ISO 27001 - Công cụ hữu hiệu quản lý an toàn, an ninh mạng máy tính và lưu trữ dữ liệu

Đặng Huỳnh Kim
Bộ KH&CN

An toàn thông tin (ATTT) là một trong những vấn đề nhức nhối ở Việt Nam hiện nay. Theo đánh giá của các chuyên gia, thách thức đảm bảo ATTT trong các cơ quan chủ yếu là do thiếu chính sách, quy trình quản lý và nhận thức của con người. Có rất nhiều giải pháp khác nhau trong việc đảm bảo ATTT trong các tổ chức, trong đó ISO 27001 là một lựa chọn phù hợp nhằm quản lý an toàn, an ninh mạng máy tính và lưu trữ dữ liệu.

ISO 27001 và tình hình triển khai áp dụng trên thế giới

Hiện nay, có khoảng 164 quốc gia đang áp dụng các tiêu chuẩn do Tổ chức tiêu chuẩn hóa quốc tế (ISO) quy định. Có 17.500 loại tiêu chuẩn quốc tế khác nhau, và có tới 1.100 tiêu chuẩn mới được thành lập mỗi năm. ISO/IEC 27000 là bộ tiêu chuẩn về hệ thống quản lý ATTT. Trong đó, ISO/IEC 27001 là chuẩn về các yêu cầu đối với hệ thống quản lý ATTT, là chuẩn được sử dụng rộng rãi bởi các cơ quan, tổ chức để đảm bảo tính bí mật, toàn vẹn và sẵn sàng của các thông tin nghiệp vụ của các tổ chức đó.

Trong năm 2013, ít nhất có 22.293 chứng nhận ISO/IEC 27001 đã được cấp tại 105 quốc gia và nền kinh tế, tăng 14% so với năm 2012. Ba quốc gia đứng đầu về số giấy chứng nhận được cấp là Nhật Bản (7.084), Ấn Độ (1.931) và Vương quốc Anh (1.923). Các lĩnh vực áp dụng ISO 27001 chiếm các tỷ lệ khác nhau. Chẳng hạn như: viễn thông được áp dụng nhiều nhất với 27% tổng số giấy chứng nhận cấp ra, tài chính ngân hàng chiếm 20%, công nghệ thông tin (CNTT) chiếm 15%...

An toàn, an ninh thông tin trong các cơ quan nhà nước ở Việt Nam

Cơ quan nhà nước (CQNN) là nơi lưu trữ và xử lý nhiều thông tin quan trọng, ảnh hưởng đến quyết sách của cả quốc gia. Vì vậy, việc đảm bảo ATTT trong các cơ quan này là yếu tố quan trọng hàng đầu. Mặc dù đã triển khai một số giải pháp mang lại kết quả bước đầu nhưng thực tế ở nhiều nơi vẫn đang ngày càng bộc lộ nhiều nguy cơ mất ATTT.

Trong bối cảnh CNTT được ứng dụng sâu rộng trong toàn bộ các lĩnh vực kinh tế, chính trị, xã hội như hiện nay thì vấn đề ATTT lại càng thu hút sự quan tâm mạnh mẽ. Đối với các CQNN, việc đẩy mạnh ứng dụng CNTT theo Nghị định 64/2007/NĐ-CP đang được triển khai quyết liệt trên phạm vi cả nước để xây dựng chính quyền điện tử, công dân điện tử, cải cách thủ tục hành chính. Đảm bảo ATTT là công việc gắn liền với nhiệm vụ thúc đẩy ứng dụng CNTT. Một giải pháp quan trọng để đảm bảo ATTT trong CQNN là xây dựng, áp dụng tiêu chuẩn quốc tế về ATTT.

Trong các CQNN, hệ thống trang tin điện tử, cổng thông tin điện tử thuộc nhóm mất an toàn cao nhất, hay bị tấn công nhất. Theo Hiệp hội ATTT Việt Nam (VNISA), đa số bị tấn công theo kiểu từ chối dịch vụ (DDoS), có đến 78% website tên miền "gov.vn" có thể bị tấn công, điển hình là các báo điện tử lớn bị tấn công kéo dài hồi tháng 7/2013. Đối với cổng thông tin của địa phương và doanh nghiệp nhà nước, lỗi phổ biến nhất là lộ mã nguồn với tỷ lệ tương ứng lên tới 76% và 71%. Trong năm 2012, khoảng 35% CQNN bị tấn công theo hình thức hacker gửi mã độc để phá hủy hệ thống thông tin, dữ liệu. Theo báo cáo tổng hợp về ATTT của nhiều hãng bảo mật nước ngoài như McAfee, Kaspersky, CheckPoint, Việt Nam đang bị xếp vào nhóm các nước thuộc diện mất ATTT cao trên thế giới về mức độ rủi ro đối với cả người sử dụng cũng như nhà cung cấp dịch vụ Internet. Nguy cơ này không chỉ tồn tại ở các doanh nghiệp, mà còn hiển hiện rất rõ trong khối các CQNN.

Đánh giá chung của các chuyên gia ATTT trong thời gian gần đây thì các hoạt động tin tặc liên tục gia tăng, mức độ nguy hiểm và tính tự động ngày càng cao, các kiểu tấn công ngày càng đa dạng. Xu hướng tấn công tập trung nhiều vào các cơ quan liên quan đến tài chính, ngân hàng. Những số liệu nêu trên cho thấy, việc đảm bảo ATTT trong CQNN chưa cao, khả năng tự bảo vệ trước mã độc và các cuộc tấn công thấp.

Để phòng, chống và khắc phục sự cố mất ATTT, các cơ quan, tổ chức, trước tiên phải xây dựng một hệ thống an ninh mạng. Hệ thống này thường gồm các thành phần như Network Security (Firewall, IPA/IDS), Endpoint Sercurity (Antivirus, Anti-Spam, NAC), và xác thực, đảm bảo tính toàn vẹn của dữ liệu (OTP, PKI, mã hóa dữ liệu). Tuy nhiên, xây dựng

được hệ thống an ninh mạng không có nghĩa đã đảm bảo được ATTT mà cần áp dụng các biện pháp vận hành duy trì hệ thống này. Việc này bao gồm xây dựng nguồn nhân lực để vận hành, duy trì hệ thống an ninh mạng thường xuyên. Đặc biệt, phải xây dựng và thực thi nghiêm chỉnh chính sách bảo mật thông tin. Trong khối các CQNN, mặc dù đã được đầu tư, triển khai nhiều biện pháp nhưng hiệu quả vẫn chưa được như mong muốn, chưa theo kịp yêu cầu của thực tế.

Sự cần thiết và tình hình áp dụng tiêu chuẩn quốc tế về ATTT tại Việt Nam

Theo đánh giá của Cục Tin học thống kê (Bộ Tài chính), thách thức đảm bảo ATTT trong các cơ quan liên quan đến công nghệ chỉ chiếm 20%, phần chủ yếu còn lại chính là do thiếu chính sách, quy trình quản lý và nhận thức của con người. Cho dù được đầu tư thiết bị tốt đến đâu đi nữa thì việc lộ lọt, mất thông tin là hoàn toàn có thể xảy ra nếu như nó xuất phát từ chính con người trong tổ chức ấy hoặc từ chính quy trình trao đổi thông tin nội bộ lỏng lẻo gây ra. Ngoài ra, chính sách, quy trình bảo mật thông tin còn cho biết cần bảo vệ tài nguyên gì, mức độ bảo vệ với từng loại tài nguyên, những điểm hạn chế cần phải khắc phục, ngăn ngừa vi phạm pháp lý và định hướng lựa chọn các giải pháp an ninh. Phân tích trên cho thấy tầm quan trọng của chính sách, quy trình quản lý bảo mật thông tin.

Các cơ quan chuyên trách của Chính phủ (Bộ Thông tin và Truyền thông, Tổng cục Tiêu chuẩn Đo lường chất lượng - Bộ KH&CN) cũng đã có khuyến cáo áp dụng ISO 27001 rộng rãi trong cả nước. Theo số liệu chính thức của Tổ chức ISO công bố năm 2013, Việt Nam có 39 tổ chức, doanh nghiệp được đánh giá đạt chuẩn ISO/IEC 27001. Có thể thấy rằng số đơn vị đạt chứng nhận ISO 27001 tại Việt Nam khá ít so với Nhật Bản (6.914 chứng nhận), Trung Quốc (1.710 chứng nhận), Thái Lan (125 chứng nhận), Malaysia (181 chứng nhận) và Singapore (84 chứng nhận).

Mặc dù lợi ích mà ISO 27001 đem lại là rất lớn, nhưng trong thực tế số lượng các đơn vị có kế hoạch triển khai xây dựng hệ thống quản lý này lại rất hạn chế, đặc biệt trong khối CQNN. Theo thống kê của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và VNISA đối với khoảng 500 doanh nghiệp và CQNN trong 2 năm 2010-2011 thì có đến 55% đơn vị chưa có kế hoạch triển khai tiêu chuẩn này, 22% chỉ định triển khai nhưng không có ý định đánh giá lấy chứng chỉ. Nguyên nhân là do chi phí triển khai và đạt được chứng chỉ ISO 27001 khá cao; thứ hai là hạn chế về nhận thức, trình độ cũng như sự tuân thủ các chính sách bảo mật thông tin; các tài liệu, hướng dẫn của ISO 27001 chủ yếu bằng tiếng Anh, được xây dựng xuất phát từ nhu cầu thực tế của các hệ thống thông tin tại các nước phát triển, rất khó khăn để có thể phổ biến rộng rãi và triển khai thực tế. Vì vậy, cần có những hoạt động để thích ứng bộ tiêu chuẩn này với thực tiễn các hệ thống thông tin tại Việt Nam nói chung và tại các hệ thống thông tin của các cơ quan quản lý nhà nước nói riêng.

Hiện tại, trong khối các bộ, ngành, Bộ KH&CN đang có hạ tầng công nghệ thông tin khá hiện đại. Mặc dù hệ thống an ninh mạng đã được trang bị các thiết bị bảo mật gồm: tường lửa, thiết bị chống xâm nhập IDS/IPS, phần mềm diệt virus, phần mềm chống thư điện tử rác, mạng riêng ảo VPN… nhưng vẫn cần hoàn thiện thêm các chính sách, quy trình đảm bảo ATTT. Bộ cũng chưa có quy chế về ATTT, vì thế sự cần thiết phải có một hệ thống quản lý ATTT tuân theo chuẩn quốc tế là điều tất yếu. Việc lựa chọn ISO 27001 là rất phù hợp với tình hình thực tế tại Bộ KH&CN hiện nay, bởi đây là hệ thống quy trình toàn diện không những đảm bảo về kỹ thuật, quy trình hoạt động của toàn hệ thống thông tin mà còn tích hợp cả quy trình các nguyên tắc của con người hoạt động trong mỗi cơ quan, tổ chức. Đây cũng là bộ tiêu chuẩn phổ biến hiện nay hướng dẫn xây dựng và áp dụng hệ thống quản lý ATTT.

Với việc thực hiện đề tài "Nghiên cứu áp dụng ISO 27001 để quản lý an toàn, an ninh mạng máy tính và quản lý hệ thống lưu trữ dữ liệu", Bộ KH&CN đã nâng tầm lên một bước trong việc quản lý an toàn, an ninh mạng máy tính và lưu trữ dự liệu, cụ thể: i) Đã xây dựng được Sổ tay bảo mật dưới dạng sách in và bản mềm; ii) Xây dựng được Quy trình quản lý an toàn, an ninh mạng máy tính; xây dựng được Quy trình quản lý hệ thống lưu trữ dữ liệu… Với kết quả trên, Bộ KH&CN đã ghi tên thêm vào danh sách những đơn vị áp dụng thành công hệ thống ISO 27001 nhằm quản lý an toàn, an ninh mạng máy tính và lưu trữ dữ liệu phục vụ công tác quản lý của Bộ ✍