệ thống và mạng và giảm thiệt hại nếu xảy ra sự cố. Các nhân viên đảm bảo an toàn cho thông tin phải hiểu rõ những khía cạnh pháp lý và đạo đức an toàn thông tin. Theo đó, họ phải luôn nắm vững môi trường pháp lý hiện tại (các luật và các quy định luật pháp) và luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp. Ngoài ra, cần thực hiện việc giáo dục ý thức về luật pháp và đạo đức an toàn thông tin cho cán bộ quản lý và nhân viên trong tổ chức, đảm bảo sử dụng đúng mục đích các công nghệ đảm bảo an toàn thông tin.

Chính sách (Policy - còn gọi là quy định, nội quy) là các quy định về các hành vi chấp nhận được của các nhân viên trong tổ chức tại nơi làm việc. Chính sách là các "luật" của tổ chức có giá trị thực thi trong nội bộ, gồm một tập các quy định và các chế tài xử phạt bắt buộc phải thực hiện. Các chính sách, hoặc nội quy cần được nghiên cứu, soạn thảo kỹ lưỡng. Đồng thời, chính sách cần đầy đủ, đúng đắn và áp dụng công bằng với mọi nhân viên. Điểm khác biệt giữa luật và chính sách là Luật luôn bắt buộc, còn với Chính sách, việc thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được.

Cần có phân biệt rõ ràng giữa *luật* (Law) và *đạo đức* (Ethic). Luật gồm những điều khoản bắt buộc hoặc cấm những hành vi cụ thể. Các điều luật thường được xây dựng từ các vấn đề đạo đức. Trong khi đó, đạo đức định nghĩa những hành vi xã hội chấp nhận được. Đạo đức thường dựa trên các đặc điểm văn hóa. Do đó, hành vi đạo đức giữa các dân tộc, các nhóm người khác nhau là khác nhau. Một số hành vi vi phạm đạo đức được luật hóa trên toàn thế giới, như trộm, cướp, cưỡng dâm, bạo hành trẻ em,... Khác biệt giữa luật và đạo đức thể

hiện ở chỗ luật được thực thi bởi các cơ quan chính quyền, còn đạo đức không được thực thi bởi các cơ quan chính quyền.

Hình 5.4. Vấn đề tuân thủ (Compliance) pháp luật, chính sách và các nội quy, quy định

Để các chính sách có thể được áp dụng hiệu quả, chúng phải đạt được các yêu cầu sau:

- Có khả năng phổ biến rộng rãi, bằng tài liệu giấy hoặc điện tử;
- Nhân viên có thể xem, hiểu được – cần thực hiện trên nhiều ngôn ngữ, ví dụ bằng tiếng Anh và tiếng địa phương;
- Chính sách cần rõ ràng dễ hiểu – tổ chức cần có các điều tra/khảo sát về mức độ hiểu biết/nắm bắt các chính sách của nhân viên;
- Cần có biện pháp để nhân viên cam kết thực hiện – thông qua ký văn bản cam kết hoặc tick vào ô xác nhận tuân thủ;
- Chính sách cần được thực hiện đồng đều, bình đẳng, nhất quán, không có ưu tiên với bất kỳ nhân viên nào, kể cả người quản lý.

2.2 Luật quốc tế về an toàn thông tin

Mục này đề cập đến một số luật và văn bản có liên quan đến an toàn thông tin của Mỹ và Châu Âu – là những nước và khu vực đã phát triển và có hệ thống luật pháp về an toàn thông tin tương đối hoàn thiện.

Có thể nói hệ thống luật pháp về an toàn thông tin của nước Mỹ khá đầy đủ và được chia thành các nhóm: các luật tội phạm máy tính, các luật về sự riêng tư, luật xuất khẩu và chống gián điệp, luật bản quyền và luật tự do thông tin. Các luật về tội phạm máy tính gồm:

- Computer Fraud and Abuse Act of 1986 (CFA Act): quy định về các tội phạm lừa đảo và lạm dụng máy tính;

- Computer Security Act, 1987: đề ra các nguyên tắc đảm bảo an toàn cho hệ thống máy tính;
- National Information Infrastructure Protection Act of 1996: là bản sửa đổi của CFA Act, tăng khung hình phạt một số tội phạm máy tính đến 20 năm tù;
- USA PATRIOT Act, 2001: cho phép các cơ quan nhà nước một số quyền theo dõi, giám sát các hoạt động trên mạng nhằm phòng chống khủng bố hiệu quả hơn;
- USA PATRIOT Improvement and Reauthorization Act: Mở rộng của USA PATRIOT Act, 2001, cấp cho các cơ quan nhà nước nhiều quyền hạn hơn cho nhiệm vụ phòng chống khủng bố.

Các luật về sự riêng tư nhằm bảo vệ quyền riêng tư của người dùng, bảo vệ các thông tin cá nhân của người dùng, gồm:

- Federal Privacy Act, 1974: luật Liên bang Mỹ bảo vệ quyền riêng tư của người dùng;
- Electronic Communications Privacy Act , 1986: luật bảo vệ quyền riêng tư trong các giao tiếp điện tử;
- Health Insurance Portability and Accountability Act, 1996 (HIPAA): bảo vệ tính bí mật và an toàn của các dữ liệu y tế của người bệnh. Tổ chức, hoặc cá nhân vi phạm có thể bị phạt đến 250.000 USD hoặc 10 năm tù;
- Financial Services Modernization Act or Gramm-Leach-Bliley Act, 1999: điều chỉnh các hoạt động liên quan đến nhà nước của các ngân hàng, bảo hiểm và các hãng an ninh.

Luật xuất khẩu và chống gián điệp hạn chế việc xuất khẩu các công nghệ và hệ thống xử lý thông tin và phòng chống gián điệp kinh tế, gồm:

- Economic Espionage Act, 1996: phòng chống việc thực hiện giao dịch có liên quan đến bí mật kinh tế và công nghệ;
- Security and Freedom through Encryption Act, 1999: quy định về các vấn đề có liên quan đến sử dụng mã hóa trong đảm bảo an toàn và tự do thông tin.

U.S. Copyright Law là Luật bản quyền của Mỹ, điều chỉnh các vấn đề có liên quan đến xuất bản, quyền tác giả của các tài liệu, phần mềm, bao gồm cả các tài liệu số. Freedom of Information Act, 1966 (FOIA) là Luật tự do thông tin nêu rõ các cá nhân được truy nhập các thông tin không gây tổn hại đến an ninh quốc gia.

Các tổ chức và luật quốc tế có liên quan đến an toàn thông tin, gồm:

- Hội đồng Châu Âu về chống tội phạm mạng (Council of Europe Convention on Cybercrime);
- Hiệp ước về chống tội phạm mạng được Hội đồng châu Âu phê chuẩn vào năm 2001;
- Hiệp ước bảo vệ quyền sở hữu trí tuệ (Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)): do Tổ chức Thương mại thế giới WTO chủ trì đàm phán trong giai đoạn 1986–1994;
- Digital Millennium Copyright Act (DMCA): Luật bản quyền số Thiên niên kỷ.

2.3 Luật Việt Nam về an toàn thông tin

Luật an toàn thông tin mạng được Quốc hội thông qua vào tháng 11 năm 2015 và chính thức có hiệu lực từ ngày 1/7/2016. Đây là cơ sở pháp lý quan trọng cho việc quản lý các hoạt động liên quan đến an toàn thông tin ở Việt Nam. Ngoài Luật an toàn thông

tin mạng, đã có nhiều văn bản có liên quan đến công nghệ thông tin và an toàn thông tin được Quốc Hội, Chính Phủ và các cơ quan nhà nước ban hành như:

- Luật công nghệ thông tin số 67/2006/QH11 của Quốc hội, ngày 12/07/2006.
- Nghị định số 90/2008/NĐ-CP của Chính Phủ "Về chống thư rác", ngày 13/08/2008.
- Quyết định số 59/2008/QĐ-BTTTT của Bộ Thông tin và Truyền thông "Ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số", ngày 31/12/2008.
- Quyết định 63/QĐ-TTg của Thủ tướng CP "Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020", ngày 13/01/2010.
- Chỉ thị số 897/CT-TTg của Thủ tướng CP "V/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số", 10/06/2011.
- Thông tư số 23/2011/TT-BTTTT của Bộ TT&TT "Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước", ngày 11/08/2011.
- Nghị định số 77/2012/NĐ-CP của Chính Phủ "Sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 của Chính phủ về chống thư rác", ngày 05/10/2012.
- Nghị định 72/2013/NĐ-CP của Chính Phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng; quy định về việc chia sẻ thông tin trên các trang mạng xã hội.

Ngoài ra, Dự thảo Luật an ninh mạng đã được Bộ Công An soạn thảo, lấy ý kiến các chuyên gia và đưa ra Quốc Hội xem xét thông qua vào cuối năm 2017.