TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN ISO/IEC 27002:2011
ISO/IEC 27002:2005

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – QUY TẮC THỰC HÀNH QUẢN LÝ AN TOÀN THÔNG TIN

Information technology – Security techniques – Code of practice for infomation security management

HÀ NỘI – 2011

Mục lục

Lời nói đầu

TCVN ISO/IEC 27002:2011 hoàn toàn tương đương với ISO/IEC 27002:2005.

TCVN ISO/IEC 27002:2011 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin – Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin

Information technology – Security techniques – Code of practice for infomation security management

1 Phạm vi áp dụng

Tiêu chuẩn này thiết lập các hướng dẫn và nguyên tắc chung cho hoạt động khởi tạo, triển khai, duy trì và cải tiến công tác quản lý an toàn thông tin trong một tổ chức. Mục tiêu của tiêu chuẩn này là đưa ra hướng dẫn chung nhằm đạt được các mục đích chung đã được chấp nhận trong quản lý an toàn thông tin.

Các mục tiêu và biện pháp quản lý của tiêu chuẩn này được xây dựng nhằm đáp ứng các yêu cầu đã được xác định bởi quá trình đánh giá rủi ro. Tiêu chuẩn này có thể đóng vai trò như một hướng dẫn thực hành trong việc xây dựng các tiêu chuẩn an toàn thông tin cho tổ chức và các quy tắc thực hành quản lý an toàn thông tin hiệu quả và giúp tạo dựng sự tin cậy trong các hoạt động liên tổ chức.

2 Thuật ngữ và định nghĩa

2.1

Tài sản (asset)

Bất cứ thứ gì có giá trị đối với tổ chức.

[ISO/IEC 13335-1:2004]

2.2

Biện pháp quản lý (control)

Các biện pháp quản lý rủi ro bao gồm các chính sách, thủ tục, hướng dẫn, thực hành hoặc các cơ cấu tổ chức, trên phương diện hành chính, kỹ thuật, quản lý hoặc bản chất pháp lý.

CHÚ THÍCH: Biện pháp quản lý cũng được sử dụng đồng nghĩa với biện pháp bảo vệ hay biện pháp đối phó.

2.3

Hướng dẫn (guideline)

Một mô tả trong đó chỉ ra điều cần làm và phương thức tiến hành nhằm đạt được các mục tiêu đã chỉ ra trong các chính sách.

[ISO/IEC 13335-1:2004]

2.4

Phương tiện xử lý thông tin (information processing facilities)

Hệ thống, dịch vụ hay cơ sở hạ tầng xử lý thông tin, hoặc các vị trí vật lý để đặt chúng.

2.5

An toàn thông tin (information security)

Sự duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin; ngoài ra còn có thể bao hàm một số tính chất khác như tính xác thực, giải trình trách nhiệm, không thể chối bỏ và tin cậy.

2.6

Sự kiện an toàn thông tin (information security event)

Một sự kiện đã được xác định của một hệ thống, dịch vụ hay trạng thái mạng chỉ ra khả năng vi phạm chính sách an toàn thông tin, sự thất bại của hệ thống bảo vệ, hoặc một tình huống chưa rõ gây ảnh hưởng đến an toàn thông tin.

[ISO/IEC TR 18004:2004]

2.7

Sự cố an toàn thông tin (information security incident)

Một hoặc một chuỗi các sự kiện an toàn thông tin không mong muốn có khả năng làm tổn hại các hoạt động nghiệp vụ và đe dọa an toàn thông tin.

[ISO/IEC TR 18044:2004]

2.8

Chính sách (policy)

Mục đích và định hướng tổng thể được công bố một cách chính thức bởi ban quản lý.

2.9

Rủi ro (risk)

Sự kết hợp giữa khả năng xảy ra một sự kiện và hậu quả.

2.10

Phân tích rủi ro (risk analysis)

Sử dụng thông tin một cách có hệ thống nhằm xác định các nguồn gốc và ước đoán rủi ro.

[ISO/IEC Guide 73:2002]

2.11

Đánh giá rủi ro (risk assessment)

Quá trình tổng thể gồm phân tích rủi ro và ước lượng rủi ro.

[ISO/IEC Guide 73:2002].

2.12

Ước lượng rủi ro (risk evaluation)

Quá trình so sánh rủi ro đã ước đoán với một chỉ tiêu rủi ro đã có nhằm xác định độ nghiêm trọng của rủi ro.

[ISO/IEC Guide 73:2002]

2.13

Quản lý rủi ro (risk management)

Các hoạt động phối hợp nhằm điều khiển và quản lý một tổ chức trước các rủi ro có thể xảy ra.

CHÚ THÍCH: Quản lý rủi ro thường gồm đánh giá rủi ro, xử lý rủi ro, chấp nhận rủi ro và thông báo rủi ro.

[ISO/IEC Guide 73:2002]

2.14

Xử lý rủi ro (risk treament)

Quá trình lựa chọn và triển khai các biện pháp hạn chế rủi ro.

[ISO/IEC Guide 73:2002]

2.15

Bên thứ ba (thirt party)

Một cá nhân hay một tổ chức được công nhận là độc lập với các bên tham gia, có liên quan đến vấn đề đang phải giải quyết.

2.16

Mối đe dọa (threat)

Nguyên nhân tiềm ẩn gây ra sự cố không mong muốn, kết quả là có thể gây tổn hại cho một hệ thống hoặc tổ chức.

[ISO/IEC 13335-1:2004]

2.17

Điểm yếu (vulnerability)

Nhược điểm của một tài sản hoặc một nhóm tài sản có khả năng bị lợi dụng bởi một hay nhiều mối đe dọa.

[ISO/IEC 13335-1:2004]

3 Đánh giá và xử lý rủi ro

3.1 Đánh giá rủi ro an toàn thông tin

Đánh giá rủi ro cần xác định, định lượng và phân loại ưu tiên các rủi ro dựa trên tiêu chí về chấp nhận rủi ro và các mục tiêu phù hợp với tổ chức. Các kết quả cần hướng dẫn và xác định hoạt động quản lý phù hợp và phân loại ưu tiên nhằm phục vụ cho việc quản lý các rủi ro an toàn thông tin và triển khai các biện pháp quản lý đã được chọn nhằm chống lại các rủi ro này. Quá trình đánh giá các rủi ro và chọn lựa các biện pháp quản lý có thể cần được thực hiện nhiều lần nhằm bao quát hết các bộ phận khác nhau của tổ chức hoặc các hệ thống thông tin riêng lẻ.

Đánh giá rủi ro cần bao hàm cách tiếp cận có hệ thống trong việc ước lượng độ lớn của các rủi ro (phân tích rủi ro) và quá trình so sánh các rủi ro đã được ước đoán với tiêu chí rủi ro nhằm xác định độ nghiêm trọng của các rủi ro (ước lượng rủi ro).

Đánh giá rủi ro cần được thực hiện định kỳ nhằm phát hiện những thay đổi về các yêu cầu an toàn và tình huống rủi ro, ví dụ trong các tài sản, các mối đe dọa, các điểm yếu, các tác động, trong ước lượng rủi ro, và khi xảy ra những thay đổi lớn. Những đánh giá rủi ro này cần được thực hiện một cách có phương pháp nhằm đưa ra các kết quả có khả năng so sánh và tái sử dụng.

Để có hiệu quả thì đánh giá rủi ro an toàn thông tin cần có một phạm vi xác định rõ ràng, và nếu thích hợp thì cần bao hàm cả các mối quan hệ với việc đánh giá rủi ro cho các lĩnh vực khác.

Phạm vi của đánh giá rủi ro có thể là trong toàn bộ tổ chức, các bộ phận của tổ chức, một hệ thống thông tin cụ thể nào đó, các thành phần hệ thống nhất định, hoặc các dịch vụ mà ở đó có thể thực hiện đánh giá rủi ro một cách khả thi, thực tế, và hữu dụng. Các ví dụ về các hệ phương pháp đánh giá rủi ro được đề cập trong ISO/IEC TR 13335-3 (Các hướng dẫn quản lý an toàn công nghệ thông tin: Các kỹ thuật quản lý an toàn công nghệ thông tin).

3.2 Xử lý các rủi ro an toàn thông tin

Trước khi xem xét xử lý rủi ro, tổ chức cần quyết định tiêu chí để xác định liệu các rủi ro có được chấp nhận hay không. Ví dụ, các rủi ro có thể được chấp nhận nếu nó được đánh giá là rủi ro ở mức thấp, hay chi phí cho xử lý rủi ro không quá nặng nề đối với tổ chức. Các quyết định như vậy cần được ghi lại.

Cần đưa ra quyết định xử lý rủi ro đối với các rủi ro đã được xác định sau đánh giá rủi ro. Dưới đây là những lựa chọn nhằm xử lý rủi ro:

a) áp dụng các biện pháp quản lý thích hợp nhằm giảm bớt rủi ro;

b) chấp nhận các rủi ro một cách khách quan và có dụng ý, miễn là chúng thỏa mãn chính sách và tiêu chí chấp nhận rủi ro của tổ chức;

c) tránh rủi ro bằng cách không cho phép các hoạt động sẽ làm phát sinh rủi ro;

d) chuyển các rủi ro liên đới tới các bên khác, ví dụ các nhà bảo hiểm hoặc các nhà cung cấp.

Đối với các rủi ro mà việc quyết định xử lý rủi ro đã xác định phải áp dụng các biện pháp quản lý thích hợp thì những biện pháp quản lý này cần được lựa chọn và thực hiện để đáp ứng các yêu cầu được xác định bởi quá trình đánh giá rủi ro. Các biện pháp quản lý cần đảm bảo rằng các rủi ro được giảm tới một mức chấp nhận, và cần quan tâm tới các vấn đề sau:

a) các yêu cầu và các ràng buộc của pháp luật và các qui định trong nước và quốc tế;

b) các mục tiêu của tổ chức;

c) các yêu cầu và các ràng buộc về vận hành;

d) chi phí triển khai và vận hành liên quan tới các rủi ro sẽ được giảm thiểu, và duy trì tương quan đối với các yêu cầu và các ràng buộc của tổ chức;

e) nhu cầu cân bằng đầu tư trong quá trình triển khai và vận hành các biện pháp quản lý để chống lại thiệt hại có thể xảy ra do các lỗi về an toàn.

Các biện pháp quản lý có thể được chọn từ tiêu chuẩn này hoặc từ bộ các biện pháp quản lý khác, hoặc các biện pháp quản lý mới có thể được thiết kế phù hợp với các yêu cầu nhất định của tổ chức. Cũng cần phải thừa nhận rằng một số biện pháp quản lý có thể không phù hợp đối với mọi môi trường và mọi hệ thống thông tin, và có thể không khả thi đối với tất cả các tổ chức. Một ví dụ là, 9.1.3 mô tả cách phân tách nhiệm vụ nhằm ngăn chặn gian lận và sai sót. Các tổ chức có qui mô nhỏ hơn khó có thể phân tách tất cả các nhiệm vụ và như vậy có thể tìm các cách khác để đạt được mục tiêu quản lý tương tự. Một ví dụ khác là, 9.10 mô tả cách giám sát hệ thống và thu thập chứng cứ. Các biện pháp quản lý được mô tả, ví dụ ghi nhật ký sự kiện, có thể lại mâu thuẫn với các điều luật hiện hành, ví dụ luật bảo vệ sự riêng tư của các khách hàng hoặc tại nơi làm việc.

Các biện pháp quản lý an toàn thông tin cần được quan tâm ở giai đoạn thiết kế và xác định các yêu cầu đối với các dự án và các hệ thống. Lỗi ở giai đoạn này có thể làm phát sinh chi phí và giảm hiệu quả của các giải pháp, và trong trường hợp xấu nhất còn không thể đạt được sự an toàn thông tin một cách thỏa đáng.

Cần lưu ý rằng không tồn tại bộ các biện pháp quản lý giúp đạt được an toàn tuyệt đối, và cần thực hiện hoạt động quản lý bổ trợ nhằm giám sát, ước lượng, và nâng cao khả năng và tính hiệu quả của các biện pháp quản lý an toàn nhằm hướng đến các mục tiêu của tổ chức.

4 Chính sách an toàn thông tin

4.1 Chính sách an toàn thông tin

Mục tiêu: Nhằm cung cấp định hướng quản lý và hỗ trợ đảm bảo an toàn thông tin thỏa mãn với các yêu cầu trong hoạt động nghiệp vụ, môi trường pháp lý và các qui định phải tuân thủ.

Ban quản lý cần thiết lập định hướng chính sách rõ ràng phù hợp với các mục tiêu nghiệp vụ, hỗ trợ và cam kết về an toàn thông tin thông qua việc ban hành và duy trì một chính sách an toàn thông tin trong toàn bộ tổ chức.

4.1.1 Tài liệu chính sách an toàn thông tin

Biện pháp quản lý

Một tài liệu về chính sách an toàn thông tin cần phải được phê duyệt bởi ban quản lý và được cung cấp, thông báo tới mọi nhân viên cũng như các bên liên quan.

Hướng dẫn triển khai

Tài liệu chính sách an toàn thông tin cần công bố rõ cam kết của ban quản lý và đưa ra phương thức quản lý an toàn thông tin của tổ chức. Văn bản này cần bao gồm các nội dung sau:

a) định nghĩa về an toàn thông tin, các mục tiêu chung, phạm vi và tầm quan trọng của an toàn thông tin như là một cơ chế cho phép chia sẻ thông tin;

b) công bố về mục đích quản lý, hỗ trợ các mục tiêu và nguyên tắc an toàn thông tin phù hợp với chiến lược và các mục tiêu nghiệp vụ;

c) khuôn khổ cho việc thiết lập các mục tiêu quản lý và các biện pháp quản lý, bao gồm cơ cấu đánh giá và quản lý rủi ro;

d) giải thích ngắn gọn các chính sách, nguyên tắc, tiêu chuẩn an toàn, và các yêu cầu tuân thủ có tầm quan trọng đặc biệt đối với tổ chức, bao gồm:

   1) tuân thủ các yêu cầu của luật pháp, qui định, và hợp đồng;

   2) các yêu cầu về giáo dục, đào tạo và nhận thức về an toàn;

   3) quản lý tính liên tục của hoạt động nghiệp vụ;

   4) các hậu quả của các vi phạm chính sách an toàn thông tin;

e) định nghĩa các trách nhiệm chung và riêng về quản lý an toàn thông tin, bao gồm cả việc báo cáo các sự cố an toàn thông tin;

f) tham chiếu tới văn bản hỗ trợ chính sách, ví dụ các chính sách và thủ tục an toàn chi tiết hơn cho các hệ thống thông tin cụ thể hoặc các quy tắc an toàn mà người dùng bắt buộc phải tuân theo.

Chính sách an toàn thông tin này cần được tổ chức phổ biến đến người dùng theo một hình thức phù hợp, dễ truy cập và dễ hiểu.

Thông tin khác

Chính sách an toàn thông tin có thể là một phần của một văn bản chính sách chung nào đó. Nếu chính sách an toàn thông tin được phổ biến ra ngoài phạm vi của tổ chức thì cần lưu ý không tiết lộ những thông tin có tính chất nhạy cảm. Thông tin chi tiết hơn có thể tham khảo trong ISO/IEC 13335-1:2004.

4.1.2 Soát xét lại chính sách an toàn thông tin

Biện pháp quản lý

Chính sách an toàn thông tin cần thường xuyên được soát xét theo kế hoạch hoặc khi có những thay đổi lớn xuất hiện để luôn đảm bảo sự phù hợp, đầy đủ và thực sự có hiệu lực.

Hướng dẫn triển khai

Cần có một người chịu trách nhiệm trong việc phát triển, soát xét, và đánh giá chính sách an toàn thông tin. Quá trình soát xét cần đánh giá các cơ hội cải tiến chính sách an toàn thông tin của tổ chức và phương thức quản lý chính sách an toàn nhằm đáp ứng với những thay đổi của môi trường tổ chức, các tình huống nghiệp vụ, các điều kiện pháp lý, hoặc môi trường kỹ thuật.

Việc soát xét chính sách an toàn thông tin cần quan tâm đến các kết quả soát xét của ban quản lý. Cũng cần có các thủ tục soát xét nhất định của ban quản lý, bao gồm cả lịch trình hoặc chu kỳ soát xét.

Thông tin đầu vào của quá trình soát xét của ban quản lý cần bao gồm thông tin về:

a) phản hồi từ các bên quan tâm;

b) các kết quả soát xét một cách độc lập (xem 5.1.8);

c) trạng thái của các hoạt động phòng ngừa và sửa chữa (xem 5.1.8 và 14.2.1);

d) kết quả của các lần soát xét trước đó của ban quản lý;

e) sự tuân thủ chính sách an toàn thông tin và hiệu suất quy trình;

f) những thay đổi có thể ảnh hưởng đến phương thức quản lý an toàn thông tin của tổ chức, bao gồm những thay đổi về môi trường tổ chức, các tình huống nghiệp vụ, sự sẵn sàng của nguồn tài nguyên, các điều kiện về pháp lý, quy định và hợp đồng, hoặc môi trường kỹ thuật;

g) các xu hướng liên quan đến các mối đe dọa và các điểm yếu;

h) các sự cố an toàn thông tin đã được báo cáo (xem 12.1);

i) các khuyến nghị của các cơ quan liên quan (xem 5.1.6).

Đầu ra của quá trình soát xét của ban quản lý phải là các quyết định và hành động bất kỳ có liên quan đến:

a) việc cải tiến phương thức của tổ chức trong việc quản lý an toàn thông tin và các quy trình quản lý an toàn thông tin;

b) việc nâng cao các mục tiêu quản lý và các biện pháp quản lý;

c) việc cải tiến trong việc phân bổ các nguồn tài nguyên và/hoặc các trách nhiệm.

Cần duy trì hồ sơ về việc soát xét của ban quản lý.

Chính sách an toàn thông tin đã được chỉnh sửa cần có sự chấp thuận của ban quản lý.

5 Tổ chức đảm bảo an toàn thông tin

5.1 Tổ chức nội bộ

Mục tiêu: Nhằm quản lý an toàn thông tin bên trong tổ chức

Cần thiết lập một khuôn khổ quản lý nhằm khởi tạo và quản lý việc triển khai an toàn thông tin trong nội bộ tổ chức.

Ban quản lý cần thông qua chính sách an toàn thông tin, phân định các vai trò an toàn, phối hợp và soát xét việc triển khai thực hiện an toàn thông tin trong toàn bộ tổ chức.

Nếu cần thiết thì cần thiết lập và sẵn sàng có nguồn hỗ trợ chuyên môn về an toàn thông tin từ trong nội bộ của tổ chức. Cũng cần thiết lập những mối liên hệ với các nhóm hoặc các chuyên gia về an toàn thông tin ở bên ngoài nhằm có thể theo kịp các xu hướng công nghiệp, giám sát các tiêu chuẩn và các phương pháp đánh giá và đưa ra các điểm vận dụng phù hợp trong quá trình xử lý các sự cố về an toàn thông tin.

Cũng cần khuyến khích cách tiếp cận an toàn thông tin đa chiều.

5.1.1 Cam kết của ban quản lý về đảm bảo an toàn thông tin

Biện pháp quản lý

Ban quản lý phải chủ động hỗ trợ đảm bảo an toàn thông tin trong tổ chức bằng các định hướng rõ ràng, các cam kết có thể thấy được, các nhiệm vụ rõ ràng, và nhận thức rõ trách nhiệm về đảm bảo an toàn thông tin.

Hướng dẫn triển khai

Ban quản lý cần:

a) đảm bảo rằng các mục tiêu an toàn thông tin đã được xác định rõ, đáp ứng được các yêu cầu của tổ chức, và được đưa vào các quy trình liên quan;

b) trình bày một cách có hệ thống, soát xét và phê chuẩn chính sách an toàn thông tin;

c) soát xét tính hiệu quả của việc triển khai chính sách an toàn thông tin;

d) đưa ra định hướng rõ ràng và sự hỗ trợ rõ ràng của ban quản lý đối với các hoạt động an toàn thông tin;

e) cung cấp các nguồn tài nguyên cần thiết cho an toàn thông tin;

f) phê chuẩn sự phân định các vai trò và trách nhiệm cụ thể về an toàn thông tin trong toàn bộ tổ chức;

g) khởi động các chương trình và kế hoạch nhằm duy trì nhận thức về an toàn thông tin;

h) đảm bảo rằng việc triển khai các biện pháp quản lý an toàn thông tin được phối hợp trong toàn thể nội bộ tổ chức (xem 5.1.2).

Ban quản lý cần xác định rõ các nhu cầu cần có hỗ trợ chuyên môn về an toàn thông tin trong nội bộ hoặc bên ngoài tổ chức, soát xét và phối hợp các kết quả từ những hỗ trợ như vậy trong toàn bộ tổ chức.

Tùy thuộc vào quy mô của tổ chức, các trách nhiệm như vậy cũng có thể được xử lý bởi một diễn đàn quản lý riêng hoặc bởi một ban quản lý đương nhiệm, ví dụ ban giám đốc.

Thông tin khác

Thông tin chi tiết hơn tham khảo trong ISO/IEC 13335-1:2004.

5.1.2 Phối hợp đảm bảo an toàn thông tin

Biện pháp quản lý

Các hoạt động đảm bảo an toàn thông tin cần được phối hợp bởi các đại diện của các bộ phận trong tổ chức với vai trò và nhiệm vụ cụ thể.

Hướng dẫn triển khai

Về cơ bản thì các hoạt động an toàn thông tin cần có sự phối hợp và cộng tác của những người quản lý, người dùng, người quản trị mạng, những nhà thiết kế ứng dụng, những đánh giá viên và nhân viên an toàn, và các kỹ năng chuyên môn trong các lĩnh vực như bảo hiểm, pháp lý, nguồn nhân lực, quản lý rủi ro hoặc IT. Hoạt động này cần:

a) đảm bảo rằng các hoạt động an toàn được thực hiện tuân thủ theo chính sách an toàn thông tin;

b) xác định rõ phương thức xử lý những điểm không tuân thủ;

c) phê chuẩn các hệ phương pháp và các quy trình an toàn thông tin, ví dụ đánh giá rủi ro, phân loại thông tin;

d) xác định những thay đổi lớn về các mối đe dọa và chỉ ra các thông tin và các phương tiện xử lý thông tin bị đe dọa;

e) đánh giá tính phù hợp và phối hợp triển khai các biện pháp quản lý an toàn thông tin;

f) thúc đẩy việc giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin trên toàn tổ chức một cách hiệu quả;

g) đánh giá thông tin nhận được từ việc giám sát và soát xét các sự cố an toàn thông tin, và khuyến nghị các hoạt động phù hợp đối với các sự cố an toàn thông tin đã được xác định.

Nếu tổ chức không sử dụng riêng một nhóm chức năng chéo, ví dụ do nhóm kiểu này không phù hợp với quy mô của tổ chức, thì các hoạt động được mô tả ở trên cần được đảm trách bởi một ban quản lý thích hợp khác hoặc một người quản lý riêng.

5.1.3 Phân định trách nhiệm đảm bảo an toàn thông tin

Biện pháp quản lý

Tất cả các trách nhiệm đảm bảo an toàn thông tin cần được xác định một cách rõ ràng.

Hướng dẫn triển khai

Việc phân bổ các trách nhiệm về an toàn thông tin cần phù hợp với chính sách an toàn thông tin (xem điều 3). Các trách nhiệm về bảo vệ tài sản cá nhân và thực hiện các quy trình an toàn cụ thể cần được xác định rõ ràng. Nếu cần thiết thì trách nhiệm này cần được bổ sung bằng hướng dẫn chi tiết hơn về các vị trí công việc cụ thể và các phương tiện xử lý thông tin. Các trách nhiệm trong nội bộ về bảo vệ tài sản và thực hiện các quy trình an toàn đặc biệt, ví dụ lập kế hoạch đảm bảo tính liên tục về nghiệp vụ, cũng cần được xác định rõ.

Những cá nhân đã được phân bổ trách nhiệm về an toàn thông tin có thể ủy quyền các nhiệm vụ an toàn cho những người khác thực hiện. Tuy nhiên, họ vẫn phải duy trì trách nhiệm và đảm bảo rằng các nhiệm vụ đã được ủy quyền đều được thực hiện đúng cách thức.

Phạm vi trách nhiệm của các cá nhân có trách nhiệm cần được công bố rõ ràng; cụ thể là:

a) các tài sản và các quy trình an toàn đối với từng hệ thống cụ thể cần được xác định và định danh rõ ràng;

b) trách nhiệm đối với từng tài sản hoặc quy trình an toàn cần được phân định cụ thể và trách nhiệm chi tiết cần được ghi thành văn bản (xem 6.1.2);

c) các mức cấp phép cần được xác định rõ và ghi thành văn bản.

Thông tin khác

Trong nhiều tổ chức, một người quản lý an toàn thông tin sẽ được bổ nhiệm nhằm thực hiện trách nhiệm chung trong việc phát triển, triển khai công tác an toàn và hỗ trợ việc tìm ra các biện pháp quản lý phù hợp.

Tuy nhiên, trách nhiệm trong việc tìm ra và triển khai các biện pháp quản lý sẽ thường thuộc về những người quản lý cụ thể. Một thực tế thường thấy là phải chỉ định ra người sở hữu đối với từng tài sản, người này có trách nhiệm đối với việc bảo vệ tài sản hàng ngày.

5.1.4 Quy trình cấp phép cho phương tiện xử lý thông tin

Biện pháp quản lý

Một quy trình cấp phép cho phương tiện xử lý thông tin phải được xác định rõ và triển khai.

Hướng dẫn triển khai

Sau đây là các hướng dẫn đối với quy trình cấp phép:

a) những phương tiện mới cần có sự cấp phép sử dụng và mục đích sử dụng từ ban quản lý. Việc cấp phép cũng cần phải được người quản lý có trách nhiệm trong việc duy trì môi trường an toàn của hệ thống thông tin thông qua nhằm đảm bảo rằng tất cả các các chính sách và yêu cầu về an toàn đều được thỏa mãn;

b) khi cần thiết thì cần kiểm tra cả phần cứng và phần mềm nhằm đảm bảo rằng chúng đều tương thích với các thành phần hệ thống khác;

c) việc sử dụng các phương tiện xử lý thông tin thuộc sở hữu cá nhân, ví dụ máy tính xách tay, máy tính tại nhà riêng, hoặc các thiết bị cầm tay, nhằm xử lý thông tin nghiệp vụ có thể làm phát sinh những yếu điểm mới và vì vậy, cần xác định và triển khai các biện pháp quản lý cần thiết.

5.1.5 Các thỏa thuận về bảo mật

Biện pháp quản lý

Các yêu cầu về bảo mật hoặc các thỏa thuận không tiết lộ phản ánh nhu cầu của tổ chức đối với việc bảo vệ thông tin phải được xác định rõ và thường xuyên soát xét lại.

Hướng dẫn triển khai

Các thỏa thuận bảo mật hoặc không tiết lộ cần tập trung vào các yêu cầu nhằm bảo vệ thông tin mật với các điều khoản có khả năng thực thi về mặt pháp lý. Khi xác định các yêu cầu đối với các thỏa thuận bảo mật hoặc không tiết lộ, cần quan tâm đến các yếu tố sau:

a) định nghĩa về thông tin cần được bảo vệ (ví dụ, thông tin mật);

b) khoảng thời gian dự kiến của thỏa thuận, bao gồm cả các trường hợp yêu cầu bảo mật không thời hạn;

c) các hoạt động được yêu cầu khi kết thúc thỏa thuận;

d) các trách nhiệm và hành động của các bên ký kết nhằm tránh tiết lộ thông tin trái phép;

e) quyền sở hữu thông tin, các bí mật giao dịch và quyền sở hữu trí tuệ, và mối quan hệ của chúng với việc bảo vệ thông tin mật;

f) việc được phép sử dụng thông tin mật và các quyền của người ký kết sử dụng thông tin;

g) quyền đánh giá và giám sát các hoạt động liên quan đến thông tin mật;

h) quy trình thông báo và báo cáo về việc tiết lộ trái phép hoặc những lỗ hổng thông tin mật;

i) các điều khoản đối với thông tin được trả về hoặc bị hủy khi chấm dứt thỏa thuận;

j) các hành động dự kiến trong trường hợp có vi phạm thỏa thuận.

Dựa trên các yêu cầu về an toàn thông tin của tổ chức, có thể đưa thêm một số điều khoản khác vào thỏa thuận không tiết lộ hoặc thỏa thuận bảo mật.

Các thỏa thuận bảo mật và không tiết lộ cần tuân thủ tất cả những quy định và điều luật phù hợp (xem thêm 14.1.1);

Các yêu cầu đối với các thỏa thuận bảo mật và không tiết lộ cần được soát xét định kỳ và tại các thời điểm xảy ra thay đổi làm ảnh hưởng đến các yêu cầu này.

Thông tin khác

Các thỏa thuận bảo mật hoặc không tiết lộ sẽ bảo vệ các thông tin của tổ chức và thông báo cho các bên ký kết về trách nhiệm của họ trong việc bảo vệ, sử dụng và tiết lộ thông tin một cách có trách nhiệm và đúng thẩm quyền.

Mỗi tổ chức cũng cần sử dụng các hình thức thỏa thuận bảo mật hoặc không tiết lộ khác nhau theo từng tình huống cụ thể.

5.1.6 Liên lạc với những cơ quan/tổ chức có thẩm quyền

Biện pháp quản lý

Phải duy trì liên lạc thỏa đáng với những cơ quan có thẩm quyền liên quan.

Hướng dẫn triển khai

Các tổ chức cần có các thủ tục xác định khi nào và ai sẽ liên hệ với các cơ quan có thẩm quyền (ví dụ, cơ quan thi hành luật, cảnh sát phòng cháy chữa cháy, các cơ quan giám sát), và cách thức báo cáo các sự cố an toàn thông tin đã xác định một cách kịp thời nếu có nghi ngờ đã có sự vi phạm luật.

Các tổ chức bị tấn công từ Internet có thể cần các bên thứ ba (ví dụ, một nhà cung cấp dịch vụ Internet hoặc một nhà khai thác viễn thông) tiến hành các hoạt động chống lại nguồn gốc tấn công.

Thông tin khác

Việc duy trì những liên lạc như vậy có thể là một yêu cầu giúp hỗ trợ quản lý các sự cố an toàn thông tin (xem 12.2) hoặc quá trình lập kế hoạch nghiệp vụ đột xuất và liên tục (xem 13). Các mối liên hệ với các cơ quan luật pháp cũng sẽ có lợi cho công tác dự báo và chuẩn bị cho những thay đổi sắp xảy ra trên phương diện luật pháp hoặc các quy định mà các tổ chức bắt buộc phải tuân theo. Những liên hệ với những cơ quan có thẩm quyền khác bao gồm cả các dịch vụ khẩn cấp, tiện ích, sức khỏe và an toàn, ví dụ các sở cứu hỏa (có liên quan đến sự liên tục về nghiệp vụ), các nhà cung cấp dịch vụ viễn thông (có liên quan đến độ sẵn sàng), các nhà cung cấp nước (có liên quan đến các phương tiện làm mát cho thiết bị).

5.1.7 Liên lạc với các nhóm chuyên gia

Biện pháp quản lý

Phải giữ liên lạc với các nhóm chuyên gia hoặc các diễn đàn và hiệp hội an toàn thông tin.

Hướng dẫn triển khai

Cần coi các thành viên trong các diễn đàn hoặc các nhóm chuyên gia như phương tiện nhằm:

a) nâng cao kiến thức về cách thức thực hành tốt nhất và cập nhật những thông tin có liên quan về an toàn;

b) đảm bảo rằng kiến thức về môi trường an toàn thông tin là đầy đủ và được phổ biến;

c) nhận được các cảnh báo sớm từ các cảnh báo, những lời tư vấn, và các bản vá liên quan đến những tấn công và những yếu điểm;

d) tiếp cận đến những lời khuyên của chuyên gia an toàn thông tin;

e) chia sẻ và trao đổi thông tin về các công nghệ, sản phẩm, những mối đe dọa hoặc những yếu điểm mới;

f) cung cấp những đầu mối liên hệ phù hợp khi giải quyết các sự cố về an toàn thông tin (xem thêm 12.2.1).

Thông tin khác

Có thể thiết lập những thỏa thuận về chia sẻ thông tin nhằm nâng cao sự phối hợp và cộng tác về các vấn đề an toàn. Những thỏa thuận như vậy cần xác định các yêu cầu về việc bảo vệ thông tin nhạy cảm.

5.1.8 Soát xét độc lập về an toàn thông tin

Biện pháp quản lý

Cách tiếp cận quản lý an toàn thông tin của tổ chức và việc triển khai của tổ chức (chẳng hạn như: các mục tiêu và biện pháp quản lý, các chính sách, các quá trình và thủ tục đảm bảo an toàn thông tin) phải được soát xét định kỳ hoặc khi xuất hiện những thay đổi quan trọng liên quan đến an toàn thông tin.

Hướng dẫn triển khai

Việc soát xét một cách độc lập cần được thực hiện bởi ban quản lý. Việc soát xét như vậy là cần thiết nhằm đảm bảo tính phù hợp, tính vẹn toàn và tính hiệu quả liên tục của phương thức triển khai an toàn thông tin của tổ chức. Việc soát xét cần bao gồm cả việc đánh giá các cơ hội trong việc cải tiến và nhu cầu cần có những thay đổi về phương thức an toàn, bao gồm cả chính sách và các mục tiêu quản lý.

Việc soát xét như vậy cũng cần được thực hiện bởi các cá nhân độc lập trong khu vực soát xét, ví dụ những người có chức năng đánh giá nội bộ, người quản lý độc lập hoặc một tổ chức bên thứ ba chuyên thực hiện những cuộc soát xét như vậy. Các cá nhân thực hiện các cuộc soát xét cần có các kỹ năng và kinh nghiệm phù hợp.

Các kết quả của những lần soát xét độc lập cần được ghi lại và báo cáo đến ban quản lý. Các bản báo cáo này cần được lưu lại.

Nếu một cuộc soát xét độc lập cho thấy rằng phương thức và việc triển khai của tổ chức trong quản lý an toàn thông tin là không phù hợp hoặc không tuân thủ chỉ dẫn về an toàn thông tin đã được công bố trong văn bản chính sách an toàn thông tin (xem 4.1.1) thì ban quản lý cần cân nhắc đến việc sửa đổi.

Thông tin khác

Các khu vực mà những người quản lý cần soát xét định kỳ cũng có thể cần được soát xét độc lập (xem 14.2.1). Các kỹ thuật soát xét có thể bao gồm các cuộc phỏng vấn của ban quản lý, kiểm tra sổ sách ghi chép hoặc soát xét các văn bản về chính sách an toàn. ISO 19011:2002, Hướng dẫn đánh giá các hệ thống quản lý môi trường và/hoặc chất lượng, cũng có thể là một hướng dẫn rất hữu ích cho việc thực hiện soát xét độc lập, trong đó bao gồm việc thiết lập và triển khai một chương trình soát xét. 14.3

sẽ tập trung vào các biện pháp quản lý liên quan đến soát xét độc lập các hệ thống thông tin điều hành và việc sử dụng các công cụ đánh giá hệ thống.

5.2 Các bên tham gia bên ngoài

Mục tiêu: Nhằm duy trì an toàn đối với thông tin và các phương tiện xử lý thông tin của tổ chức được truy cập, xử lý, truyền tới, hoặc quản lý bởi các bên tham gia bên ngoài tổ chức.

Tính an toàn của thông tin và các phương tiện xử lý thông tin của tổ chức không được bị làm thuyên giảm bởi sự xuất hiện của các sản phẩm hoặc dịch vụ của tổ chức bên ngoài.

Cần quản lý tất cả các truy cập tới các phương tiện xử lý thông tin của tổ chức; việc xử lý và truyền thông được thực hiện bởi các tổ chức bên ngoài.

Khi có nhu cầu nghiệp vụ cần làm việc với các tổ chức bên ngoài mà công việc ấy có thể đòi hỏi phải truy cập đến thông tin và các phương tiện xử lý thông tin của tổ chức, hoặc có nhu cầu cần nhận được hoặc cung cấp một sản phẩm và dịch vụ từ hoặc tới một tổ chức bên ngoài thì cần thực hiện đánh giá rủi ro nhằm xác định các ảnh hưởng liên quan đến an toàn thông tin và các yêu cầu về biện pháp quản lý. Các biện pháp quản lý cũng cần được thỏa thuận và xác định trong một bản thỏa thuận với tổ chức bên ngoài.

5.2.1 Xác định các rủi ro liên quan đến các bên tham gia bên ngoài

Biện pháp quản lý

Các rủi ro đối với thông tin và các phương tiện xử lý thông tin của tổ chức từ các quy trình nghiệp vụ liên quan đến các bên tham gia bên ngoài phải được nhận biết và triển khai biện pháp quản lý thích hợp trước khi cấp quyền truy cập.

Hướng dẫn triển khai

Khi có nhu cầu cho phép tổ chức bên ngoài truy cập đến các phương tiện xử lý thông tin hoặc thông tin của tổ chức thì cần thực hiện đánh giá rủi ro (xem điều 3) nhằm xác định các yêu cầu đối với các biện pháp quản lý cụ thể. Việc xác định các rủi ro liên quan đến truy cập của tổ chức bên ngoài cần xem xét các yếu tố sau:

a) các phương tiện xử lý thông tin mà tổ chức bên ngoài được yêu cầu truy cập;

b) hình thức truy cập mà tổ chức bên ngoài sẽ thực hiện đối với thông tin và các phương tiện xử lý thông tin, ví dụ:

   1) truy cập mức vật lý, ví dụ tới các văn phòng, các phòng máy tính, các ngăn tài liệu;

   2) truy cập logic, ví dụ đến cơ sở dữ liệu, hệ thống thông tin của tổ chức;

   3) kết nối mạng giữa mạng của tổ chức và của tổ chức bên ngoài, ví dụ kết nối cố định, truy cập từ xa;

4) truy cập được thực hiện tại chỗ hay từ xa;

c) giá trị và độ nhạy cảm của thông tin liên quan, và sự quan trọng của nó đối với các hoạt động nghiệp vụ;

d) các biện pháp quản lý cần thiết nhằm bảo vệ những thông tin mà các tổ chức bên ngoài không được quyền truy cập;

e) nhân viên thuộc tổ chức bên ngoài tham gia vào việc xử lý thông tin của tổ chức;

f) có thể cần xác định cách thức truy cập mà tổ chức hoặc cá nhân được cấp phép, cần kiểm tra giấy phép, và xác định khoảng thời gian cần xác minh lại việc cấp phép;

g) các phương tiện và các biện pháp kiểm soát khác nhau được tổ chức bên ngoài sử dụng khi lưu trữ, xử lý, truyền thông, chia sẻ và trao đổi thông tin;

h) ảnh hưởng của việc truy cập chưa sẵn sàng đối với tổ chức bên ngoài khi có yêu cầu, và việc nhập vào hoặc nhận thông tin không chính xác hoặc sai lệch của tổ chức bên ngoài;

i) các thủ tục và biện pháp xử lý sự cố an toàn thông tin và các thiệt hại tiềm ẩn, các điều kiện và điều khoản truy cập của tổ chức bên ngoài trong trường hợp có xảy ra sự cố an toàn thông tin;

j) Các yêu cầu pháp lý và quy tắc và các nghĩa vụ thỏa thuận liên quan đến tổ chức bên ngoài;

Không được cho phép các tổ chức bên ngoài truy cập tới thông tin của tổ chức trừ khi đã triển khai các biện pháp quản lý phù hợp, và nếu khả thi thì cần ký một bản hợp đồng xác định thời hạn và các điều kiện kết nối hoặc truy cập. Nhìn chung, tất cả các yêu cầu về an toàn khi làm việc với các tổ chức bên ngoài hoặc các biện pháp quản lý bên trong cần được đề cập trong một bản thỏa thuận với tổ chức bên ngoài (xem thêm trong 5.2.2 và 5.2.3).

Cũng cần đảm bảo rằng tổ chức bên ngoài nhận thức được các nghĩa vụ của họ, và chấp thuận các trách nhiệm và nghĩa vụ pháp lý khi truy cập, xử lý, truyền thông, hoặc quản lý thông tin và các phương tiện xử lý thông tin của tổ chức.

Thông tin khác

Thông tin có thể bị rủi ro do các tổ chức thứ ba quản lý an toàn thông tin không phù hợp. Các biện pháp quản lý cần được xác định và sử dụng nhằm quản lý việc truy cập của tổ chức bên ngoài tới các phương tiện xử lý thông tin. Ví dụ, nếu có yêu cầu đặc biệt về tính bí mật của thông tin thì có thể sử dụng các thỏa thuận không tiết lộ thông tin.

Các tổ chức có thể phải đối mặt với những rủi ro liên quan đến việc xử lý, quản lý và truyền thông liên tổ chức nếu áp dụng thuê khoán ngoài ở mức độ cao, hoặc có sự tham gia của nhiều tổ chức.

Các biện pháp quản lý trong 5.2.2 và 5.2.3 bao hàm các biện pháp khi làm việc với nhiều loại tổ chức thứ ba, ví dụ bao gồm:

a) các nhà cung cấp dịch vụ, như ISP, các nhà cung cấp mạng, các dịch vụ điện thoại, các dịch vụ hỗ trợ và bảo trì;

b) các dịch vụ an toàn được quản lý;

c) các khách hàng;

d) thuê khoán các thiết bị và/hoặc các dịch vụ điều hành, ví dụ các hệ thống IT, các dịch vụ thu thập dữ liệu, các trung tâm khai thác cuộc gọi;

e) các nhà tư vấn về quản lý và nghiệp vụ và các đánh giá viên;

f) các nhà cung cấp và phát triển, ví dụ các hệ thống IT và các sản phẩm phần mềm;

g) các dịch vụ vệ sinh, rác thải và các dịch vụ hỗ trợ được thuê khoán khác;

h) lao động tạm thời, sử dụng sinh viên, và các vị trí ngắn hạn khác;

Những thỏa thuận này có thể giúp làm giảm các rủi ro liên quan tới các tổ chức bên ngoài.

5.2.2 Giải quyết an toàn khi làm việc với khách hàng

Biện pháp quản lý

Tất cả các yêu cầu về an toàn phải được giải quyết trước khi cho phép khách hàng truy cập tới thông tin hoặc tài sản của tổ chức.

Hướng dẫn triển khai

Cần quan tâm đến các vấn đề sau nhằm giải quyết an toàn thông tin trước khi cho phép khách hàng truy cập đến bất kỳ tài sản nào của tổ chức (tùy thuộc vào loại và quy mô của truy cập, không phải áp dụng toàn bộ):

a) bảo vệ tài sản, bao gồm:

   1) các quy trình bảo vệ các tài sản của tổ chức, bao gồm thông tin và phần mềm, và quản lý các yếu điểm đã biết trước;

   2) các thủ tục xác định tổn hại đến tài sản, ví dụ dữ liệu có bị mất hoặc bị làm thay đổi không;

   3) tính toàn vẹn;

   4) hạn chế việc sao chép và tiết lộ thông tin;

b) mô tả sản phẩm hoặc dịch vụ được cung cấp;

c) các lý do, yêu cầu khác nhau, và các lợi ích trong việc truy cập của khách hàng;

d) chính sách quản lý truy cập, bao gồm:

   1) các phương pháp truy cập được cho phép, biện pháp quản lý và sử dụng các thông tin cá nhân như ID và mật khẩu của người dùng;

2) một quy trình cấp phép truy cập và đặc quyền cho người dùng;

3) một thông báo rằng tất cả các truy cập chưa được cấp phép hợp lệ đều bị cấm;

4) một quy trình thu hồi quyền truy cập hoặc ngắt kết nối giữa các hệ thống;

e) các bước thực hiện báo cáo, thông báo, và điều tra về về những sai lệch của thông tin (ví dụ các thông tin chi tiết về cá nhân), các sự cố an toàn thông tin và các lỗ hổng bảo mật;

f) mô tả về từng dịch vụ sẽ được cung cấp;

g) mức kỳ vọng của dịch vụ và các mức không chấp nhận được của dịch vụ;

h) quyền giám sát, thu hồi, và thực hiện hoạt động bất kỳ liên quan đến các tài sản của tổ chức;

i) các nghĩa vụ tương ứng của tổ chức và khách hàng;

j) các trách nhiệm liên quan đến các vấn đề luật pháp và phương thức nhằm đảm bảo rằng các yêu cầu về luật pháp đều được đáp ứng, ví dụ cưỡng chế bảo vệ dữ liệu, đặc biệt là phải tính đến các hệ thống luật pháp quốc gia khác nếu thỏa thuận có sự phối hợp với các khách hàng ở các quốc gia khác (xem thêm trong 14.1);

k) các quyền sở hữu trí tuệ (IPR) và vấn đề bản quyền (xem 14.1.2) và việc bảo vệ các kết quả công việc có sự cộng tác (xem thêm 5.1.5).

Thông tin khác

Các yêu cầu về an toàn thông tin liên quan đến các khách hàng truy cập vào tài sản của tổ chức có thể rất khác nhau tùy theo các phương tiện xử lý thông tin và thông tin đang bị truy cập. Các yêu cầu về an toàn này có thể được đề cập trong các thỏa thuận với khách hàng, các thỏa thuận này bao gồm tất cả các rủi ro và các yêu cầu an toàn đã xác định (xem 5.2.1).

Các thỏa thuận với các tổ chức bên ngoài cũng có thể bao gồm các bên khác. Các thỏa thuận chấp nhận việc truy cập của tổ chức bên ngoài cần bao gồm cả việc cho phép chỉ định các tổ chức có đủ tư cách khác, các điều kiện truy cập và sự tham gia của họ

5.2.3 Giải quyết an toàn trong các thỏa thuận với bên thứ ba

Biện pháp quản lý

Các thỏa thuận với bên thứ ba liên quan đến truy cập, xử lý, truyền thông, quản lý thông tin và các phương tiện xử lý thông tin của tổ chức, hoặc các sản phẩm, dịch vụ phụ trợ của các phương tiện xử lý thông tin phải bao hàm tất cả các yêu cầu an toàn có liên quan.

Hướng dẫn triển khai

Thỏa thuận cần đảm bảo rằng không có sự hiểu nhầm giữa tổ chức và bên thứ ba.

Các điều khoản sau cần được xem xét đưa vào bản thỏa thuận nhằm thỏa mãn các yêu cầu an toàn đã xác định (xem 5.2.1):

a) chính sách an toàn thông tin;

b) các biện pháp quản lý nhằm đảm bảo tài sản được bảo vệ, bao gồm:

1) các thủ tục bảo vệ tài sản của tổ chức, bao gồm thông tin, phần mềm và phần cứng;

2) các cơ chế và biện pháp quản lý vật lý được yêu cầu;

3) các biện pháp quản lý nhằm đảm bảo việc bảo vệ chống lại phần mềm độc hại;

4) các thủ tục xác định xem có tổn hại nào đến tài sản hay không, ví dụ mất mát hoặc chỉnh sửa thông tin, phần mềm và phần cứng;

5) các biện pháp quản lý nhằm đảm bảo khôi phục hoặc cấu trúc lại thông tin và tài sản khi kết thúc hoặc tại một thời điểm thỏa thuận trong toàn bộ giai đoạn hiệu lực của thỏa thuận;

6) tính bí mật, tính toàn vẹn, tính sẵn sàng, và thuộc tính liên quan bất kỳ của các tài sản;

7) các hạn chế về sao chép và tiết lộ thông tin, và áp dụng các thỏa thuận về bảo mật (xem 5.1.5);

c) đào tạo người dùng và người quản lý về các phương pháp, thủ tục và an toàn thông tin;

d) đảm bảo rằng người dùng hiểu về các vai trò và trách nhiệm của mình về an toàn thông tin;

e) các quy định về điều chuyển nhân sự khi có yêu cầu;

f) các trách nhiệm về lắp đặt và bảo dưỡng phần cứng và phần mềm;

g) cấu trúc báo cáo rõ ràng và các định dạng báo cáo đã thỏa thuận;

h) quy trình rõ ràng về quản lý các thay đổi;

i) chính sách giám sát truy cập, bao gồm:

1) các lý do, yêu cầu và lợi ích khác nhau chứng minh nhu cầu cần truy cập của tổ chức thứ ba;

2) các phương pháp truy cập được phép, quản lý và sử dụng các thông tin cá nhân như ID và mật khẩu của người dùng;

3) một quy trình cấp phép truy cập và đặc quyền đối với người dùng;

4) một yêu cầu duy trì danh sách các cá nhân được cấp phép sử dụng dịch vụ, và quyền và đặc quyền truy cập của họ;

5) một thông báo rằng tất cả các truy cập chưa được cấp phép một cách hợp lệ đều bị cấm;

6) một quy trình thu hồi quyền truy cập hoặc ngắt kết nối giữa các hệ thống;

j) các thủ tục báo cáo, thông báo và điều tra về các sự cố an toàn thông tin và các lỗ hổng an toàn, cũng như những vi phạm các yêu cầu đã công bố trong bản thỏa thuận;

k) mô tả về sản phẩm hoặc dịch vụ được cung cấp, và mô tả về thông tin đã sẵn sàng cùng với phân cấp an toàn của thông tin (xem 6.2.1);

l) mức kỳ vọng của dịch vụ và các mức không chấp nhận được của dịch vụ;

m) định nghĩa về chỉ tiêu hiệu suất, việc giám sát và báo cáo chúng;

n) quyền giám sát, và thu hồi, khai thác liên quan đến các tài sản của tổ chức;

o) quyền được đánh giá các trách nhiệm đã xác định trong thỏa thuận, quyền được thuê tổ chức thứ ba thực hiện các công việc đánh giá, và quyền được công bố các quyền do luật pháp quy định của nhân viên đánh giá;

p) thiết lập quy trình nâng dần cấp xử lý để xử lý sự cố;

q) các yêu cầu về tính liên tục của dịch vụ, bao gồm các chỉ tiêu về độ sẵn sàng và độ tin cậy, phù hợp với các thứ tự ưu tiên về nghiệp vụ;

r) các nghĩa vụ pháp lý tương ứng của các tổ chức theo thỏa thuận;

s) các trách nhiệm đối với các vấn đề pháp lý và phương thức nhằm đảm bảo rằng các yêu cầu pháp lý đều được thỏa mãn, ví dụ cưỡng chế bảo vệ dữ liệu, đặc biệt quan tâm đến các hệ thống luật pháp quốc gia khác nếu thỏa thuận có sự hợp tác với các tổ chức của các quốc gia khác (xem thêm 14.1);

t) các quyền sở hữu trí tuệ (IPR) và đăng ký bản quyền (xem 14.1.2) và bảo vệ công việc có sự phối hợp cộng tác (xem thêm 5.1.5);

u) nếu việc hợp tác với tổ chức thứ ba có thêm các nhà thầu phụ thì cần triển khai các biện pháp quản lý an toàn đối với các nhà thầu phụ này;

v) các điều kiện thương lượng lại/hủy bỏ các thỏa thuận:

   1) cần thực hiện một kế hoạch đột xuất trong trường hợp cả hai phía đều mong muốn kết thúc mối quan hệ trước thời điểm kết thúc thỏa thuận như đã định;

   2) thương lượng lại các thỏa thuận nếu các yêu cầu về an toàn của tổ chức thay đổi;

   3) lập tài liệu danh sách các tài sản, các giấy phép, các thỏa thuận hoặc quyền liên quan đến chúng.

Các thông tin khác

Các thỏa thuận có thể rất khác nhau tùy theo các loại các tổ chức khác nhau và giữa các loại bên thứ ba khác nhau. Do vậy, cần cẩn trọng việc đưa ra các rủi ro và các yêu cầu về an toàn (xem thêm 5.2.1)

trong các thỏa thuận. Khi cần thiết thì có thể mở rộng các biện pháp quản lý và các thủ tục cần thiết trong kế hoạch quản lý an toàn.

Nếu tổ chức thuê bên thứ ba quản lý an toàn thông tin, thì các thỏa thuận cần nhấn mạnh cách thức mà bên thứ ba cần nhằm đảm bảo đạt được độ an toàn thỏa đáng như đã xác định bởi công tác đánh giá rủi ro, và cách thức xác định và xử lý những thay đổi của các rủi ro.

Một vài trong số các khía cạnh khác nhau giữa thuê khoán và các hình thức cung cấp dịch vụ khác của bên thứ ba bao gồm vấn đề về nghĩa vụ pháp lý, việc lập kế hoạch về giai đoạn chuyển đổi và sự đổ vỡ tiềm ẩn của các hoạt động giai đoạn này, các công việc chuẩn bị cho việc lập kế hoạch đột xuất, thu thập và quản lý thông tin về các sự cố an toàn thông tin. Do vậy, vấn đề quan trọng là tổ chức phải lập kế hoạch và quản lý giai đoạn chuyển sang thuê khoán và có những xử lý phù hợp nhằm quản lý những thay đổi và thương lượng lại/kết thúc các thỏa thuận.

Các thủ tục duy trì xử lý thông tin trong trường hợp bên thứ ba không có khả năng cung cấp dịch vụ cũng cần được xem xét trong thỏa thuận nhằm ngăn chặn trì hoãn dàn xếp các dịch vụ thay thế.

Các thỏa thuận với bên thứ ba có thể có sự tham gia của các bên khác. Các thỏa thuận chấp nhận cho bên thứ ba truy cập cần cho phép chỉ định các bên có đủ tư cách khác và các điều kiện truy cập và tham gia của họ.

Nhìn chung các thỏa thuận chủ yếu đều được triển khai bởi tổ chức. Có thể có một số trường hợp mà bên thứ ba triển khai và áp đặt thỏa thuận đối với tổ chức. Tổ chức cần đảm bảo rằng an toàn thông tin của bản thân tổ chức sẽ không bị tác động một cách không cần thiết bởi các yêu cầu của tổ chức thứ ba được quy định trong các thỏa thuận áp đặt.

6 Quản lý tài sản

6.1 Trách nhiệm đối với tài sản

Mục tiêu: Nhằm hoàn thành và duy trì các biện pháp bảo vệ thích hợp đối với tài sản của tổ chức.

Tất cả các tài sản đều cần được kê khai và giao cho một người sở hữu.

Những người sở hữu tài sản cần được xác định đối với tất cả các tài sản và được giao trách nhiệm trong việc duy trì các biện pháp quản lý phù hợp. Nếu thích hợp thì người sở hữu tài sản có thể ủy quyền cho người khác triển khai các biện pháp quản lý nhất định nào đó nhưng người sở hữu vẫn phải duy trì trách nhiệm trong việc bảo vệ tài sản.

6.1.1 Kiểm kê tài sản

Biện pháp quản lý

Mọi tài sản cần được xác định rõ ràng, cần thực hiện và duy trì kiểm kê đối với tất cả các tài sản quan trọng.

Hướng dẫn triển khai

Tổ chức cần xác định tất cả các tài sản và tầm quan trọng của các tài sản này cần được ghi vào văn bản. Biên bản kiểm kê tài sản cần chứa tất cả các thông tin cần thiết nhằm phục vụ việc khôi phục thông tin trong trường hợp có thảm họa, bao gồm loại tài sản, định dạng, vị trí, thông tin dự phòng, thông tin đăng ký, và giá trị nghiệp vụ. Biên bản kiểm kê không được sao chép các biên bản kiểm kê khác những thông tin không cần thiết, nhưng cần đảm bảo nội dung thống nhất.

Hơn nữa, quyền sở hữu (xem 6.1.2) và phân loại thông tin (xem 6.2) đối với các tài sản cần được thỏa thuận và ghi thành văn bản. Các mức độ bảo vệ tương ứng với tầm quan trọng của các tài sản cũng cần được xác định dựa trên tầm quan trọng của các tài sản, giá trị nghiệp vụ và phân loại an toàn của tài sản đó (xem ISO/IEC TR 13335-3 để có thông tin chi tiết hơn về cách thức định giá các tài sản nhằm thể hiện được tầm quan trọng của chúng).

Thông tin khác

Có rất nhiều loại tài sản, bao gồm:

a) thông tin: cơ sở dữ liệu và các tệp dữ liệu, các hợp đồng và thỏa thuận, văn bản về hệ thống, thông tin tìm kiếm, hướng dẫn sử dụng, tài liệu tập huấn, các thủ tục khai thác hoặc hỗ trợ, các kế hoạch nghiệp vụ liên tục, các truy vết, và thông tin thu thập được;

b) các tài sản phần mềm: phần mềm ứng dụng, phần mềm hệ thống, các công cụ phát triển, và các tiện ích;

c) các tài sản vật chất: thiết bị máy tính, thiết bị truyền thông, thiết bị di động và các thiết bị khác;

d) các dịch vụ: các dịch vụ truyền thông và tính toán, các tiện ích chung, ví dụ sưởi, chiếu sáng, năng lượng, và điều hòa nhiệt độ;

e) con người, và các văn bằng chứng chỉ, các kỹ năng và kinh nghiệm của họ;

f) tài sản vô hình, như danh tiếng và hình ảnh của tổ chức.

Các cuộc kiểm kê tài sản giúp đảm bảo rằng việc bảo vệ tài sản một cách hiệu quả đã được thực hiện, và có thể được yêu cầu cho các mục đích nghiệp vụ khác, như các lý do về sức khỏe và an toàn, bảo hiểm hoặc tài chính (quản lý tài sản). Quy trình kiểm kê tài sản là một điều kiện tiên quyết vô cùng quan trọng trong quản lý rủi ro (xem thêm điều 3).

6.1.2 Quyền sở hữu tài sản

Biện pháp quản lý

Mọi thông tin và tài sản gắn với phương tiện xử lý thông tin phải được quản lý, kiểm soát bởi một bộ phận do tổ chức chỉ định.

Hướng dẫn triển khai

Người sở hữu tài sản cần có trách nhiệm trong việc:

a) đảm bảo rằng thông tin và các tài sản liên quan đến các phương tiện xử lý thông tin được phân loại phù hợp;

b) xác định và định kỳ soát xét lại các giới hạn và phân loại truy cập, cân nhắc các chính sách quản lý truy cập có thể áp dụng.

Quyền sở hữu có thể được chỉ định cho:

a) một quy trình nghiệp vụ;

b) các hoạt động nhất định;

c) một ứng dụng; hoặc

d) một tập các dữ liệu xác định;

Thông tin khác

Có thể ủy quyền thực hiện các nhiệm vụ thông thường, ví dụ ủy quyền cho một người chăm sóc tài sản hàng ngày, nhưng người sở hữu vẫn phải duy trì trách nhiệm của họ.

Với các hệ thống thông tin phức tạp, thì có thể gom tài sản vào thành các nhóm, các nhóm hình thành một chức năng đặc biệt giống như "các dịch vụ". Trong trường hợp này, người sở hữu dịch vụ có trách nhiệm phân phối dịch vụ, bao gồm cả việc thực hiện chức năng của các tài sản.

6.1.3 Sử dụng hợp lý tài sản

Biện pháp quản lý

Các quy tắc sử dụng hợp lý thông tin và tài sản gắn với phương tiện xử lý thông tin phải được xác định, ghi thành văn bản và triển khai.

Hướng dẫn triển khai

Tất cả nhân viên, người của nhà thầu và bên thứ ba cần tuân theo các quy tắc sử dụng được phép các thông tin và tài sản liên quan đến các phương tiện xử lý thông tin, bao gồm:

a) các quy tắc sử dụng internet và thư điện tử (xem 9.8);

b) các hướng dẫn sử dụng các thiết bị di động, đặc biệt là sử dụng ở bên ngoài trụ sở của tổ chức (xem 10.7.1);

Các quy tắc hoặc hướng dẫn cụ thể cần được ban quản lý liên quan đề xuất. Những nhân viên, các nhà thầu và những người dùng thuộc tổ chức thứ ba đang sử dụng hoặc đang truy cập tới tài sản của tổ chức cần phải biết các giới hạn đang áp dụng trong việc sử dụng thông tin và tài sản của tổ chức liên quan đến các phương tiện xử lý thông tin và các nguồn tài nguyên. Họ cần có trách nhiệm trong việc sử dụng mọi nguồn tài nguyên xử lý thông tin và mọi hình thức sử dụng tài nguyên xử lý thông tin theo trách nhiệm của họ.

6.2 Phân loại thông tin

Mục tiêu: Nhằm đảm bảo thông tin sẽ có mức độ bảo vệ thích hợp.

Thông tin cần được phân loại nhằm chỉ ra nhu cầu, độ ưu tiên, và mức độ bảo vệ dự kiến khi xử lý thông tin.

Thông tin có các mức độ nhạy cảm và độ quan trọng thay đổi. Một số danh mục thông tin có thể cần mức bảo vệ cao hơn hoặc cần được xử lý đặc biệt. Cần sử dụng cơ chế phân loại thông tin nhằm xác định tập các mức bảo vệ phù hợp và trao đổi về nhu cầu cần có các biện pháp xử lý đặc biệt.

6.2.1 Hướng dẫn phân loại

Biện pháp quản lý

Thông tin cần được phân loại theo giá trị, các yêu cầu pháp lý, độ nhạy cảm và mức độ quan trọng đối với tổ chức.

Hướng dẫn triển khai

Việc phân loại và các biện pháp quản lý bảo vệ liên quan cần xem xét đến nhu cầu nghiệp vụ trong việc chia sẻ hoặc hạn chế thông tin và các ảnh hưởng nghiệp vụ liên quan đến các nhu cầu này.

Các hướng dẫn phân loại cần đưa ra các quy ước cho việc phân loại ban đầu và việc phân loại lại theo thời gian phù hợp với chính sách quản lý truy cập đã định trước nào đó (xem 10.1.1).

Cần xác định trách nhiệm của người sở hữu tài sản (xem 6.1.2) trong việc xác định phân loại tài sản, định kỳ soát xét lại phân loại, và đảm bảo rằng phân loại này đã cập nhật và ở mức độ phù hợp. Việc phân loại cần xem xét đến hậu quả kết hợp như đề cập trong 9.7.2.

Cũng cần quan tâm đến số các cấp độ phân loại và lợi ích thu được khi sử dụng chúng. Các cơ chế phân loại quá phức tạp cũng có thể trở thành cồng kềnh và không có hiệu quả về mặt kinh tế hoặc lại không khả thi. Cần cẩn trọng trong việc biên dịch các nhãn phân loại trong các văn bản giữa các tổ chức, các nhãn có tên giống nhau hoặc tương tự nhau có thể có các định nghĩa khác nhau.

Thông tin khác

Mức bảo vệ có thể được quyết định bởi việc phân tích tính bí mật, tính toàn vẹn, tính sẵn sàng và các yêu cầu bất kỳ khác đối với thông tin.

Thông tin thường không còn nhạy cảm hoặc quan trọng nữa sau một khoảng thời gian nhất định, ví dụ, khi thông tin đã được công bố. Các khía cạnh này cũng cần được quan tâm, vì việc phân loại quá phức tạp cũng có thể dẫn đến việc triển khai các biện pháp quản lý không cần thiết và làm phát sinh thêm chi phí.

Việc cân nhắc các văn bản với các yêu cầu an toàn tương tự nhau khi quyết định các mức phân loại cũng có thể giúp làm đơn giản hóa công tác phân loại.

Nhìn chung, việc phân loại thông tin là một con đường nhanh nhất trong việc xác định phương thức xử lý và bảo vệ thông tin.

6.2.2 Gắn nhãn và xử lý thông tin

Biện pháp quản lý

Các thủ tục cần thiết cho việc gán nhãn và quản lý thông tin cần được phát triển và triển khai phù hợp với lược đồ phân loại thông tin đã được tổ chức chấp nhận.

Hướng dẫn triển khai

Các thủ tục dán nhãn thông tin cần được xây dựng cho tất cả các tài sản thông tin ở cả dạng vật lý và điện tử.

Đầu ra của các hệ thống chứa các thông tin đã được phân loại là nhạy cảm hoặc quan trọng cần mang một nhãn phân loại phù hợp (ở đầu ra). Việc dán nhãn cần thể hiện phân loại theo các quy tắc đã thiết lập trong 6.2.1. Các danh mục cần quan tâm bao gồm các báo cáo in sẵn, các màn hình hiển thị, phương tiện lưu giữ (ví dụ băng, đĩa, CD), các thông điệp điện tử, và các phần mềm truyền tệp.

Đối với từng mức phân loại, cũng cần xác định các thủ tục xử lý bao gồm xử lý an toàn, lưu trữ, truyền, phân loại lại, và hủy bỏ. Cũng cần có các thủ tục về thất chặt giám sát và ghi lại bất kỳ sự kiện nào liên quan đến an toàn.

Các thỏa thuận với các tổ chức khác về chia sẻ thông tin cần chứa các thủ tục xác định phân loại của thông tin đó và biên dịch các nhãn phân loại giữa các tổ chức.

Thông tin khác

Việc dán nhãn và xử lý thông tin đã phân loại một cách an toàn là một yêu cầu then chốt đối với các chia sẻ thông tin. Các nhãn vật lý là một dạng nhãn thông thường. Tuy nhiên, một số tài sản thông tin, như các tài liệu ở dạng điện tử, thì không thể dán nhãn dưới dạng vật lý và khi đó cần thực hiện dán nhãn điện tử. Ví dụ, nhãn thông tin có thể xuất hiện trên màn hình hoặc được hiển thị bằng máy tính. Nếu việc dán nhãn không khả thi thì các phương tiện phân loại thông tin khác có thể được áp dụng, ví dụ thông qua các thủ tục hoặc các mô tả về dữ liệu.

7 Đảm bảo an toàn thông tin từ nguồn nhân lực

7.1 Trước khi tuyển dụng

Mục tiêu: Đảm bảo rằng các nhân viên, người của nhà thầu và bên thứ ba hiểu rõ trách nhiệm của mình và phù hợp với vai trò được giao, đồng thời giảm thiểu các rủi ro do đánh cắp, gian lận và lạm dụng chức năng, quyền hạn.

Các trách nhiệm về an toàn cần được nhấn mạnh trước khi sử dụng lao động theo những đặc điểm công việc tương xứng, và theo các điều khoản và điều kiện về sử dụng lao động.

Tất cả những ứng viên, người của các nhà thầu và bên thứ ba đều cần được kiểm tra đầy đủ, nhất là đối với những công việc có tính chất nhạy cảm.

Các nhân viên, người của các nhà thầu và bên thứ ba của các phương tiện xử lý thông tin cần ký vào một bản thỏa thuận về vai trò và trách nhiệm đảm bảo an toàn thông tin của họ.

7.1.1 Các vai trò và trách nhiệm

Biện pháp quản lý

Các vai trò và trách nhiệm đảm bảo an toàn thông tin của các nhân viên, người của nhà thầu và bên thứ ba phải được xác định và ghi thành văn bản phù hợp với chính sách an toàn thông tin của tổ chức.

Hướng dẫn triển khai

Các vai trò và trách nhiệm về an toàn cần gồm các yêu cầu về:

a) triển khai và hành động phù hợp với các chính sách an toàn thông tin của tổ chức (xem 4.1);

b) bảo vệ tài sản trước sự truy nhập, đánh cắp, chỉnh sửa, phá hoại hoặc can thiệp bất hợp pháp;

c) thực hiện các hoạt động và xử lý an toàn bảo mật cụ thể;

d) báo cáo các sự kiện an toàn, những sự kiện tiềm ẩn hoặc những rủi ro an toàn khác đến tổ chức.

Các vai trò và trách nhiệm cần được xác định rõ và thông báo một cách rõ ràng đến các ứng viên trong suốt quá trình trước khi sử dụng lao động.

Thông tin khác

Những mô tả về công việc có thể được sử dụng để ghi lại các vai trò và trách nhiệm về an toàn thông tin. Các vai trò và trách nhiệm về an toàn của các cá nhân chưa được cam kết trong quá trình sử dụng nhân lực của tổ chức, ví dụ đã được cam kết qua một tổ chức thứ ba, cũng cần được xác định rõ và thông báo đến toàn bộ nhân viên.

7.1.2 Thẩm tra

Biện pháp quản lý

Việc xác minh lai lịch của mọi ứng viên tuyển dụng, người của nhà thầu và bên thứ ba phải được thực hiện phù hợp với pháp luật, quy định, đạo đức và phù hợp với các yêu cầu của công việc, phân loại thông tin được truy nhập và các rủi ro có thể nhận thấy được.

Hướng dẫn triển khai

Các cuộc xác minh lai lịch cần quan tâm đến tính riêng tư, việc bảo vệ dữ liệu cá nhân và/hoặc luật sử dụng lao động, và nếu được phép cần bao gồm những vấn đề sau:

a) sự sẵn sàng của các giấy tờ chứng minh danh tính, ví dụ công việc và cá nhân;

b) kiểm tra (tính đầy đủ và chính xác) hồ sơ của ứng viên;

c) xác nhận về các văn bằng nghề nghiệp và học thuật đã khai ;

d) kiểm tra giấy tờ tùy thân (hộ chiếu hoặc giấy tờ tương tự);

e) các kiểm tra chi tiết hơn, ví dụ các kiểm tra về tài chính hoặc các kiểm tra về hồ sơ tội phạm;

Với các công việc, cho dù là được chỉ định từ đầu hoặc do thăng tiến, có sự truy cập của cá nhân tới các phương tiện xử lý thông tin, đặc biệt là nếu các thiết bị này đang xử lý thông tin nhạy cảm, ví dụ thông tin tài chính hoặc thông tin có độ bảo mật cao, thì tổ chức cũng cần xem xét thực hiện các cuộc kiểm tra chi tiết hơn.

Các thủ tục cần xác định tiêu chí và các giới hạn đối với các cuộc xác minh lai lịch, ví dụ người có đủ tư cách thẩm tra, cách thức, thời gian và lý do thực hiện các cuộc thẩm tra.

Quá trình thẩm tra cũng cần được thực hiện với các nhà thầu, và những người dùng thuộc bên thứ ba. Nếu các nhà thầu này được cung cấp qua một công ty môi giới thì hợp đồng với công ty này cần xác định rõ trách nhiệm của công ty trong việc thẩm tra và các thủ tục khai báo mà họ cần tuân thủ nếu việc thẩm tra không hoàn tất hoặc nếu các kết quả thẩm tra gây ra hồ nghi hoặc lo ngại. Tương tự như vậy, thỏa thuận với bên thứ ba (xem thêm 5.2.3) cũng cần xác định rõ tất cả các trách nhiệm và các thủ tục thông báo về việc thẩm tra.

Thông tin của tất cả các ứng viên đang được cân nhắc cho các vị trí tuyển dụng trong tổ chức cũng cần được thu thập và xử lý theo pháp luật hiện hành với phạm vi quyền hạn tương xứng. Tuy theo quy định của luật pháp phù hợp mà các ứng viên cần phải được thông báo trước về các hoạt động thẩm tra này.

7.1.3 Điều khoản và điều kiện tuyển dụng

Biện pháp quản lý

Như một phần của các ràng buộc trong hợp đồng, các nhân viên, người của nhà thầu và bên thứ ba phải đồng ý và ký vào các điều khoản và điều kiện của hợp đồng tuyển dụng. Việc này làm rõ trách nhiệm của người được tuyển dụng và tổ chức đối với an toàn thông tin.

Hướng dẫn triển khai

Các điều khoản và điều kiện tuyển dụng cần thể hiện cả chính sách an toàn của tổ chức bên cạnh việc công bố rằng :

a) tất cả các nhân viên, người của nhà thầu và bên thứ ba- những người được phép truy cập đến thông tin nhạy cảm, cần ký vào một thỏa thuận bảo mật hoặc không tiết lộ trước khi được cấp phép truy cập đến các phương tiện xử lý thông tin;

b) các quyền và trách nhiệm pháp lý của các nhân viên, người của các nhà thầu và những người dùng khác, ví dụ các quyền và trách nhiệm liên quan đến luật bản quyền hoặc pháp chế về bảo vệ dữ liệu (xem thêm 14.1.1 và 13.1.2);

c) các trách nhiệm đối với việc phân loại thông tin và quản lý tài sản thuộc tổ chức liên quan đến các dịch vụ và hệ thống thông tin được xử lý bởi các những nhân viên, người của nhà thầu hoặc bên thứ ba (xem thêm 6.2.1 và 9.7.3);

d) các trách nhiệm của người nhân viên, người của nhà thầu hoặc bên thứ ba trong việc xử lý thông tin nhận được từ các công ty khác hoặc các tổ chức bên ngoài;

e) các trách nhiệm của tổ chức trong việc xử lý thông tin cá nhân, bao gồm thông tin cá nhân có được sau hoặc trong quá trình sử dụng lao động của tổ chức (xem thêm 14.1.4);

f) các trách nhiệm sử dụng tài sản bên ngoài trụ sở của tổ chức và bên ngoài thời gian làm việc bình thường, ví dụ trong trường hợp làm việc tại nhà (xem thêm 8.2.5 và 10.7.1);

g) các hoạt động sẽ được thực thi nếu nhân viên, người của nhà thầu hoặc bên thứ ba thiếu quan tâm đến các yêu cầu về an toàn của tổ chức (xem thêm 7.3).

Tổ chức cần đảm bảo rằng các nhân viên, người của nhà thầu và bên thứ ba đồng ý các điều khoản và điều kiện liên quan đến an toàn thông tin phù hợp với bản chất và phạm vi truy cập mà họ sẽ thực hiện với các tài sản của tổ chức liên quan đến các dịch vụ và hệ thống thông tin.

Nếu thích hợp thì các trách nhiệm nằm trong các điều khoản và điều kiện sử dụng lao động cần được tiếp tục duy trì trong thời gian xác định sau khi đã chấm dứt sử dụng lao động (xem thêm 7.3).

Thông tin khác

Có thể sử dụng một bản hướng dẫn trong đó đưa ra các trách nhiệm của các nhân viên, người của nhà thầu và bên thứ ba liên quan đến tính bảo mật, bảo vệ dữ liệu, nội quy, việc sử dụng phù hợp thiết bị và tài sản của tổ chức, cũng như cách thực hiện dự kiến. Nhà thầu hoặc những người dùng thuộc bên thứ ba có thể liên kết với một tổ chức bên ngoài, tổ chức này có thể được yêu cầu tham gia vào các thương thảo hợp đồng với sự đại diện của một cá nhân ký kết.

7.2 Trong thời gian làm việc

Mục tiêu: đảm bảo rằng mọi nhân viên của tổ chức, người của nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan đến an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ, và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc, và giảm thiểu các rủi ro do con người gây ra.
Cần được xác định các trách nhiệm của ban quản lý nhằm đảm bảo đạt được sự an toàn thông tin trong quá trình sử dụng lao động.
Cần trang bị cho toàn thể nhân viên, người của nhà thầu và bên thứ ba một mức độ hiểu biết, giáo dục, và đào tạo phù hợp về các thủ tục an toàn và việc sử dụng đúng các phương tiện xử lý thông tin nhằm giảm thiểu các rủi ro có thể về an toàn thông tin. Cần xây dựng một qui trình kỷ luật chính thức trong việc xử lý các vi phạm an toàn thông tin.

7.2.1 Trách nhiệm của ban quản lý

Biện pháp quản lý

Ban quản lý cần yêu cầu các nhân viên, người của nhà thầu và bên thứ ba chấp hành an toàn thông tin phù hợp với các chính sách và các thủ tục an toàn thông tin đã được thiết lập của tổ chức.

Hướng dẫn triển khai

Ban quản lý cần có trách nhiệm đảm bảo rằng các nhân viên, người của nhà thầu và bên thứ ba:

a) được chỉ dẫn tường tận về các trách nhiệm và vai trò của họ đối với an toàn thông tin trước khi được chấp nhận truy cập thông tin hoặc các hệ thống thông tin nhạy cảm;

b) được cung cấp các hướng dẫn phù hợp vai trò về an toàn thông tin của họ trong tổ chức;

c) được đốc thúc thực hiện các chính sách an toàn của tổ chức;

d) đạt được một mức độ hiểu biết về an toàn thông tin tương xứng với các vai trò và trách nhiệm của họ trong tổ chức (xem thêm 7.2.2);

e) tuân theo các điều khoản và điều kiện tuyển dụng, bao gồm chính sách an toàn thông tin của tổ chức và các phương pháp làm việc phù hợp;

f) tiếp tục đạt được các kỹ năng và chứng chỉ phù hợp.

Thông tin khác

Nếu các nhân viên, người của nhà thầu và bên thứ ba không nhận thức được các trách nhiệm an toàn thông tin của họ thì họ có thể gây ra những thiệt hại đáng kể cho tổ chức. Các cá nhân được đốc thúc sẽ có xu hướng đáng tin cậy hơn và ít gây ra những sự cố về an toàn thông tin hơn.

Quản lý kém cũng có thể làm cho nhân viên coi thường và dẫn đến kết quả là làm ảnh hưởng xấu đến công tác an toàn thông tin của tổ chức. Ví dụ, việc quản lý kém có thể dẫn đến công tác an toàn thông tin bị xao nhãng hoặc tiềm ẩn sự sử dụng sai các tài sản của tổ chức.

7.2.2 Nhận thức, giáo dục và đào tạo về an toàn thông tin

Biện pháp quản lý

Tất cả các nhân viên trong tổ chức và, nếu liên quan, cả người của nhà thầu và bên thứ ba cần phải được đào tạo nhận thức và cập nhật thường xuyên những chính sách, thủ tục an toàn thông tin của tổ chức như một phần công việc bắt buộc.

Hướng dẫn triển khai

Việc đào đạo kiến thức cần mở đầu bằng việc giới thiệu chính thức về các chính sách an toàn và những mong muốn của tổ chức trước khi truy cập đến thông tin hoặc dịch vụ đã được cấp phép truy cập.

Các nội dung đào tạo tiếp theo cần bao gồm các yêu cầu về an toàn, các trách nhiệm pháp lý và các biện pháp quản lý nghiệp vụ, cũng như đào tạo sử dụng các phương tiện xử lý thông tin một cách đúng đắn, ví dụ thủ tục đăng nhập, sử dụng các gói phần mềm và thông tin về xử lý kỷ luật (xem 7.2.3).

Thông tin khác

Các hoạt động đào tạo, giáo dục và nhận thức về an toàn cần phù hợp và liên quan đến vai trò, các trách nhiệm và kỹ năng của cá nhân, và cần chứa các thông tin về các mối đe dọa đã biết trước, người cần liên hệ khi cần sự hỗ trợ về an toàn thông tin và các kênh thích hợp cho việc báo cáo về các sự cố an toàn thông tin (xem thêm 12.1).

Cần lập kế hoạch đào tạo nâng cao kiến thức cho nhân viên để họ có thể nhận ra được các vấn đề và sự cố an toàn thông tin, và đáp ứng được với những yêu cầu về vai trò công việc của họ.

7.2.3 Xử lý kỷ luật

Biện pháp quản lý

Phải có hình thức xử lý kỷ luật chính thức đối với các nhân viên vi phạm an toàn thông tin.

Hướng dẫn triển khai

Không được bắt đầu quy trình kỷ luật mà không xác minh trước về sự vi phạm an toàn đã xảy ra (xem thêm 12.2.3 phần thu thập chứng cứ).

Quy trình kỷ luật chính thức cần đảm bảo xử lý công bằng và đúng đắn đối với các nhân viên bị nghi ngờ có hành vi vi phạm an toàn. Quy trình kỷ luật chính thức cần đưa ra đáp ứng từng bước trong đó quan tâm đến các yếu tố như bản chất và tính nghiêm trọng của vi phạm và ảnh hưởng nghiệp vụ của nó, xem xét xem đây là vi phạm lần đầu hay lặp lại, xem xét xem người vi phạm đã được đào tạo phù hợp chưa, các vấn đề pháp lý liên quan, các hợp đồng nghiệp vụ và các yếu tố khác nếu cần. Trong những trường hợp vi phạm nghiêm trọng thì quy trình kỷ luật cần cho phép tước bỏ ngay các nhiệm vụ, quyền truy cập và các đặc quyền, và nếu cần thì phải bị hộ tống đuổi ra khỏi nơi làm việc ngay.

Thông tin khác

Quy trình kỷ luật cũng cần được sử dụng như một biện pháp ngăn chặn các nhân viên, người của các nhà thầu và bên thứ ba vi phạm các thủ tục và chính sách an toàn của tổ chức, và những vi phạm khác về an toàn của họ.

7.3 Chấm dứt hoặc thay đổi công việc

Mục tiêu: Nhằm đảm bảo rằng các nhân viên của tổ chức, người của nhà thầu và bên thứ ba nghỉ việc hoặc thay đổi vị trí một cách có tổ chức.

Các trách nhiệm cần được thực hiện nhằm đảm bảo rằng việc nghỉ việc của các nhân viên, người của nhà thầu và thuộc bên thứ ba đều được quản lý, và việc bàn giao tất cả các thiết bị và hủy bỏ các quyền truy cập đã được hoàn tất.

Việc thay đổi các trách nhiệm và nhân viên trong tổ chức cần được quản lý khi chấm dứt trách nhiệm hoặc việc sử dụng lao động tương ứng, và việc sử dụng lao động mới cũng cần được quản lý như mô tả trong 7.1.

7.3.1 Trách nhiệm khi kết thúc hợp đồng

Biện pháp quản lý

Các trách nhiệm trong việc kết thúc hoặc thay đổi nhân sự cần được xác định và phân định rõ ràng.

Hướng dẫn triển khai

Các trách nhiệm về chấm dứt sử dụng lao động cần bao gồm các yêu cầu tiếp theo về an toàn, các trách nhiệm pháp lý và, nếu thích hợp, cả các trách nhiệm đã được ghi trong thỏa thuận bảo mật bất kỳ (xem 5.1.5), và các điều khoản và điều kiện về tuyển dụng (xem 7.1.3) được duy trì trong một thời gian xác định sau khi chấm dứt sử dụng lao động của nhân viên, người của nhà thầu và bên thứ ba.

Các trách nhiệm và nhiệm vụ vẫn được duy trì sau khi chấm dứt sử dụng lao động cần được ghi vào các bản hợp đồng của các nhân viên, người của nhà thầu và bên thứ ba.

Những thay đổi về trách nhiệm hoặc việc sử dụng lao động cần được quản lý khi chấm dứt trách nhiệm hoặc việc sử dụng lao động tương ứng, và trách nhiệm hoặc việc sử dụng lao động mới cũng cần được quản lý như mô tả trong 7.1.

Thông tin khác

Phòng Tổ chức nhân sự phải chịu trách nhiệm chung đối với các công việc và toàn bộ quy trình chấm dứt cùng với người quản lý của người chấm dứt lao động nhằm quản lý được các vấn đề về an toàn của các thủ tục liên quan. Trong trường hợp với nhà thầu thì quy trình chấm dứt có thể được thực thi bởi đại diện có trách nhiệm của nhà thầu, trong các trường hợp với người dùng khác thì có thể được xử lý bởi tổ chức của họ.

Cũng cần thông báo cho các nhân viên, người của nhà thầu và bên thứ ba về những thay đổi và việc sắp xếp công việc mới.

7.3.2 Bàn giao tài sản

Biện pháp quản lý

Tất cả các nhân viên, người của nhà thầu và bên thứ ba cần hoàn trả tất cả các tài sản của tổ chức mà họ quản lý ngay khi kết thúc hợp đồng, thoả thuận hoặc thuyên chuyển công tác.

Hướng dẫn triển khai

Quy trình chấm dứt cần được chính thức hóa bao gồm cả việc hoàn trả tất các phần mềm, các văn bản và thiết bị mà trước kia tổ chức đã giao cho. Các tài sản khác thuộc tổ chức như các thiết bị tính toán di động, các thẻ tín dụng, các thẻ truy cập, phần mềm, các sách hướng dẫn, và cả thông tin được lưu trên các phương tiện điện tử cũng cần được trả lại.

Trong các trường hợp mà một nhân viên, người của nhà thầu hoặc bên thứ ba mua thiết bị của tổ chức hoặc sử dụng thiết bị cá nhân thuộc sở hữu của họ thì cần thực hiện các thủ tục nhằm đảm bảo rằng

tất cả các thông tin liên quan đều đã được chuyển lại cho tổ chức và đã được xóa khỏi thiết bị này (xem thêm 9.7.1).

Trong các trường hợp mà một nhân viên, người của nhà thầu hoặc bên thứ ba nắm giữ các kiến thức quan trọng cho các hoạt động tiếp theo thì thông tin đó cần được lập thành văn bản và chuyển cho tổ chức.

7.3.3 Hủy bỏ quyền truy cập

Biện pháp quản lý

Các quyền truy cập thông tin và các phương tiện xử lý thông tin của mọi nhân viên, người của nhà thầu hoặc bên thứ ba phải được hủy bỏ khi họ kết thúc hợp đồng, thỏa thuận, hoặc thuyên chuyển công tác.

Hướng dẫn triển khai

Khi kết thúc hợp đồng, cần xem xét lại các quyền truy cập của người đó tới các tài sản liên quan đến các dịch vụ và hệ thống thông tin. Khi đó sẽ xác định xem liệu có cần thiết phải hủy bỏ các quyền truy cập không. Khi thay đổi lao động, cần hủy bỏ tất cả các quyền truy cập chưa được chấp thuận đối với nhân viên mới. Các quyền truy cập cần bị hủy bỏ hoặc điều chỉnh bao gồm truy cập vật lý và logic, chìa khóa, thẻ nhận dạng, các phương tiện xử lý thông tin (xem thêm 10.2.4), các bản đăng ký, và loại bỏ khỏi tất cả các văn bản xác định họ là một thành viên hiện tại của tổ chức. Nếu một nhân viên, người của nhà thầu hoặc bên thứ ba rời khỏi tổ chức mà vẫn biết các mật khẩu của các tài khoản đang hoạt động thì cần thay đổi các mật khẩu ngay khi chấm dứt hoặc thay đổi lao động, hợp đồng hoặc thỏa thuận.

Cần giảm bớt hoặc hủy bỏ quyền truy cập tới các tài sản thông tin và các phương tiện xử lý thông tin trước khi chấm dứt sử dụng hoặc thay đổi lao động, tùy theo việc đánh giá các yếu tố rủi ro như:

a) việc kết thúc hợp đồng hoặc thay đổi đó là xuất phát từ nhân viên, người của nhà thầu hoặc bên thứ ba hay từ ban quản lý và lý do kết thúc;

b) các trách nhiệm hiện tại của nhân viên, người của nhà thầu hoặc những người dùng khác;

c) giá trị của các tài sản hiện tại có thể được truy cập.

Thông tin khác

Trong điều kiện hiện nay, các quyền truy cập có thể được phân bổ trên cơ sở phải sẵn sàng đối với nhiều người chứ không phải chỉ đối với nhân viên, người của nhà thầu hoặc bên thứ ba dời khỏi tổ chức, ví dụ dưới dạng các ID của nhóm. Trong các trường hợp này, các cá nhân dời khỏi tổ chức cần bị loại khỏi các danh sách truy cập nhóm và cần thực hiện các công việc chuẩn bị để báo cho tất cả các nhân viên, người của nhà thầu hoặc bên thứ ba khác có liên quan không tiếp tục chia sẻ thông tin này với người dời khỏi tổ chức nữa.

Trong các trường hợp mà việc kết thúc hợp đồng xuất phát từ ban quản lý thì các nhân viên, người của nhà thầu hoặc bên thứ ba có thể bất bình và có thể sửa đổi thông tin một cách có chủ ý hoặc phá

hoại các phương tiện xử lý thông tin. Trong các trường hợp với những người được ký lại hợp đồng, họ có thể có gắng thu thập thông tin để sử dụng trong tương lai.

8 Đảm bảo an toàn vật lý và môi trường

8.1 Các khu vực an toàn

Mục tiêu: Nhằm ngăn chặn sự truy cập vật lý, làm hư hại và cản trở thông tin và tài sản của tổ chức.

Các phương tiện xử lý thông tin nhạy cảm hoặc quan trọng cần được đặt trong phòng nằm trong các khu vực an toàn, được bảo vệ bởi các vành đai an ninh, bằng các rào chắn an toàn và các biện pháp quản lý ra vào phù hợp. Chúng cần được bảo vệ về mặt vật lý trước sự truy cập, hủy hoại và can thiệp trái phép.

Hình thức bảo vệ cần tương xứng với các rủi ro đã được xác định.

8.1.1 Vành đai an toàn vật lý

Biện pháp quản lý

Các vành đai an toàn (các rào chắn như tường, cổng ra/vào có kiểm soát bằng thẻ hoặc bàn đón tiếp) phải được sử dụng để bảo vệ các khu vực chứa thông tin và phương tiện xử lý thông tin.

Hướng dẫn triển khai

Cần quan tâm và triển khai các hướng dẫn sau đối với vành đai an toàn vật lý:

a) các vành đai an toàn cần được xác định rõ ràng, vị trí và chiều dài của mỗi vành đai cần tùy thuộc vào các yêu cầu an toàn của các tài sản nằm ở khu vực bên trong vành đai và các kết quả có được từ đánh giá rủi ro;

b) các vành đai an toàn của các tòa nhà hoặc các khu vực chứa các phương tiện xử lý thông tin cần vững chắc (tức là không được có lỗ hổng ở vành đai và các khu vực dễ xảy ra đột nhập); các bức tường bảo vệ bên ngoài địa điểm đó cần có cấu trúc vững chãi và tất cả các cửa ra vào bên ngoài cần được bảo vệ bằng các cơ chế điều khiển, ví dụ thanh chắn, chuông báo, khóa...; cửa ra vào và cửa sổ cần được khóa khi không có người bên trong và cần quan tâm bảo vệ bên ngoài các cửa sổ, đặc biệt tại tầng hầm;

c) có thể thiết lập khu vực có người đón tiếp hoặc các hình thức quản lý truy cập vật lý tới tòa nhà hoặc địa điểm; cần giới hạn chỉ cho những người được cấp phép đi vào các địa điểm hoặc tòa nhà;

d) nếu phù hợp thì cần sử dụng các rào chắn vật lý nhằm ngăn chặn xâm nhập trái phép và làm ô nhiễm môi trường;

e) tất cả các cửa chống cháy trên vành đai an toàn cần được đặt còi báo động, được giám sát và kiểm tra kết hợp với các bức tường bao quanh nhằm đạt được mức đảm bảo yêu cầu theo các tiêu chuẩn khu vực, quốc gia và quốc tế phù hợp; chúng cũng cần hoạt động tuân theo quy tắc báo cháy nội bộ theo phương thức dự phòng để đảm bảo an toàn;

f) các hệ thống phát hiện xâm nhập cần được cài đặt theo các tiêu chuẩn quốc gia, khu vực hoặc quốc tế và thường xuyên được kiểm tra để bao quát tất cả các cửa bên ngoài và các cửa sổ dễ xâm nhập; các khu vực bỏ trống cũng cần được đặt báo động tại mọi thời điểm; cần bao quát kiểm tra tất cả các khu vực khác, ví dụ phòng máy tính hoặc các phòng truyền thông;

g) các phương tiện xử lý thông tin do tổ chức quản lý cần được đặt cách biệt khỏi các thiết bị được quản lý bởi bên thứ ba.

Thông tin khác

Có thể đạt được sự bảo vệ vật lý nếu thiết lập một hoặc nhiều rào chắn xung quanh trụ sở và các phương tiện xử lý thông tin của tổ chức. Việc sử dụng nhiều rào chắn sẽ làm tăng khả năng bảo vệ, vì như vậy, khi có sự cố ở một rào chắn sẽ chưa chắc sẽ lập tức ảnh hưởng đến an toàn tài sản.

Một khu vực an toàn có thể là một văn phòng có khóa hoặc nhiều phòng được bao quanh bởi một rào chắn an toàn vật lý liền. Có thể dùng thêm nhiều rào chắn và vành đai an toàn giữa các khu vực có các yêu cầu an toàn khác nhau nằm bên trong hàng rào an ninh để quản lý xâm nhập.

Cần quan tâm đặc biệt đến sự an toàn xâm nhập với các tòa nhà có nhiều tổ chức làm việc.

8.1.2 Kiểm soát cổng truy cập vật lý

Biện pháp quản lý

Các khu vực cần được bảo vệ bằng các biện pháp kiểm soát truy cập thích hợp nhằm đảm bảo chỉ những người có quyền mới được phép truy cập.

Hướng dẫn triển khai

Cần quan tâm đến các hướng dẫn sau:

a) ngày tháng và thời gian vào ra của khách cần được ghi lại, và cần giám sát tất cả khách ra vào trừ khi trước đây họ đã được phép ra/vào; họ cần được chỉ dẫn các yêu cầu an ninh ở khu vực và các thủ tục khẩn cấp;

b) truy cập đến các khu vực xử lý và lưu trữ thông tin nhạy cảm phải được quản lý và chỉ giới hạn ở những người được phép; các biện pháp xác thực, như thẻ kiểm soát truy cập và PIN, cần được sử dụng nhằm xác thực và kiểm tra tất cả các truy cập; truy vết của tất cả các truy cập cần được duy trì một cách an toàn;

c) tất cả các nhân viên, người của nhà thầu hoặc bên thứ ba và khách đến cần được yêu cầu mang một thẻ dạng nhận dạng dễ nhìn thấy nào đó và phải lập tức thông báo cho nhân viên an ninh nếu họ trông thấy những khách đi một mình và những người không mang thẻ nhận dạng;

d) tổ chức thứ ba cung cấp nhân viên phục vụ cũng cần đảm bảo bị hạn chế truy cập đến các khu vực hoặc các phương tiện xử lý thông tin nhạy cảm khi có yêu cầu; truy cập này cần được cấp phép và giám sát;

c) các quyền truy cập nhằm đảm bảo an toàn cho các khu vực cần được soát xét, cập nhật thường xuyên, và bị thu hồi khi cần thiết (xem 7.3.3).

8.1.3 Bảo vệ các văn phòng, phòng làm việc và vật dụng

Biện pháp quản lý

Biện pháp bảo vệ an toàn vật lý cho các văn phòng, phòng làm việc và vật dụng cần được thiết kế và áp dụng

Hướng dẫn triển khai

Nhằm đảm bảo an toàn cho các văn phòng, phòng làm việc và vật dụng, cần quan tâm đến các hướng dẫn sau :

a) cần quan tâm đến các quy định và tiêu chuẩn về an toàn và sức khỏe có liên quan;

b) các thiết bị quan trọng cần được đặt tại những vị trí tránh được sự truy cập công cộng;

c) nếu khả thi thì các tòa nhà cần được bài trí kín đáo và chỉ bộc lộ tối thiểu mục đích của chúng, cả phía ngoài và phía trong tòa nhà đều không có các dấu hiệu rõ ràng về sự hiện diện của các hoạt động xử lý thông tin;

d) các tài liệu hướng dẫn và các quyển danh bạ điện thoại nội bộ thể hiện vị trí của các phương tiện xử lý thông tin không được để ở các vị trí mà nhiều người dễ dàng lấy được.

8.1.4 Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường

Biện pháp quản lý

Biện pháp bảo vệ vật lý chống lại những nguy cơ do cháy nổ, ngập lụt, động đất, tình trạng náo loạn và các thảm họa khác do thiên nhiên và con người gây ra cần được thiết kế và áp dụng.

Hướng dẫn triển khai

Cần quan tâm đến những mối đe dọa do môi trường xung quanh, ví dụ như đám cháy ở một tòa nhà bên cạnh, nước rò rỉ từ mái hoặc từ sàn nhà xuống tầng hầm hoặc một vụ nổ trên đường phố.

Cần quan tâm đến những hướng dẫn sau nhằm phòng tránh thiệt hại do cháy, nổ, lũ lụt, động đất, náo loạn và các thảm họa do con người và thiên nhiên khác:

a) các vật liệu nguy hiểm hoặc dễ cháy cần được cất giữ ở khoảng cách an toàn với khu vực an toàn;

b) thiết bị dự trữ và phương tiện dự phòng cần được đặt ở khoảng cách an toàn nhằm tránh thiệt hại từ thảm họa ở địa điểm chính;

c) cần trang bị thiết bị dập lửa phù hợp và đặt chúng ở các vị trí thích hợp.

8.1.5 Làm việc trong các khu vực an toàn

Biện pháp quản lý

Biện pháp bảo vệ vật lý và các hướng dẫn làm việc trong các khu vực an toàn cần được thiết kế và áp dụng.

Hướng dẫn triển khai

Cần quan tâm đến những hướng dẫn sau:

a) nhân viên làm việc chỉ được biết đến các khu vực an toàn và các hoạt động ở trong khu vực này ở mức độ cần phải biết;

b) vì các lý do an toàn và nhằm phòng tránh cơ hội cho các hoạt động cố tình gây hại thì cần tránh làm việc mà không có giám sát trong các khu vực an toàn;

c) các khu vực an toàn còn bỏ trống cần được khóa cẩn thận và định kỳ kiểm tra;

d) chụp ảnh, ghi hình, ghi âm hoặc các thiết bị ghi khác, như máy quay phim trong các thiết bị di động đều bị cấm, trừ khi được phép sử dụng.

Các biện pháp quản lý làm việc trong các khu vực an toàn phải bao gồm các biện pháp đối với nhân viên, người của nhà thầu hoặc bên thứ ba làm việc trong các khu vực an toàn, cũng như các hoạt động khác của tổ chức thứ ba thực hiện trong khu vực đó.

8.1.6 Các khu vực truy cập tự do, phân phối và tập kết hàng

Biện pháp

Các điểm truy cập mà người truy cập không cần cấp phép như khu vực chung, phân phối và tập kết hàng... phải được quản lý và, nếu có thể, được cách ly khỏi các phương tiện xử lý thông tin để tránh tình trạng truy cập trái phép.

Hướng dẫn triển khai

Cần quan tâm đến những hướng dẫn sau :

a) cần giới hạn chỉ cho những người đã xác định và đã được cho phép truy cập từ bên ngoài tòa nhà đến các khu vực phân phối và tập kết hàng;

b) khu vực phân phối và tập kết hàng cần được thiết kế sao cho các nguồn hàng có thể được dỡ xuống mà nhân viên phân phối không phải tiếp cận đến các khu vực khác của tòa nhà;

c) cần đảm bảo an toàn cho các cửa ra vào bên ngoài của khu vực phân phối và tập kết hàng khi các cửa bên trong đang mở;

d) vật liệu mang vào cần được kiểm tra các mối đe dọa tiềm ẩn (xem 8.2.1d) trước khi vật liệu này được chuyển từ khu vực phân phối và tập kết hàng đến điểm sử dụng;

e) vật liệu mang vào cần được đăng ký theo các thủ tục quản lý tài sản (xem 6.1.1) ở lối vào khu vực đó;

f) nếu có thể thì hàng vào và hàng ra cần được đặt cách xa nhau.

8.2 Đảm bảo an toàn trang thiết bị

Mục tiêu: Nhằm ngăn ngừa mất mát, hư hại, đánh cắp hoặc lợi dụng tài sản và làm gián đoạn các hoạt động của tổ chức.

Trang thiết bị cần được bảo vệ trước các mối đe dọa vật lý và môi trường.

Bảo vệ trang thiết bị (bao gồm cả các thiết bị được sử dụng bên ngoài trụ sở tổ chức, và việc di dời tài sản) là cần thiết nhằm giảm bớt các rủi ro do truy cập thông tin trái phép và bảo vệ trước những mất mát hoặc hư hại. Cũng cần lưu ý đến việc chọn vị trí đặt và loại bỏ thiết bị. Các biện pháp quản lý đặc biệt có thể được yêu cầu nhằm bảo vệ thiết bị trước những mối đe dọa vật lý, và bảo vệ các thiết bị hỗ trợ, như thiết bị cấp nguồn điện và hệ thống dây cáp.

8.2.1 Bố trí và bảo vệ thiết bị

Biện pháp quản lý

Thiết bị phải được bố trí tại các địa điểm an toàn hoặc được bảo vệ nhằm giảm thiểu các rủi ro do các mối đe dọa, hiểm họa từ môi trường hay các truy cập trái phép.

Hướng dẫn triển khai

Để bảo vệ thiết bị, cần quan tâm tới những hướng dẫn sau đây :

a) cần lựa chọn vị trí đặt thiết bị nhằm giảm thiểu truy cập không cần thiết vào các khu vực làm việc;

b) các phương tiện xử lý thông tin thực hiện công việc xử lý dữ liệu nhạy cảm cũng cần được bố trí vị trí đặt và được đặt ở góc quan sát hạn chế nhằm giảm rủi ro thông tin bị quan sát bởi các cá nhân không được phép, và các thiết bị lưu trữ được an toàn nhằm tránh truy cập trái phép;

c) các thiết bị yêu cầu bảo vệ đặc biệt cần được đặt riêng nhằm giảm mức độ yêu cầu bảo vệ chung;

d) cần thực hiện các biện pháp quản lý nhằm giảm thiểu rủi ro do các mối đe dọa vật lý tiềm ẩn, ví dụ đánh cắp, cháy, nổ, khói, nước (hoặc sự cố ở nguồn cung cấp nước), bụi, chấn động, các ảnh hưởng của hóa chất, nhiễu nguồn điện, nhiễu viễn thông, phát xạ điện từ, và các hành động phá hoại;

e) cần đưa ra các hướng dẫn đối với việc ăn, uống, và hút thuốc ở khu vực lân cận các phương tiện xử lý thông tin;

f) các điều kiện môi trường, như nhiệt độ và độ ẩm, cũng cần được giám sát, vì chúng có thể ảnh hưởng bất lợi đến các phương tiện xử lý thông tin;

g) cần sử dụng các biện pháp chống sét cho tất cả các toà nhà và các bộ lọc sét cần được lắp đặt cho tất cả các đường dây thông tin và đường dây cấp nguồn;

h) cần quan tâm đến việc sử dụng các biện pháp bảo vệ đặc biệt, ví dụ màng bảo vệ bàn phím, đối với các thiết bị sử dụng trong các môi trường công nghiệp;

i) cần bảo vệ phương tiện xử lý thông tin nhạy cảm nhằm giảm thiểu rủi ro rò rỉ thông tin do sự phát xạ.

8.2.2 Các tiện ích hỗ trợ

Biện pháp quản lý

Thiết bị phải được bảo vệ khỏi sự cố về nguồn điện cũng như các gián đoạn hoạt động có nguyên nhân từ các tiện ích hỗ trợ.

Hướng dẫn triển khai

Tất cả các tiện ích hỗ trợ, như nguồn điện, nguồn nước, rác thải, hệ thống sưởi/thông gió, và điều hòa không khí cần phù hợp với các hệ thống mà chúng hỗ trợ. Các tiện ích hỗ trợ cần được xem xét và kiểm tra thường xuyên nhằm đảm bảo chúng hoạt động tốt và làm giảm rủi ro do lỗi hoặc hoạt động sai chức năng. Cần cung cấp nguồn cấp điện phù hợp theo các chỉ tiêu kỹ thuật của nhà sản xuất thiết bị.

Khuyến nghị sử dụng nguồn cấp điện liên tục (UPS) để cấp điện liên tục cho các thiết bị hỗ trợ các hoạt động nghiệp vụ có tính cấp bách. Các kế hoạch xử lý những sự cố bất ngờ về nguồn điện cũng cần tính đến sự cố về UPS. Cần quan tâm đến việc sử dụng bộ phát điện dự phòng nếu quá trình xử lý đòi hỏi phải liên tục trong trường hợp có sự cố nguồn điện kéo dài. Nguồn cung cấp nhiên liệu phù hợp cũng cần sẵn sàng nhằm đảm bảo rằng bộ phát điện có thể làm việc trong thời gian dài. Thiết bị UPS và các bộ phát điện cần được kiểm tra thường xuyên nhằm đảm bảo rằng chúng có đầy đủ tính năng và được kiểm tra tuân thủ các khuyến nghị của nhà sản xuất. Thêm vào đó, cũng cần quan tâm đến việc sử dụng nhiều nguồn điện hoặc, nếu vị trí đủ lớn, thì cần có nơi đặt nguồn riêng.

Các công tắc điện khẩn cấp cần được đặt ở vị trí gần các lối thoát hiểm trong các phòng thiết bị nhằm hỗ trợ tắt nguồn nhanh chóng trong trường hợp khẩn cấp. Đèn khẩn cấp cần được sử dụng trong trường hợp hỏng nguồn điện chính.

Nguồn cung cấp nước cần ổn định và phù hợp nhằm hỗ trợ các hệ thống thiết bị điều hòa không khí, thiết bị làm ẩm và thiết bị dập lửa (nếu được sử dụng). Các sự cố về nguồn nước có thể làm hư hại thiết bị hoặc khiến cho thiết bị dập lửa làm việc không hiệu quả. Nếu có yêu cầu thì cần tính đến việc sử dụng hệ thống cảnh báo phát hiện các sự cố đối với các tiện ích hỗ trợ.

Thiết bị viễn thông cần được kết nối đến nhà cung cấp tiện ích qua ít nhất hai tuyến khác nhau nhằm tránh việc sự cố trên một luồng kết nối làm đứt các dịch vụ thoại. Các dịch vụ thoại cũng cần phù hợp nhằm đáp ứng được các yêu cầu pháp lý nội bộ đối với truyền thông khẩn cấp.

Thông tin khác

Cần có nhiều nguồn cung cấp điện để đạt được sự liên tục về cấp điện nhằm tránh sự cố về nguồn điện.

8.2.3 An toàn cho dây cáp

Biện pháp quản lý

Dây dẫn nguồn điện và cáp truyền thông mang dữ liệu hoặc các hỗ trợ các dịch vụ thông tin cần được bảo vệ khỏi sự xâm phạm hoặc làm hư hại.

Hướng dẫn triển khai

Cần quan tâm đến các hướng dẫn sau:

a) các đường dây điện và đường cáp viễn thông dẫn tới các phương tiện xử lý thông tin nếu có thể cần được đặt ngầm, hoặc được bảo vệ theo phương thức phù hợp;

b) hệ thống cáp mạng cũng cần được bảo vệ khỏi việc nghe trộm hoặc hư hại, ví dụ sử dụng ống bọc bảo vệ hoặc tránh các tuyến đi qua các khu vực công cộng;

c) cần tách riêng đường cáp điện và đường cáp viễn thông nhằm ngăn chặn nhiễu;

d) cần sử dụng cách đánh dấu dễ nhận biết cho cáp và thiết bị nhằm giảm thiểu các lỗi khi sửa chữa, ví dụ như vô tình đấu sai đường cáp mạng;

e) cần sử dụng tài liệu sơ đồ đấu nối nhằm làm giảm khả năng xảy ra lỗi;

f) đối với các hệ thống nhạy cảm hoặc quan trọng, cần quan tâm đến các biện pháp khác như:

1) lắp đặt ống dẫn bọc sắt và sử dụng các phòng hoặc hộp có khóa tại các điểm kết cuối và điểm có nghi ngờ;

2) sử dụng các tuyến cáp và/hoặc môi trường truyền dẫn khác nhau nhằm đảm bảo độ an toàn;

3) sử dụng cáp quang;

4) sử dụng tấm chắn điện từ để bảo vệ cáp;

5) kiểm tra kỹ thuật và rà soát vật lý đối với các thiết bị trái phép được gắn vào đường cáp;

6) truy cập được quản lý tới các phiến đấu nối và các buồng cáp.

8.2.4 Bảo dưỡng thiết bị

Biện pháp quản lý

Thiết bị cần được bảo dưỡng đúng quy cách nhằm đảm bảo luôn sẵn sàng và toàn vẹn.

Hướng dẫn triển khai

Cần quan tâm tới các hướng dẫn sau trong việc bảo dưỡng thiết bị:

a) thiết bị cần được bảo dưỡng tuân theo các chu kỳ bảo dưỡng và các chỉ tiêu kỹ thuật dịch vụ được nhà cung cấp khuyến nghị;

b) chỉ người bảo dưỡng được cấp phép mới được thực hiện các công việc sửa chữa và bảo dưỡng thiết bị;

c) cần giữ lại các báo cáo về các lỗi thực sự hoặc lỗi khả nghi, và toàn bộ quá trình bảo dưỡng phòng ngừa và bảo dưỡng khắc phục;

d) cần triển khai các biện pháp quản lý phù hợp khi thiết bị được lập lịch cho bảo trì, trong đó cần quan tâm xem nhân viên bảo trì là người thuộc tổ chức hay ngoài tổ chức; khi cần thiết thì thông tin nhạy cảm cần bị xóa khỏi thiết bị, hoặc nhân viên bảo dưỡng cần được giải thích rõ ràng;

e) cần tuân thủ tất cả các yêu cầu của các chính sách bảo hiểm.

8.2.5 An toàn cho thiết bị hoạt động bên ngoài trụ sở của tổ chức

Biện pháp quản lý

Phải đảm bảo an toàn cho các thiết bị sử dụng bên ngoài, chú ý các rủi ro khác khau khi thiết bị làm việc bên ngoài trụ sở của tổ chức.

Hướng dẫn triển khai

Cho dù người sở hữu là ai thì việc sử dụng phương tiện xử lý thông tin bên ngoài trụ sở của tổ chức cũng cần được cấp phép bởi ban quản lý.

Cần quan tâm đến các hướng dẫn sau:

a) thiết bị và phương tiện khi được mang ra ngoài trụ sở thì không được gây chú ý ở nơi công cộng; máy tính xách tay cần được cho vào túi xách và được ngụy trang ở mức có thể khi di chuyển;

b) cần luôn thực thi các hướng dẫn về bảo vệ thiết bị của nhà sản xuất, ví dụ bảo vệ khi ở trong các môi trường điện từ mạnh;

c) các biện pháp quản lý khi làm việc tại nhà cần được xác định qua đánh giá rủi ro và áp dụng các biện pháp quản lý phù hợp, ví dụ các tủ hồ sơ có khóa, chính sách bàn sạch, quản lý truy cập máy tính và truyền thông an toàn với cơ quan (xem thêm tiêu chuẩn ISO/IEC 18028: An toàn mạng);

d) cần sử dụng hình thức bọc bảo vệ phù hợp để bảo vệ thiết bị ở bên ngoài trụ sở.

Các rủi ro về an toàn, ví dụ hư hại, trộm cắp hoặc nghe trộm, có thể khác nhau tùy theo địa điểm và cần được quan tâm xem xét khi xác định các biện pháp quản lý phù hợp nhất.

Thông tin khác

Thiết bị lưu trữ và xử lý thông tin bao gồm tất cả các dạng máy tính cá nhân, các loại điện thoại di động, thẻ thông minh, giấy tờ hoặc các hình thức khác được sử dụng khi làm việc tại nhà hoặc được mang ra ngoài vị trí làm việc thông thường.

8.2.6 An toàn khi loại bỏ hoặc tái sử dụng thiết bị

Biện pháp quản lý

Tất cả các bộ phận của thiết bị có chứa các phương tiện lưu trữ thông tin phải được kiểm tra nhằm đảm bảo rằng tất cả dữ liệu nhạy cảm và phần mềm có bản quyền phải được xóa bỏ hoặc ghi đè trước khi loại bỏ hoặc tái sử dụng thiết bị cho mục đích khác.

Hướng dẫn triển khai

Các thiết bị chứa thông tin nhạy cảm cần bị loại bỏ về mặt vật lý hoặc thông tin trong đó cần bị loại bỏ, bị xóa bỏ hoặc bị ghi đè bằng các kỹ thuật làm cho thông tin ban đầu không thể khôi phục được nữa, chứ không dùng chức năng xóa hoặc định dạng thông thường.

Thông tin khác

Các thiết bị hư hỏng nhưng lại chứa dữ liệu nhạy cảm có thể cần phải được đánh giá rủi ro nhằm xác định xem liệu các thiết bị đó có cần bị loại bỏ về mặt vật lý không hay cần được sửa chữa.

Thông tin có thể bị tổn hại khi loại bỏ hoặc tái sử dụng thiết bị không cẩn thận (xem thêm 9.7.2).

8.2.7 Di dời tài sản

Biện pháp quản lý

Không được mang thiết bị, thông tin hoặc phần mềm ra khỏi trụ sở nếu chưa được phép.

Hướng dẫn triển khai

Cần quan tâm đến những hướng dẫn sau:

a) không được mang thiết bị, thông tin hoặc phần mềm ra khỏi trụ sở khi chưa được phép;

b) cần xác định rõ các nhân viên, người của nhà thầu và bên thứ ba được cho phép mang tài sản ra khỏi trụ sở;

c) cần xác định giới hạn thời gian được mang thiết bị ra ngoài và phải kiểm tra tuân thủ;

d) khi cần thiết và nếu thích hợp thì cần ghi vào sổ sách mỗi khi thiết bị được mang ra ngoài và khi được trả lại.

Thông tin khác

Có thể thực hiện các cuộc kiểm tra đột xuất nhằm phát hiện các thiết bị ghi trái phép, vũ khí... và ngăn chặn việc đưa chúng vào trụ sở làm việc. Các cuộc kiểm tra đột xuất như vậy cần được thực hiện tuân thủ các quy định và luật pháp liên quan. Cần thông báo về các cuộc kiểm tra này và chỉ được thực hiện chúng theo các yêu cầu pháp lý và quy định.

9 Quản lý truyền thông và vận hành

9.1 Các trách nhiệm và thủ tục vận hành

Mục tiêu: Nhằm đảm bảo sự vận hành các phương tiện xử lý thông tin đúng đắn và an toàn.

Cần thiết lập các trách nhiệm và thủ tục quản lý và vận hành cho tất cả các phương tiện xử lý thông tin. Bao gồm cả việc xây dựng các thủ tục vận hành phù hợp.

Nếu phù hợp thì cần triển khai phân định các nhiệm vụ nhằm giảm rủi ro do sử dụng cẩu thả hoặc lạm dụng hệ thống một cách có chủ ý.

9.1.1 Các thủ tục vận hành được ghi thành văn bản

Biện pháp quản lý

Các thủ tục vận hành cần được ghi thành văn bản, duy trì, và luôn sẵn sàng đối với mọi người cần dùng đến.

Hướng dẫn triển khai

Cần chuẩn bị các văn bản thủ tục cho các hoạt động hệ thống có liên quan đến các thiết bị trao đổi và xử lý thông tin, ví dụ các thủ tục khởi động và tắt máy tính, sao lưu, bảo dưỡng thiết bị, điều khiển thiết bị, quản lý phòng máy tính và xử lý thư từ, và vấn đề an toàn.

Các thủ tục vận hành cần đưa ra các hướng dẫn thực hiện chi tiết từng công việc gồm:

a) xử lý và quản lý thông tin

b) sao lưu (xem 9.5.1);

c) các yêu cầu về thời gian biểu, bao hàm cả sự phụ thuộc với các hệ thống khác, các thời điểm bắt đầu công việc sớm nhất và các thời điểm kết thúc công việc muộn nhất;

d) các hướng dẫn xử lý các sự cố hoặc các điều kiện ngoại lệ khác, những vấn đề này có thể xuất hiện trong khi thực hiện công việc, bao gồm cả các giới hạn sử dụng các tiện ích của hệ thống (xem 10.5.4);

e) hỗ trợ liên lạc trong các trường hợp có trở ngại không mong muốn về vận hành hoặc kỹ thuật;

f) các hướng dẫn xử lý thiết bị và dữ liệu đầu ra đặc biệt, như sử dụng đồ dùng văn phòng đặc biệt hoặc quản lý dữ liệu đầu ra bảo mật bao gồm các thủ tục loại bỏ một cách an toàn dữ liệu đầu ra từ các công việc bị lỗi (xem 9.7.2 và 9.7.3);

g) các thủ tục khởi động và khôi phục hệ thống trong trường hợp có lỗi hệ thống;

h) quản lý truy vết và thông tin nhật ký của hệ thống (xem 9.10).

Các thủ tục khai thác và các văn bản thủ tục cho các hoạt động của hệ thống cần được coi như các văn bản chính thức và được cấp phép thay đổi bởi ban quản lý. Nếu điều kiện kỹ thuật cho phép thì các hệ thống thông tin cần được quản lý liên tục bằng các thủ tục, công cụ và các tiện ích nhất quán.

9.1.2 Quản lý thay đổi

Biện pháp quản lý

Các thay đổi trong các phương tiện và hệ thống xử lý thông tin phải được kiểm soát.

Hướng dẫn triển khai

Cần quản lý chặt chẽ các thay đổi đối với phần mềm ứng dụng và các hệ thống vận hành.

Cụ thể là, những vấn đề sau cần được quan tâm:

a) Xác định và ghi lại những thay đổi quan trọng;

b) Lập kế hoạch và kiểm tra những thay đổi;

c) Đánh giá những ảnh hưởng tiềm ẩn, bao gồm những ảnh hưởng về an toàn của những thay đổi đó;

d) Thủ tục chấp nhận chính thức đối với những thay đổi đã được phát hiện;

e) Thông báo chi tiết về các thay đổi cho tất cả những người liên quan;

f) Các thủ tục phục hồi lại hệ thống trước thay đổi, bao gồm các thủ tục và trách nhiệm đối với việc hủy bỏ và khôi phục dữ liệu từ những thay đổi không thành công và các sự kiện bất ngờ xảy ra.

Các thủ tục và trách nhiệm quản lý chính thức cần được đặt ra nhằm đảm bảo quản lý thỏa đáng tất cả những thay đổi đối với thiết bị, phần mềm hoặc các thủ tục. Khi những thay đổi được thực hiện thì cần lưu lại nhật ký đánh giá chứa tất cả các thông tin liên quan.

Thông tin khác

Việc quản lý những thay đổi của các phương tiện xử lý thông tin không thích hợp là nguyên nhân phổ biến dẫn đến các sự cố đối với hệ thống và an toàn thông tin. Những thay đổi về môi trường khai thác, đặc biệt là khi chuyển một hệ thống từ giai đoạn phát triển sang giai đoạn khai thác, có thể ảnh hưởng đến độ tin cậy của các ứng dụng (xem thêm 11.5.1).

Chỉ được thực thi những thay đổi đối với các hệ điều hành khi có lý do nghiệp vụ hợp lệ, chẳng hạn khi có sự gia tăng rủi ro đối với hệ thống. Việc nâng cấp các hệ thống bằng các phiên bản hệ điều hành hoặc ứng dụng mới nhất thường không hay được quan tâm vì có thể gây ra những nguy hiểm và sự mất ổn định hơn so với phiên bản hiện tại. Việc nâng cấp các phiên bản phần mềm có thể cũng làm phát sinh thêm các yêu cầu về đào tạo, các chi phí cho việc đăng ký, chi phí cho hỗ trợ, duy trì và quản lý, và đặc biệt là phần cứng mới trong quá trình chuyển phiên bản.

9.1.3 Phân tách nhiệm vụ

Biện pháp quản lý

Các nhiệm vụ và phạm vi trách nhiệm phải được phân tách nhằm giảm thiểu khả năng sửa đổi trái phép hoặc vô tình, hoặc lạm dụng tài sản của tổ chức.

Hướng dẫn triển khai

Phân tách nhiệm vụ là một phương pháp làm giảm rủi ro do vô tình hoặc cố ý lạm dụng hệ thống. Cần theo dõi chặt chẽ nhằm đảm bảo không một cá nhân nào có thể truy cập, chỉnh sửa hoặc sử dụng tài sản khi chưa được phép hoặc không bị phát hiện. Việc khởi tạo một sự kiện cần được tách ra khỏi quá trình cấp phép cho sự kiện đó. Khả năng câu kết giữa các cá nhân cũng cần được quan tâm trong khi thiết kế các biện pháp quản lý.

Các tổ chức có quy mô nhỏ có thể sẽ gặp khó khăn trong việc phân tách nhiệm vụ, nhưng cần áp dụng nguyên tắc này đến mức có thể và khả thi. Bất cứ khi nào gặp khó khăn trong việc phân tách nhiệm vụ thì cần quan tâm đến các biện pháp khác như giám sát các hoạt động, truy vết và giám sát của ban quản lý. Điều quan trọng là việc đánh giá tính an toàn phải được thực hiện độc lập.

9.1.4 Phân tách các chức năng phát triển, kiểm thử và vận hành

Biện pháp quản lý

Các chức năng phát triển, kiểm thử và vận hành cần được phân tách nhằm giảm thiểu các rủi ro do truy cập hoặc thay đổi hệ thống vận hành trái phép.

Hướng dẫn triển khai

Cần xác định mức độ phân tách giữa các môi trường vận hành, kiểm thử và phát triển cần cho việc phòng chống các sự cố về vận hành và thực thi các biện pháp quản lý thích hợp.

Cần quan tâm đến các vấn đề sau:

a) các quy tắc chuyển đổi phần mềm từ trạng thái phát triển sang khai thác cần được xác định và lập thành văn bản;

b) phần mềm phát triển và vận hành cần chạy trên các hệ thống hoặc các bộ xử lý máy tính khác nhau và nằm trong các thư mục hoặc miền khác nhau;

c) nếu không có yêu cầu thì từ các hệ thống vận hành không thể truy cập được vào các trình biên dịch, trình biên soạn và các tiện ích hệ thống;

d) môi trường hệ thống thử nghiệm cần mô phỏng môi trường khai thác gần nhất đến mức có thể;

e) người dùng cần sử dụng các hồ sơ người dùng khác nhau cho các hệ thống thử nghiệm và vận hành, và các tùy chọn trong hồ sơ cũng cần hiển thị các thông tin nhận dạng phù hợp nhằm giảm rủi ro mắc lỗi;

f) Không được sao chép dữ liệu nhạy cảm vào môi trường hệ thống thử nghiệm (xem 11.4 ?)

Thông tin khác

Các hoạt động phát triển và thử nghiệm có thể gây ra các vấn đề nghiêm trọng, ví dụ làm sửa đổi không mong muốn các tệp hoặc môi trường hệ thống, hoặc gây ra sự cố hệ thống. Trong trường hợp

này, cần duy trì một môi trường ổn định để có thể thực hiện thử nghiệm theo mục đích và ngăn chặn truy cập không phù hợp.

Khi nhân viên phát triển và nhân viên thử nghiệm truy cập vào hệ thống vận hành và các thông tin của nó thì họ có khả năng đưa vào mã trái phép và chưa được kiểm tra hoặc làm thay đổi dữ liệu hoạt động. Ở một số hệ thống, khả năng này có thể bị lợi dụng nhằm gian lận, hoặc đưa vào mã chưa được kiểm tra hoặc độc hại, và gây ra các sự cố nghiêm trọng.

Các nhân viên phát triển và thử nghiệm cũng có thể đe dọa tới tính bí mật của thông tin vận hành. Các hoạt động thử nghiệm và phát triển có thể gây ra những thay đổi không định trước đối với phần mềm hoặc thông tin nếu họ cùng chia sẻ môi trường hoạt động máy tính. Việc phân tách các thiết bị hỗ trợ phát triển, thử nghiệm và vận hành do vậy rất cần thiết trong việc giảm rủi ro do vô tình thay đổi hoặc truy cập trái phép tới phần mềm khai thác và dữ liệu nghiệp vụ (xem thêm 11.4.2 về vấn đề bảo vệ dữ liệu kiểm tra).

9.2 Quản lý chuyển giao dịch vụ của bên thứ ba

Mục tiêu: Nhằm triển khai và duy trì mức độ an toàn thông tin và việc chuyển giao dịch vụ phù hợp với các thỏa thuận chuyển giao dịch vụ của bên thứ ba.

Tổ chức cần kiểm tra việc triển khai các thỏa thuận, giám sát sự tuân thủ theo các thỏa thuận và quản lý những thay đổi nhằm đảm bảo rằng các dịch vụ được chuyển giao đáp ứng tất cả các yêu cầu đã thỏa thuận với bên thứ ba.

9.2.1 Chuyển giao dịch vụ

Biện pháp quản lý

Cần đảm bảo rằng các biện pháp kiểm soát an toàn, các định nghĩa dịch vụ và mức độ chuyển giao dịch vụ đã được ghi trong thỏa thuận chuyển giao dịch vụ với bên thứ ba đều được bên thứ ba triển khai, vận hành và duy trì.

Hướng dẫn triển khai

Việc chuyển giao dịch vụ do bên thứ ba thực hiện cần bao gồm các chuẩn bị về an toàn đã được thỏa thuận, các định nghĩa dịch vụ, và các vấn đề về quản lý dịch vụ. Trong trường hợp sử dụng nhà thầu bên ngoài thì tổ chức cần lập kế hoạch cho những chuyển giao cần thiết (về thông tin, các thiết bị xử lý thông tin, và bất cứ những gì cần được chuyển giao), và cần đảm bảo rằng vấn đề an toàn được duy trì trong suốt thời gian chuyển giao.

Tổ chức cũng cần đảm bảo rằng bên thứ ba duy trì đủ năng lực dịch vụ cùng với các kế hoạch khả thi đã được thiết kế nhằm đảm bảo rằng các mức duy trì dịch vụ đã thỏa thuận phải được duy trì kể cả trong trường hợp có thảm họa hoặc sự cố dịch vụ nghiêm trọng (xem 13.1).

9.2.2 Giám sát và soát xét các dịch vụ của bên thứ ba

Biện pháp quản lý

Các dịch vụ, báo cáo và hồ sơ do bên thứ ba cung cấp phải được giám sát và soát xét thường xuyên và việc đánh giá phải được tiến hành một cách thường xuyên.

Hướng dẫn triển khai

Việc giám sát và soát xét các dịch vụ của tổ chức thứ ba cần đảm bảo rằng các điều khoản về an toàn thông tin và các điều kiện của các thỏa thuận phải được tôn trọng triệt để, và các sự cố và các vấn đề về an toàn thông tin được quản lý một cách phù hợp. Công việc này cũng cần đến một quy trình và mối quan hệ quản lý dịch vụ giữa tổ chức và bên thứ ba nhằm:

a) giám sát các mức chất lượng dịch vụ để kiểm tra sự tuân thủ các thỏa thuận;

b) soát xét các báo cáo dịch vụ từ bên thứ ba và sắp xếp các cuộc họp xúc tiến định kỳ theo yêu cầu của các thỏa thuận;

c) cung cấp thông tin về các sự cố an toàn thông tin và soát xét thông tin này bởi tổ chức và bên thứ ba như yêu cầu trong các thỏa thuận và các hướng dẫn và thủ tục hỗ trợ bất kỳ;

d) soát xét các truy vết của bên thứ ba và các bản ghi về các sự kiện an toàn, các sự cố vận hành, các lỗi, truy vết các lỗi và các sự cố đứt dịch vụ;

e) giải quyết và quản lý các vấn đề bất kỳ đã được xác định.

Trách nhiệm trong việc quản lý mối quan hệ với bên thứ ba cần được giao cho một cá nhân nào đó hoặc cho đơn vị quản lý dịch vụ. Hơn nữa, tổ chức cần đảm bảo rằng bên thứ ba cũng đã phân định các trách nhiệm về kiểm tra tuân thủ và bắt buộc thực hiện các yêu cầu của các thỏa thuận. Các kỹ năng kỹ thuật và các nguồn tài nguyên cần sẵn sàng cho việc giám sát xem các yêu cầu của các thỏa thuận (xem 5.2.3), đặc biệt là các yêu cầu về an toàn thông tin, có được đáp ứng không. Cần thực hiện hành động phù hợp khi phát hiện thấy có những thiếu sót trong phân phối dịch vụ.

Tổ chức cũng cần duy trì biện pháp quản lý tổng quát thỏa đáng và quản lý được tất cả các khía cạnh về an toàn đối với các thông tin quan trọng, nhạy cảm hoặc các phương tiện xử lý thông tin được truy cập, xử lý hoặc quản lý bởi một tổ chức thứ ba. Tổ chức cần đảm bảo rằng họ vẫn duy trì kiểm soát các hoạt động an toàn như quản lý thay đổi, nhận dạng các yếu điểm, và báo cáo/phản ứng đối với các sự cố an toàn thông tin thông qua một quá trình báo cáo rõ ràng.

Thông tin khác

Trong trường hợp sử dụng nhà thầu thì tổ chức cũng cần lưu ý rằng trách nhiệm sau cùng đối với thông tin được xử lý bởi nhà thầu sẽ vẫn thuộc tổ chức.

9.2.3 Quản lý thay đổi đối với các dịch vụ của bên thứ ba

Biện pháp quản lý

Các thay đổi về cung cấp dịch vụ, bao gồm việc duy trì và cải tiến các chính sách, thủ tục và biện pháp quản lý an toàn thông tin hiện hành cần phải được quản lý, chú ý đến tính quan trọng của các hệ thống và quy trình nghiệp vụ liên quan cũng như việc đánh giá lại các rủi ro.

Hướng dẫn triển khai

Quy trình quản lý các thay đổi về dịch vụ của bên thứ ba cần quan tâm đến:

a) các thay đổi từ tổ chức nhằm triển khai;

1) các cải tiến đối với các dịch vụ hiện tại đang được cung cấp;

2) phát triển các ứng dụng và các hệ thống mới;

3) chỉnh sửa hoặc cập nhật các chính sách và thủ tục của tổ chức;

4) các biện pháp quản lý mới nhằm giải quyết các sự cố an toàn thông tin và nâng cao an toàn thông tin;

b) các thay đổi về dịch vụ của bên thứ ba nhằm triển khai:

1) các thay đổi và cải tiến về mạng;

2) sử dụng các công nghệ mới;

3) sử dụng các sản phẩm mới hoặc các phiên bản mới hơn;

4) các công cụ và các môi trường phát triển mới;

5) các thay đổi về vị trí vật lý của các thiết bị nghiệp vụ;

6) các thay đổi về nhà cung cấp.

9.3 Lập kế hoạch và chấp nhận hệ thống

Mục tiêu: Giảm thiểu rủi ro do lỗi hệ thống

Cần lên kế hoạch và chuẩn bị trước nhằm đảm bảo đủ năng lực và các nguồn tài nguyên sẵn sàng để có hiệu suất hệ thống theo yêu cầu.

Cũng cần đặt kế hoạch cho các yêu cầu năng lực trong tương lai nhằm giảm rủi ro do quá tải hệ thống.

Các yêu cầu về khai thác của các hệ thống mới cần được thiết lập, lập thành văn bản, và kiểm tra trước khi chấp nhận và sử dụng chúng.

9.3.1 Quản lý năng lực hệ thống

Biện pháp quản lý

Việc sử dụng tài nguyên phải được giám sát, điều chỉnh và có dự đoán các yêu cầu về năng lực hệ thống trong tương lai nhằm đảm bảo hiệu suất theo yêu cầu.

Hướng dẫn triển khai

Cần xác định các yêu cầu về năng lực cho từng hoạt động mới và sắp tới. Cần giám sát và điều chỉnh hệ thống nhằm đảm bảo và, nếu cần thiết, nâng cao độ sẵn sàng và hiệu quả của các hệ thống. Cần thực thi các biện pháp quản lý dò tìm nhằm chỉ ra các vấn đề đúng lúc. Các kế hoạch thực thi các yêu

cầu năng lực trong tương lai cần quan tâm đến các yêu cầu hệ thống và nghiệp vụ mới và các xu hướng hiện tại và được dự đoán về các năng lực xử lý thông tin của tổ chức.

Cần đặc biệt lưu ý đến các nguồn tài nguyên có chi phí cao; những người quản lý cần giám sát việc sử dụng các nguồn tài nguyên hệ thống quan trọng. Họ cần xác định những xu hướng sử dụng, đặc biệt trong mối quan hệ với các ứng dụng nghiệp vụ hoặc các công cụ hệ thống thông tin quản lý.

Những người quản lý cần sử dụng thông tin này nhằm xác định và phòng tránh hiện tượng nút cổ chai tiềm ẩn và tránh phụ thuộc vào một cá nhân chủ chốt vì điều đó có thể đe dọa đến sự an toàn hệ thống hoặc các dịch vụ, và lên kế hoạch hành động phù hợp.

9.3.2 Chấp nhận hệ thống

Biện pháp quản lý

Tiêu chí chấp nhận các hệ thống thông tin mới, các cải tiến và các phiên bản mới cần được thiết lập và cần thực hiện các cuộc kiểm tra hệ thống một cách phù hợp trong suốt quá trình phát triển và trước khi chấp nhận hệ thống.

Hướng dẫn triển khai

Những người quản lý cần đảm bảo rằng các yêu cầu và tiêu chí chấp nhận các hệ thống mới phải được xác định rõ ràng, được đồng thuận, được lập thành văn bản, và được kiểm tra. Các hệ thống mới, những nâng cấp, và các phiên bản mới chỉ được chuyển sang giai đoạn sản xuất sau khi đã được chính thức chấp nhận. Các điều khoản sau cần được quan tâm trước khi đưa ra chấp nhận chính thức:

a) hiệu suất và các yêu cầu về năng lực máy tính;

b) các thủ tục khởi động lại và khôi phục sau lỗi, và các kế hoạch đối phó với các sự kiện bất ngờ;

c) chuẩn bị và kiểm tra các thủ tục hoạt động thông thường theo các tiêu chẩn nhất định;

d) bộ các biện pháp quản lý an toàn đã được thông qua;

e) các thủ tục điều hành hiệu quả;

f) các hoạt động nghiệp vụ thường xuyên (xem 13.1);

g) chứng cứ cho thấy việc lắp đặt hệ thống mới này sẽ không gây bất lợi cho các hệ thống hiện tại, đặc biệt tại các thời gian xử lý cao điểm, như cuối tháng;

h) chứng cứ cho thấy vấn đề tác động của hệ thống mới lên sự an toàn chung của tổ chức đã được quan tâm xem xét;

i) đào tạo khai thác hoặc sử dụng các hệ thống mới;

j) tính dễ sử dụng, vì điều này ảnh hưởng đến hiệu suất sử dụng của khách hàng và tránh các lỗi do con người.

Đối với những hệ thống mới quan trọng, bộ phận điều hành và người dùng cần được tư vấn ở tất cả các giai đoạn trong quá trình phát triển nhằm đảm bảo hiệu suất khai thác theo thiết kế hệ thống. Cần

thực hiện các cuộc kiểm tra phù hợp nhằm chắc chắn rằng tất cả các chỉ tiêu chấp nhận đã được thỏa mãn hoàn toàn.

Thông tin khác

Thủ tục chấp nhận có thể bao gồm cả thủ tục cấp chứng chỉ chính thức và chính thức công nhận nhằm xác nhận rằng các yêu cầu về an toàn đã được thỏa mãn.

9.4 Bảo vệ chống lại mã độc hại và mã di động

Mục tiêu: Nhằm bảo vệ tính toàn vẹn của thông tin và phần mềm.

Cần có những đề phòng nhằm ngăn ngừa và phát hiện sự có mặt của mã độc hại và mã di động trái phép.

Phần mềm và các phương tiện xử lý thông tin là các đối tượng rất dễ bị tổn tại bởi mã độc, ví dụ các loại virut máy tính, sâu mạng, ngựa trojan, và bom máy tính. Người dùng cần có nhận thức về những mối nguy hiểm từ mã độc hại. Nếu thích hợp thì người quản lý cần đưa ra các biện pháp quản lý nhằm ngăn chặn, phát hiện, loại bỏ mã độc hại và xử lý mã di động.

9.4.1 Quản lý chống lại mã độc hại

Biện pháp quản lý

Các biện pháp quản lý trong việc phát hiện, ngăn chặn, và phục hồi nhằm chống lại các đoạn mã độc hại và các thủ tục tuyên truyền nâng cao nhận thức của người dùng phải được thực hiện.

Hướng dẫn triển khai

Bảo vệ chống lại mã độc hại cần dựa trên cơ sở phát hiện mã độc hại và sửa chữa phần mềm, nâng cao nhận thức về an toàn thông tin, và các biện pháp quản lý thay đổi và truy cập hệ thống phù hợp. Cần quan tâm đến những hướng dẫn sau:

a) thiết lập một chính sách chính thức ngăn cấm sử dụng phần mềm trái phép (xem 14.1.2);

b) thiết lập một chính sách chính thức nhằm bảo vệ chống lại các rủi ro liên quan đến việc sử dụng các tệp và phần mềm đến từ hoặc đi qua các mạng bên ngoài, hoặc bất kỳ một môi trường nào khác, chỉ ra các biện pháp bảo vệ cần thực hiện;

c) chỉ đạo các cuộc soát xét thường xuyên phần mềm và các nội dung dữ liệu của các hệ thống hỗ trợ các quá trình nghiệp vụ then chốt; cần chính thức điều tra sự xuất hiện của các tệp chưa được chấp nhận hoặc các bổ sung trái phép;

d) cài đặt và thường xuyên cập nhật phần mềm khắc phục và phát hiện mã độc hại để quét máy tính và các phương tiện với vai trò như một biện pháp phòng ngừa; các cuộc kiểm tra cần bao gồm:

    1) trước khi sử dụng cần kiểm tra mã độc hại đối với tất cả các tệp trên thiết bị điện tử hoặc quang học, và các tệp nhận được trên mạng;

2) trước khi sử dụng cần kiểm tra mã độc hại đối với các tệp đính kèm trên thư điện tử và các tệp tải được trên mạng; việc kiểm tra này cần được thực hiện tại các nơi khác nhau, ví dụ tại cả các máy chủ thư điện tử, các máy tính để bàn và cả khi xâm nhập vào mạng của tổ chức;

3) kiểm tra mã độc hại trong các trang mạng;

e) xác định các thủ tục và trách nhiệm quản lý trong việc bảo vệ chống lại mã độc hại trên các hệ thống, đào tạo sử dụng các thủ tục này, báo cáo và khôi phục hệ thống trước sự tấn công của mã độc hại (xem 12.1 và 12.2);

f) chuẩn bị các kế hoạch đảm bảo sự liên tục về nghiệp vụ cho việc khôi phục sau những tấn công của mã độc hại, bao gồm toàn bộ những chuẩn bị khôi phục và sao lưu phần mềm và dữ liệu cần thiết (xem 13);

g) triển khai các thủ tục nhằm thường xuyên thu thập thông tin, ví dụ đăng ký vào danh sách thư điện tử và/hoặc kiểm tra các địa chỉ mạng cho thông tin về các loại mã độc hại mới;

h) triển khai các thủ tục xác thực thông tin liên quan đến mã độc hại và đảm bảo rằng các bản tin cảnh báo là chính xác và cung cấp được nhiều thông tin; những người quản lý cần đảm bảo có các nguồn tin cậy, ví dụ các tờ báo có tiếng tăm, các địa chỉ internet hoặc các nhà sản xuất phần mềm chống mã độc hại đáng tin cậy, được sử dụng nhằm phân biệt giữa các trò lừa đảo và mã độc hại thực sự; tất cả những người dùng cần được trang bị kiến thức về những trò lừa đảo và những việc phải làm khi nhận được chúng

Thông tin khác

Sử dụng hai hoặc nhiều sản phẩm phần mềm chống mã độc hại của nhiều nhà cung cấp khác nhau trong môi trường xử lý thông tin có thể nâng cao hiệu quả phòng chống mã độc.

Phần mềm giúp bảo vệ chống lại mã độc hại có thể được cài đặt nhằm cung cấp các nội dung cập nhật của các tệp định nghĩa và các công cụ quét nhằm chắc chắn rằng việc bảo vệ đã được cập nhật. Hơn nữa, phần mềm này có thể được cài đặt trên mọi máy tính để bàn nhằm thực hiện kiểm tra tự động.

Cần quan tâm đến việc bảo vệ chống lại sự xâm nhập của mã độc hại trong các thủ tục bảo dưỡng và khẩn cấp, do chúng có thể bị bỏ qua khi sử dụng các biện pháp chống mã độc hại thuần túy.

9.4.2 Kiểm soát các mã di động

Biện pháp quản lý

Đối với các mã di động hợp lệ, việc cài đặt phải đảm bảo phù hợp với các chính sách an toàn đã được đặt ra. Ngược lại, các đoạn mã di động trái phép sẽ bị ngăn chặn.

Hướng dẫn triển khai

Cần quan tâm đến các hoạt động sau nhằm ngăn chặn mã di động thực hiện các hoạt động chưa được cấp phép:

a) thực thi mã di động trong một môi trường được cô lập về mặt logic;

b) hạn chế sử dụng mã di động;

c) hạn chế nhận mã di động;

d) kích hoạt các biện pháp kỹ thuật sẵn sàng trên một hệ thống chuyên dụng nhằm quản lý mã di động;

e) quản lý các nguồn tài nguyên sẵn sàng cho truy cập mã di động;

f) quản lý bằng mật mã nhằm xác thực mã di động.

Thông tin khác

Mã di động là một mã phần mềm truyền từ máy tính này sang máy tính khác và sau đó tự động thực hiện một chức năng nào đó mà không có tương tác người dùng hoặc chỉ có một ít. Mã di động liên quan đến rất nhiều dịch vụ phần mềm trung gian.

Bên cạnh việc đảm bảo mã di động không chứa mã độc hại thì việc quản lý mã độc hại cũng rất cần thiết nhằm ngăn ngừa sử dụng trái phép hoặc làm phá vỡ hệ thống, mạng, hoặc các nguồn tài nguyên ứng dụng và các vi phạm an toàn thông tin khác.

9.5 Sao lưu

Mục tiêu: Nhằm duy trì sự toàn vẹn và sự sẵn sàng của thông tin và các phương tiện xử lý thông tin.

Cần thiết lập các thủ tục thường xuyên nhằm thực hiện chiến lược và chính sách sao lưu đã được thỏa thuận (xem 13.1) trong việc sao lưu và kịp thời khôi phục dữ liệu.

9.5.1 Sao lưu thông tin

Biện pháp quản lý

Thông tin và phần mềm cần được sao lưu và thường xuyên kiểm tra lại chúng theo chính sách sao lưu đã được thỏa thuận.

Hướng dẫn triển khai

Cần cung cấp các phương tiện sao lưu thích hợp nhằm đảm bảo rằng tất cả các thông tin và phần mềm cần thiết có thể được khôi phục lại sau thảm họa hoặc lỗi hỏng thiết bị.

Cần quan tâm đến các vấn đề sau trong việc sao lưu thông tin:

a) cần xác định mức độ cần thiết của thông tin sao lưu;

b) cần đưa ra các bản sao lưu đầy đủ và chính xác và các văn bản về thủ tục khôi phục;

c) phạm vi (ví dụ sao lưu đầy đủ hoặc từng phần) và tần suất sao lưu cần thể hiện các yêu cầu nghiệp vụ của tổ chức, các yêu cầu về an toàn thông tin có liên quan, và độ quan trọng của thông tin trong việc đảm bảo tính liên tục về nghiệp vụ của tổ chức;

d) các bản sao cần được lưu giữ ở một vị trí ở xa, với khoảng cách phù hợp nhằm tránh những thiệt hại do thảm họa tại trụ sở chính.

e) thông tin sao chép cần được đặt ở mức độ bảo vệ vật lý và môi trường phù hợp (xem điều 8) tuân thủ các tiêu chuẩn được áp dụng tại trụ sở chính; các biện pháp quản lý được áp dụng đối với thiết bị tại trụ sở chính cũng cần được thực hiện tại nơi chứa bản sao lưu;

f) thiết bị sao chép cần được kiểm tra định kỳ nhằm đảm bảo rằng chúng có thể tin cậy trong điều kiện sử dụng khẩn cấp;

g) các thủ tục khôi phục thông tin cần được xem xét và kiểm tra định kỳ nhằm đảm bảo chúng hoạt động hiệu quả và chúng có thể được thực hiện đầy đủ trong khoảng thời gian đã được xác định trong các thủ tục khai thác về khôi phục;

h) Trong các trường hợp khi tính bí mật là một yêu cầu quan trọng thì các bản sao cần được bảo vệ bằng các hình thức mã hóa.

Các thủ tục sao lưu dành cho các hệ thống riêng cần được kiểm tra thường xuyên nhằm đảm bảo rằng chúng đáp ứng được các yêu cầu của các kế hoạch đảm bảo tính liên tục về nghiệp vụ (xem điều 13). Đối với các hệ thống quan trọng thì cần thực hiện sao lưu tất cả thông tin, các ứng dụng, dữ liệu cần thiết của hệ thống nhằm có thể phục hồi được toàn bộ hệ thống trong trường hợp có thảm họa xảy ra.

Thời gian lưu trữ các thông tin nghiệp vụ cần thiết và các yêu cầu lưu trữ bản sao lâu dài cũng cần được xác định (xem 14.1.3).

Thông tin khác

Có thể thực hiện sao lưu tự động nhằm làm dễ dàng quy trình sao lưu và khôi phục. Các giải pháp tự động như vậy cần được kiểm tra phù hợp trước khi triển khai và vào các thời điểm định kỳ.

9.6 Quản lý an toàn mạng

Mục tiêu: Nhằm đảm bảo an toàn cho thông tin trên mạng và an toàn cho cơ sở hạ tầng hỗ trợ.

Việc quản lý an toàn mạng, có thể mở rộng ra ngoài phạm vi tổ chức, đòi hỏi phải chú ý đến luồng dữ liệu, các vấn đề pháp lý liên quan, việc giám sát, và bảo vệ.

Có thể yêu cầu thêm các biện pháp quản lý hỗ trợ nhằm bảo vệ không cho thông tin nhạy cảm lọt ra các mạng công cộng.

9.6.1 Kiểm soát mạng

Các biện pháp quản lý

Các mạng cần được quản lý và kiểm soát một cách thỏa đáng nhằm bảo vệ khỏi các mối đe dọa và duy trì sự an toàn cho các hệ thống, các ứng dụng sử dụng mạng và thông tin đang được truyền trên mạng.

Hướng dẫn triển khai

Những người quản lý mạng cần triển khai các biện pháp quản lý nhằm đảm bảo sự an toàn của thông tin trên mạng, và đảm bảo bảo vệ các dịch vụ kết nối trước sự truy cập trái phép. Cụ thể là, cần quan tâm đến các vấn đề sau:

a) nếu cần, phải tách bạch trách nhiệm về mặt khai thác mạng với việc vận hành máy tính (xem 9.1.3);

b) cần thiết lập các trách nhiệm và thủ tục đối với việc quản lý thiết bị ở xa, bao gồm cả thiết bị ở trong phạm vi của người dùng;

c) cần thiết lập các biện pháp quản lý đặc biệt nhằm bảo vệ tính bí mật và sự toàn vẹn của dữ liệu đi qua các mạng công cộng hoặc qua các mạng vô tuyến, và bảo vệ các hệ thống được kết nối và các ứng dụng (xem 10.4 và 11.3); các biện pháp bảo vệ đặc biệt có thể được yêu cầu nhằm duy trì khả năng sẵn sàng của các dịch vụ mạng và các máy tính được kết nối;

d) cần áp dụng hình thức ghi nhật ký và giám sát phù hợp nhằm ghi lại các hoạt động liên quan đến an toàn thông tin;

e) cần phối hợp chặt chẽ các hoạt động quản lý nhằm tối ưu dịch vụ đồng thời đảm bảo rằng các biện pháp quản lý đã được áp dụng nhất quán qua hạ tầng xử lý thông tin.

Thông tin khác

Có thể tìm thêm thông tin về an toàn mạng trong ISO/IEC 18028, Công nghệ thông tin - Các kỹ thuật an toàn – An toàn mạng IT.

9.6.2 An toàn cho các dịch vụ mạng

Biện pháp quản lý

Các tính năng an toàn, các mức dịch vụ và các yêu cầu quản lý của tất cả các dịch vụ mạng cần được xác định và ghi rõ trong thỏa thuận về các dịch vụ mạng, bất kể dịch vụ là do nội bộ cấp hay thuê khoán.

Hướng dẫn triển khai

Cần xác định và thường xuyên giám sát khả năng của nhà cung cấp dịch vụ mạng trong việc quản lý an toàn các dịch vụ đã thỏa thuận, và cũng cần thỏa thuận về quyền đánh giá.

Cũng cần xác định các yêu cầu về an toàn cần thiết cho các dịch vụ cụ thể, ví dụ như các thuộc tính dịch vụ, các mức dịch vụ, và các yêu cầu về quản lý. Tổ chức cần đảm bảo rằng các nhà cung cấp dịch vụ có triển khai các biện pháp này.

Thông tin khác

Các dịch vụ mạng bao gồm cung cấp kết nối, các dịch vụ mạng riêng, và các mạng cung cấp dịch vụ giá trị gia tăng và các giải pháp an toàn mạng được quản lý, ví dụ các hệ thống tường lửa và các hệ

thống phát hiện xâm nhập. Các dịch vụ này có thể là dạng dịch vụ đơn giản có băng thông không được quản lý đến các dịch vụ giá trị gia tăng phức tạp.

Các thuộc tính an toàn của các dịch vụ mạng có thể là:

a) công nghệ được áp dụng nhằm đảm bảo sự an toàn của các dịch vụ mạng, như xác thực, mã hóa, và các biện pháp quản lý kết nối;

b) các tham số kỹ thuật về kết nối an toàn của các dịch vụ mạng tuân theo độ an toàn và các quy tắc kết nối mạng;

c) các thủ tục sử dụng dịch vụ mạng nhằm hạn chế truy cập tới các dịch vụ mạng hoặc các ứng dụng, nếu cần thiết.

9.7 Xử lý phương tiện

Mục tiêu: Nhằm ngăn chặn tiết lộ, sửa đổi, xóa bỏ hoặc phá hoại tài sản trái phép, và làm gián đoán các hoạt động nghiệp vụ.

Phương tiện hỗ trợ cần được quản lý và bảo vệ vật lý.

Cần thiết lập các thủ tục hoạt động phù hợp nhằm bảo vệ các tài liệu, phương tiện hỗ trợ máy tính (ví dụ, băng từ, đĩa), tài liệu hệ thống và dữ liệu đầu vào/đầu ra khỏi việc tiết lộ, sửa đổi, xóa bỏ và phá hủy trái phép.

9.7.1 Quản lý các phương tiện có thể di dời

Biện pháp quản lý

Cần có các thủ tục sẵn sàng cho việc quản lý các phương tiện có thể di dời.

Hướng dẫn triển khai

Khi quản lý các phương tiện có thể di dời, cần quan tâm đến các hướng dẫn sau:

a) nếu không cần nữa thì nội dung của các phương tiện có thể tái sử dụng mà sắp bị loại bỏ khỏi tổ chức cần được xử lý sao cho không thể khôi phục được;

b) nếu cần thiết và khả thi thì việc loại bỏ phương tiện khỏi tổ chức cần được cấp phép và báo cáo về các phương tiện bị loại bỏ cần được giữ lại nhằm duy trì truy vết;

c) tất cả các phương tiện cần được đặt trong môi trường an toàn, bảo mật theo các chỉ tiêu kỹ thuật của nhà sản xuất;

d) thông tin lưu giữ mà cần phải tồn tại lâu hơn tuổi thọ của phương tiện lưu giữ (theo các chỉ tiêu kỹ thuật của nhà sản xuất) cũng cần được cất ở một nơi khác nhằm tránh mất mát thông tin do hư hỏng thiết bị;

e) cũng cần quan tâm đến việc đăng ký phương tiện có thể di dời nhằm hạn chế khả năng bị mất dữ liệu;

f) chỉ cho phép các ổ đĩa rời nếu có lý do nghiệp vụ.

Tất cả các thủ tục và các mức độ cấp phép phải được lập thành văn bản rõ ràng.

Thông tin khác

Phương tiện có thể di dời bao gồm các loại băng, đĩa, ổ cứng di động, các ổ cứng dễ di dời, CD, DVD, và các tài liệu in sẵn.

9.7.2 Loại bỏ phương tiện

Biện pháp quản lý

Các phương tiện cần được loại bỏ một cách an toàn và bảo mật khi không còn cần thiết theo các thủ tục xử lý chính thức.

Hướng dẫn triển khai

Các thủ tục chính thức nhằm loại bỏ phương tiện một cách an toàn cần phải tối giảm rủi ro tiết lộ thông tin cho những người không được phép. Các thủ tục hủy bỏ phương tiện chứa thông tin nhạy cảm cần tương xứng với độ nhạy cảm của thông tin. Cần quan tâm đến các vấn đề sau:

a) phương tiện chứa thông tin nhạy cảm cần được lưu giữ và loại bỏ an toàn và đảm bảo, ví dụ bằng cách đốt hoặc cắt nhỏ, hoặc xóa dữ liệu;

b) cần thực hiện các thủ tục nhằm xác định danh mục các phương tiện yêu cầu phải bị loại bỏ một cách an toàn;

c) sẽ thuận tiện nếu gom tất cả các phương tiện phải được thu thập và loại bỏ một cách an toàn hơn là cố gắng tách ra các danh mục phương tiện nhạy cảm;

d) có rất nhiều các tổ chức cung cấp các dịch vụ thu thập và loại bỏ báo chí, thiết bị và các phương tiện; tuy nhiên, cần thận trọng trong việc lựa chọn nhà thầu có các biện pháp và kinh nghiệm phù hợp;

e) nếu có thể thì cần ghi lại việc loại bỏ các phương tiện nhạy cảm nhằm duy trì truy vết;

Khi gom các phương tiện cần loại bỏ thì cần quan tâm đến hậu quả kết hợp, hậu quả này có thể làm cho một lượng lớn thông tin không nhạy cảm lại trở thành thông tin nhạy cảm.

Thông tin khác

Thông tin nhạy cảm có thể được loại bỏ thông qua quy trình loại bỏ phương tiện một cách cẩn thận (xem thêm 8.2.6 để có thông tin về việc loại bỏ thiết bị).

9.7.3 Các thủ tục xử lý thông tin

Biện pháp quản lý

Các thủ tục xử lý và lưu giữ thông tin phải được thiết lập nhằm bảo vệ thông tin khỏi sự tiết lộ hoặc sử dụng bất hợp pháp.

Hướng dẫn triển khai

Cần xây dựng các thủ tục thu thập, xử lý, lưu giữ và trao đổi thông tin theo phân lớp của nó (xem 6.2). Cần quan tâm đến các vấn đề sau:

a) xử lý và dán nhãn cho tất cả các phương tiện theo mức phân loại của nó;

b) các hạn chế truy cập nhằm ngăn chặn truy cập của các cá nhân chưa được cấp phép;

c) lưu lại hồ sơ chính thức về những người nhận dữ liệu đã được cấp phép;

d) đảm bảo rằng dữ liệu đầu vào là đầy đủ, quá trình xử lý đã hoàn tất và đã áp dụng quá trình phê chuẩn đầu ra;

e) bảo vệ đầu ra của dữ liệu đồng tác theo mức tương ứng với độ nhạy của nó;

f) cất giữ phương tiện theo các chỉ tiêu kỹ thuật của nhà sản xuất;

g) giữ cho việc phân phối dữ liệu ở mức hạn chế nhất;

h) đánh dấu rõ ràng tất cả các bản sao của phương tiện để người nhận hợp pháp lưu ý;

i) soát xét lại các danh sách phân phối và danh sách những người nhận hợp pháp.

Thông tin khác

Các thủ tục này áp dụng đối với thông tin trong các văn bản, hệ thống máy tính, mạng, tính toán di động, truyền thông di động, thư, hộp thư thoại, truyền thông thoại nói chung, đa phương tiện, các dịch vụ/tiện ích bưu chính, sử dụng các máy sao chép và các danh mục nhạy cảm nào khác, ví dụ các tờ séc trống, hóa đơn.

9.7.4 An toàn cho các tài liệu hệ thống

Biện pháp quản lý

Các tài liệu hệ thống cần được bảo vệ khỏi sự truy cập trái phép.

Hướng dẫn triển khai

Nhằm đảm bảo an toàn cho các tài liệu hệ thống, cần quan tâm đến các vấn đề sau:

a) tài liệu hệ thống cần được cất giữ một cách an toàn;

b) danh sách truy cập tài liệu hệ thống cần được giữ lại ở mức tối thiểu và được cấp phép bởi người sở hữu ứng dụng;

c) cần bảo vệ một cách thích hợp các tài liệu hệ thống được giữ ở mạng công cộng, hoặc được cung cấp qua mạng công cộng.

Thông tin khác

Tài liệu hệ thống có thể chứa các thông tin nhạy cảm, ví dụ các bản mô tả về các quy trình ứng dụng, các thủ tục, các cấu trúc dữ liệu, các quy trình cấp phép.

9.8 Trao đổi thông tin

Mục tiêu: Nhằm duy trì an toàn cho các thông tin và phần mềm được trao đổi trong nội bộ tổ chức hoặc với các thực thể bên ngoài.

Những trao đổi thông tin và phần mềm giữa các tổ chức cần dựa trên một chính sách trao đổi chính thức, được thực hiện theo các thỏa thuận trao đổi, và cần tuân thủ các quy định của pháp luật liên quan.

Cần thiết lập các thủ tục và các tiêu chuẩn nhằm bảo vệ thông tin và phương tiện vật lý chứa thông tin trong quá trình trao đổi

9.8.1 Các chính sách và thủ tục trao đổi thông tin

Biện pháp quản lý

Các chính sách, thủ tục và biện pháp quản lý chính thức cần phải sẵn có để bảo vệ sự trao đổi thông tin thông qua hệ thống truyền thông.

Hướng dẫn triển khai

Các biện pháp và thủ tục cần tuân thủ khi sử dụng các phương tiện truyền thông điện tử trong trao đổi thông tin cần quan tâm đến các vấn đề sau:

a) các thủ tục được thiết kế nhằm bảo vệ thông tin được trao đổi khỏi sự nghe lén, sao chép, sửa đổi, sai địa chỉ, và phá hủy;

b) các thủ tục nhằm phát hiện và bảo vệ chống lại mã độc hại bị phát tán khi sử dụng các phương tiện truyền thông điện tử (xem 9.4.1);

c) các thủ tục nhằm bảo vệ thông tin điện tử nhạy cảm được trao đổi có tệp tin đính kèm;

d) chính sách hoặc các hướng dẫn sơ lược về sử dụng các phương tiện truyền thông điện tử (xem 6.1.3);

e) các thủ tục sử dụng các phương tiện truyền thông vô tuyến, quan tâm đến các rủi ro cụ thể;

f) trách nhiệm của nhân viên, người của nhà thầu và những người dùng khác trong việc không làm ảnh hưởng xấu đến tổ chức, ví dụ phỉ báng, quấy rối, mạo danh, chuyển các bức thư hàng loạt, mua bán trái phép...;

g) có thể sử dụng các kỹ thuật mật mã nhằm bảo vệ tính bí mật, tính toàn vẹn và tính xác thực của thông tin (xem 11.3);

h) hướng dẫn ngăn chặn và hủy bỏ các thư từ giao dịch, bao gồm cả các thông điệp, theo các quy định và quy chế nội bộ và quốc gia có liên quan;

i) không được để thông tin nhạy cảm hoặc thông tin quan trọng trên các thiết bị in ấn, ví dụ các máy sao chụp tài liệu, máy in, máy quét, vì chúng có thể bị truy cập bởi những cá nhân không được phép;

j) các biện pháp quản lý và các hạn chế liên quan đến việc chuyển tiếp các phương tiện truyền thông, ví dụ tự động chuyển tiếp thư điện tử vào các địa chỉ hộp thư bên ngoài;

k) nhắc nhở với mọi người về việc thực hiện đề phòng, ví dụ không tiết lộ thông tin nhạy cảm nhằm tránh không bị nghe lỏm hoặc bị nghe trộm khi đang gọi điện thoại bởi:

   1) những người ở xung quanh, đặc biệt là khi đang sử dụng điện thoại di động;

   2) nghe trộm, và các hình thức nghe trộm khác thông qua truy nhập vật lý đến máy điện thoại cầm tay hoặc đường điện thoại, hoặc sử dụng các máy thu quét;

   3) những người ở đầu máy kia;

l) không để các thông điệp chứa thông tin nhạy cảm ở các máy trả lời vì các thông điệp này có thể bị những người không có quyền nghe lại, cất giữ trên các hệ thống công cộng hoặc cất giữ không đúng quy cách do quay số nhầm;

m) nhắc nhở với mọi người về các sự cố do sử dụng máy sao chép, cụ thể là:

   1) truy cập trái phép vào các bộ lưu giữ thông điệp bên trong nhằm lấy các thông điệp;

   2) cố ý hoặc vô tình lập trình cho các máy thực hiện gửi các thông điệp đến các số cụ thể nào đó;

   3) do quay số sai hoặc sử dụng số lưu trữ sai mà gửi nhầm các tài liệu và các thông điệp;

n) nhắc nhở mọi người không được đăng ký dữ liệu cá nhân, ví dụ các thông tin như địa chỉ thư điện tử hoặc các thông tin cá nhân khác, trong bất cứ phần mềm nào nhằm tránh bị thu thập thông tin cho các mục đích sử dụng trái phép;

o) nhắc nhở mọi người rằng các máy sao chụp tài liệu hiện đại đều có các bộ nhớ trong và có thể lưu được nội dung các trang trong trường hợp có lỗi truyền dẫn hoặc lỗi về giấy in, các trang này sẽ được in lại ngay khi lỗi được khắc phục.

Hơn nữa, cũng cần nhắc nhở mọi người không được nói những điều bí mật ở các nơi công cộng hoặc các văn phòng rộng và các nơi hộp họp không có tường cách âm.

Các phương tiện trao đổi thông tin cần tuân thủ các yêu cầu pháp lý liên quan (xem 14).

Thông tin khác

Có thể xảy ra trao đổi thông tin khi sử dụng nhiều loại phương tiện truyền thông khác nhau, bao gồm thư điện tử, thoại, sao chụp, và hình ảnh.

Có thể xảy ra trao đổi phần mềm thông qua nhiều phương thức khác nhau, bao gồm tải thông tin từ internet và tải thông tin được các nhà cung cấp các sản phẩm mua có sẵn yêu cầu.

Cần quan tâm đến những vấn đề về an toàn, pháp lý và nghiệp vụ liên quan đến việc trao đổi dữ liệu điện tử, thương mại điện tử, truyền thông điện tử và các yêu cầu về các biện pháp quản lý.

Thông tin có thể bị tổn hại do sự thiếu hiểu biết, các thủ tục và chính sách sử dụng các phương tiện trao đổi thông tin, ví dụ bị nghe trộm trên máy điện thoại di động ở nơi công cộng, chuyển sai địa chỉ của thông điệp thư điện tử, các máy trả lời bị nghe trộm, truy cập trái phép đến các hệ thống hộp thư thoại quay số hoặc vô tình gửi nhầm đến thiết bị sao chụp tài liệu.

Các hoạt động nghiệp vụ có thể bị phá vỡ và thông tin có thể bị tổn hại nếu các phương tiện truyền thông bị lỗi, bị quá tải hoặc bị ngắt kết nối (xem 9.3 và điều 13). Thông tin có thể bị tổn hại nếu bị truy cập bởi những người dùng trái phép (xem điều 10).

9.8.2 Các thỏa thuận trao đổi

Biện pháp quản lý

Các thỏa thuận cần được thiết lập cho việc trao đổi thông tin và phần mềm giữa tổ chức và các thực thể bên ngoài.

Hướng dẫn triển khai

Các thỏa thuận trao đổi cần quan tâm đến các điều kiện an toàn sau đây:

a) các trách nhiệm của ban quản lý trong việc quản lý và thông báo về việc truyền, gửi và nhận thông tin chuyển giao;

b) các thủ tục thông báo với người gửi về việc truyền, gửi và nhận;

c) các thủ tục đảm bảo khả năng truy vết và không thể chối bỏ;

d) các tiêu chuẩn kỹ thuật tối thiểu cho việc đóng gói và truyền;

e) các thỏa thuận giao kèo;

f) các tiêu chuẩn nhận dạng cách thức chuyển;

g) các trách nhiệm và nghĩa vụ khi có các sự kiện an toàn thông tin, như mất dữ liệu;

h) sử dụng hệ thống dán nhãn đã thỏa thuận đối với các thông tin quan trọng hoặc nhạy cảm, đảm bảo rằng ý nghĩa của các nhãn có thể được hiểu ngay và thông tin đó đã được bảo vệ phù hợp;

i) quyền sở hữu và các trách nhiệm bảo vệ dữ liệu, bản quyền, tuân thủ bản quyền phần mềm và các vấn đề tương tự khác (xem 14.1.2 và 14.1.4);

j) các tiêu chuẩn kỹ thuật cho ghi và đọc thông tin và phần mềm;

k) các biện pháp quản lý đặc biệt có thể được yêu cầu nhằm bảo vệ các danh mục thông tin nhạy cảm, như các khóa bảo mật (xem 11.3).

Các chính sách, thủ tục, và tiêu chuẩn cần được thiết lập và được quản lý nhằm bảo vệ thông tin và phương tiện vật lý trong quá trình trao đổi (xem thêm 9.8.3), và cần được tham chiếu trong các thỏa thuận trao đổi.

Nội dung về an toàn của các thỏa thuận cần thể hiện độ nhạy cảm của thông tin nghiệp vụ liên quan.

Thông tin khác

Các thỏa thuận có thể ở dạng điện tử hoặc viết tay, và hình thức có thể như các bản hợp đồng chính thức hoặc các điều kiện tuyển dụng. Đối với thông tin nhạy cảm thì các cơ chế đặc biệt sử dụng cho trao đổi thông tin đó cần phù hợp với tất cả các tổ chức và các loại thỏa thuận.

9.8.3 Vận chuyển phương tiện vật lý

Biện pháp quản lý

Phương tiện chứa thông tin cần được bảo vệ khỏi sự truy cập trái phép, sự lạm dụng hoặc làm sai lệch khi vận chuyển vượt ra ngoài phạm vi địa lý của tổ chức.

Hướng dẫn triển khai

Cần quan tâm đến các hướng dẫn sau nhằm bảo vệ phương tiện chứa thông tin trong quá trình vận chuyển giữa các địa điểm:

a) sử dụng phương tiện và người vận chuyển tin cậy;

b) cần thỏa thuận với ban quản lý về danh sách những người được phép vận chuyển;

c) cần áp dụng các thủ tục kiểm tra lai lịch người vận chuyển;

d) đóng gói cẩn thận nhằm bảo vệ nội dung của các phương tiện khỏi các hư hại vật lý có khả năng xảy ra trong quá trình vận chuyển và tuân theo các chỉ tiêu kỹ thuật của nhà sản xuất (ví dụ đối với phần mềm), ví dụ bảo vệ chống lại các yếu tố về môi trường có khả năng làm giảm hiệu quả khôi phục dữ liệu của phương tiện như nhiệt độ, độ ẩm hoặc các trường điện từ;

e) nếu cần, phải sử dụng các biện pháp quản lý nhằm bảo vệ thông tin nhạy cảm khỏi sự sửa đổi hoặc tiết lộ trái phép, ví dụ :

    1) sử dụng các hộp chứa có khóa;

    2) vận chuyển bằng tay;

    3) dán niêm phong (nhằm phát hiện truy cập);

    4) trong các trường hợp ngoại lệ, phân chia thành nhiều phần và gửi đi theo các đường khác nhau.

Thông tin khác

Thông tin có thể bị đe dọa bởi truy cập trái phép, lạm dụng hoặc bị sửa đổi sai lệch trong quá trình vận chuyển vật lý, ví dụ khi gửi phương tiện bằng dịch vụ bưu chính hoặc qua người chuyển.

9.8.4 Thông điệp điện tử

Biện pháp quản lý

Thông tin bao hàm trong các thông điệp điện tử cần được bảo vệ một cách thỏa đáng.

Hướng dẫn triển khai

Cần quan tâm đến các vấn đề an toàn sau đối với thông điệp điện tử:

a) bảo vệ thông điệp khỏi sự truy cập trái phép, sửa đổi hoặc từ chối dịch vụ;

b) đảm bảo đánh đúng địa chỉ và gửi đúng địa chỉ thông điệp;

c) độ tin cậy và độ sẵn sàng chung của dịch vụ;

d) các vấn đề pháp lý, ví dụ các yêu cầu về chữ ký điện tử;

e) được chấp thuận trước khi sử dụng các dịch vụ công cộng bên ngoài như nhắn tin nhanh hoặc chia sẻ tệp;

f) truy cập từ các mạng công cộng dễ truy cập phải được quản lý bằng mức xác thực cao hơn.

Thông tin khác

Thông điệp điện tử như thư điện tử, trao đổi dữ liệu điện tử (EDI), và nhắn tin nhanh đóng vai trò ngày càng cao trong các giao dịch thương mại. Thông điệp điện tử chứa nhiều rủi ro hơn truyền thông bằng giấy.

9.8.5 Các hệ thống thông tin nghiệp vụ

Biện pháp quản lý

Các chính sách và thủ tục cần được phát triển và triển khai nhằm bảo vệ các thông tin liên quan đến sự kết nối các hệ thống thông tin nghiệp vụ.

Hướng dẫn triển khai

Cần quan tâm đến những vấn đề về an toàn và nghiệp vụ khi kết nối các phương tiện:

a) hiểu rõ những yếu điểm trong các hệ thống quản trị và kế toán nơi thông tin được chia sẻ giữa các bộ phận khác nhau của tổ chức;

b) các yếu điểm của thông tin trong các hệ thống truyền thông nghiệp vụ, ví dụ ghi các cuộc gọi điện thoại hoặc các cuộc gọi hội nghị, sự bảo mật của các cuộc gọi, cất giữ các bản sao, mở thư, phân phát thư;

c) chính sách và các biện pháp quản lý thích hợp nhằm quản lý chia sẻ thông tin;

d) không cho phép chia sẻ các thông tin nghiệp vụ nhạy cảm và các tài liệu phân loại nếu hệ thống không cung cấp mức bảo vệ phù hợp (xem 6.2);

e) hạn chế truy cập vào thông tin nhật ký liên quan đến các cá nhân được lựa chọn, ví dụ những người làm việc trong các dự án nhạy cảm;

f) các loại nhân viên, nhà thầu hoặc các đối tác nghiệp vụ được phép sử dụng hệ thống và các vị trí mà từ đó hệ thống có thể được truy cập (xem 5.2);

g) giới hạn sử dụng các thiết bị nhất định chỉ với những người dùng nhất định;

h) xác định tình trạng của những người dùng, ví dụ các nhân viên của tổ chức hoặc người của các nhà thầu;

i) cất giữ và sao lưu thông tin chứa trên hệ thống (xem 9.5.1);

j) các yêu cầu và thủ tục lưu giữ (xem 13).

Thông tin khác

Các hệ thống thông tin văn phòng có nhiều cơ hội cho việc phổ biến và chia sẻ thông tin nghiệp vụ nhanh chóng bằng cách kết hợp các tài liệu, máy tính, tính toán di động, truyền thông di động, thư, thư thoại, truyền thông thoại nói chung, đa phương tiện, các dịch vụ/phương tiện bưu chính và máy sao chụp.

9.9 Các dịch vụ thương mại điện tử

Mục tiêu: Nhằm đảm bảo an toàn cho các dịch vụ thương mại điện tử và sử dụng chúng một cách an toàn

Cần quan tâm đến các vấn đề an toàn liên quan đến việc sử dụng các dịch vụ thương mại điện tử, bao gồm cả giao dịch trực tuyến, và các yêu cầu về kiểm soát. Cũng cần quan tâm đến tính toàn vẹn và độ sẵn sàng của thông tin đã được xuất bản điện tử thông qua các hệ thống công cộng.

9.9.1 Thương mại điện tử

Biện pháp quản lý

Thông tin trong thương mại điện tử truyền qua các mạng công cộng cần được bảo vệ khỏi các hoạt động gian lận, các tranh cãi về giao kèo, sửa đổi và tiết lộ trái phép.

Hướng dẫn triển khai

Cần quan tâm đến vấn đề về an toàn sau trong thương mại điện tử:

a) xác định mức độ tin cậy mà mỗi bên yêu cầu bên kia, ví dụ thông qua xác thực;

b) quy trình cấp phép liên quan đến người được phép định giá, ban hành hoặc ký các văn bản thương mại quan trọng;

c) chắc chắn rằng các đối tác thương mại đã được thông báo đầy đủ về quyền của họ;

d) xác định và tuân theo các yêu cầu về bảo mật, toàn vẹn, xác minh việc gửi và nhận các tài liệu quan trọng, và không thể chối bỏ các bản hợp đồng, ví dụ các bản hợp đồng liên quan đến các quá trình bỏ thầu và ký hợp đồng;

e) mức tin cậy được yêu cầu về tính toàn vẹn của các bảng giá được công bố;

f) tính bí mật của thông tin và dữ liệu nhạy cảm;

g) tính bí mật và tính toàn vẹn của các giao dịch đặt hàng, thông tin về thanh toán, chi tiết về địa chỉ giao hàng, và xác nhận của người nhận hàng;

h) mức độ xác thực phù hợp nhằm kiểm tra thông tin thanh toán do khách hàng cung cấp;

i) lựa chọn hình thức thanh toán phù hợp nhất nhằm bảo vệ chống gian lận;

j) mức bảo vệ được yêu cầu nhằm duy trì tính bí mật và tính toàn vẹn của thông tin đặt hàng;

k) tránh mất mát hoặc sao chép thông tin giao dịch;

l) trách nhiệm pháp lý liên quan đến các giao dịch lừa đảo;

m) các yêu cầu về bảo hiểm

Rất nhiều trong số các vấn đề trên có thể được giải quyết nếu áp dụng các kỹ thuật mật mã (xem 11.3), lưu ý tuân thủ các yêu cầu pháp lý (xem 14.1, đặc biệt là 14.1.6 về luật mật mã hóa).

Các hoạt động thương mại điện tử giữa các bên cần được hỗ trợ bằng một văn bản thỏa thuận có các điều khoản thỏa thuận về thương mại ký giữa các bên, văn bản này chứa các chi tiết về cấp phép (xem b) ở trên). Có thể cần thêm các thỏa thuận khác với các nhà cung cấp mạng giá trị gia tăng và dịch vụ thông tin.

Các hệ thống thương mại công cộng cần công khai các điều khoản về giao dịch với khách hàng.

Cần lưu ý tới khả năng phục hồi sau tấn công của các máy chủ được sử dụng cho thương mại điện tử và các vấn đề an toàn của kết nối mạng được yêu cầu cho triển khai các dịch vụ thương mại điện tử (xem 10.4.6).

Thông tin khác

Thương mại điện tử thường bị đe dọa bởi những mối đe dọa từ các hoạt động gian lận, các tranh cãi về giao kèo, tiết lộ hoặc sửa đổi thông tin.

Thương mại điện tử có thể sử dụng các phương pháp xác thực an toàn, ví dụ sử dụng mật mã khóa công khai và chữ ký số (xem thêm 11.3) nhằm giảm các rủi ro. Ngoài ra, có thể sử dụng các bên thứ ba đủ tin cậy nếu có các yêu cầu về dịch vụ.

9.9.2 Các giao dịch trực tuyến

Biện pháp quản lý

Thông tin trong các giao dịch trực tuyến cần được bảo vệ khỏi việc truyền thông tin không đầy đủ, sai địa chỉ, sửa đổi thông điệp trái phép, tiết lộ trái phép, sao chép thông điệp trái phép hoặc thực hiện lại giao dịch.

Hướng dẫn triển khai

Cần quan tâm đến các vấn đề an toàn sau trong thương mại điện tử:

a) việc sử dụng chữ ký điện tử của các bên tham gia giao dịch;

b) tất cả các khía cạnh về giao dịch, nhằm đảm bảo rằng:

1) các ủy nhiệm người dùng của tất cả các bên đều hợp lệ và đã được xác minh;

2) giao dịch đảm bảo tin cậy; và

3) tính riêng tư của tất cả các bên đều được duy trì;

c) luồng thông tin trao đổi giữa tất cả các bên tham gia đều được mã hóa;

d) các giao thức sử dụng nhằm trao đổi thông tin giữa tất cả các bên tham gia được đảm bảo an toàn;

e) đảm bảo rằng các thông tin chi tiết về giao dịch được lưu trữ ở bên ngoài môi trường công cộng dễ truy cập, ví dụ nằm trong một bộ phận lưu trữ thuộc mạng nội bộ của tổ chức, và không được lưu trữ trong một môi trường lưu trữ dễ dàng truy cập trực tiếp từ Internet;

f) nếu sử dụng một chuyên gia đủ tin cậy (ví dụ để ban hành và duy trì các chữ ký số và/hoặc các chứng chỉ số) thì an toàn thông tin sẽ là sự kết hợp và nằm trong toàn bộ quy trình quản lý chứng chỉ/chữ ký từ đầu đến cuối.

Thông tin khác

Phạm vi của các biện pháp quản lý được sử dụng cần tương ứng với mức độ rủi ro liên quan đến từng loại hình giao dịch trực tuyến.

Các giao dịch có thể cần phải tuân theo các quy định của luật pháp, các quy tắc và điều lệ trong phạm vi pháp lý mà giao dịch được khởi tạo, được xử lý, được hoàn thành, và/hoặc được lưu trữ.

Có rất nhiều loại hình giao dịch có thể được thực hiện theo phương thức trực tuyến, ví dụ hợp đồng, tài chính...

9.9.3 Thông tin công khai

Biện pháp quản lý

Tính toàn vẹn của các thông tin công khai trên hệ thống công cộng cần phải được bảo vệ nhằm ngăn chặn sửa đổi trái phép.

Hướng dẫn triển khai

Cần có các cơ chế bảo vệ thích hợp, ví dụ chữ ký số (xem 11.3), nhằm bảo vệ các phần mềm, dữ liệu và các thông tin yêu cầu mức toàn vẹn cao khác sẽ được công bố trên hệ thống thông tin đại chúng,. Hệ thống truy cập công cộng cần được kiểm tra trước khi thông tin được công bố.

Cần có một quá trình phê chuẩn chính thức trước khi thông tin được công bố. Hơn nữa, tất cả các đầu vào được cung cấp từ bên ngoài hệ thống cũng cần được xác minh và phê chuẩn.

Các hệ thống xuất bản điện tử, đặc biệt là các hệ thống cho phép phản hồi và đưa trực tiếp thông tin vào, cần được quản lý cẩn thận sao cho:

a) thông tin thu được tuân theo các quy định pháp lý về bảo vệ dữ liệu (xem 14.1.4);

b) đầu vào thông tin tới và được xử lý bởi hệ thống xuất bản sẽ được xử lý hoàn chỉnh và chính xác đúng lúc;

c) thông tin nhạy cảm sẽ được bảo vệ trong quá trình thu thập, xử lý và lưu trữ;

d) truy cập đến hệ thống xuất bản không cho phép truy cập không có mục đích vào các mạng mà hệ thống kết nối tới.

Thông tin khác

Thông tin trên hệ thống công cộng, ví dụ thông tin trên một máy chủ Web có thể truy cập qua Internet, có thể cần phải tuân theo các quy định của luật pháp, các quy tắc và điều lệ ở phạm vi pháp lý mà hệ thống đang tồn tại, nơi xảy ra giao dịch hoặc nơi người sở hữu cư trú. Việc chỉnh sửa trái phép thông tin được xuất bản có thể làm tổn hại đến danh tiếng của tổ chức phát hành.

9.10 Giám sát

Mục tiêu: Nhằm phát hiện các hoạt động xử lý thông tin trái phép

Cần giám sát các hệ thống và ghi lại các sự kiện liên quan đến an toàn thông tin. Các nhật ký của người điều hành và nhật ký lỗi có thể được sử dụng nhằm đảm bảo nhận biết được tất cả các vấn đề về hệ thống thông tin.

Tổ chức cần tuân thủ tất cả các yêu cầu pháp lý liên quan trong các hoạt động giám sát và ghi nhật ký.

Giám sát hệ thống cũng cần được sử dụng nhằm kiểm tra tính hiệu quả của các biện pháp quản lý được áp dụng và kiểm chứng sự phù hợp với một mô hình chính sách truy cập.

9.10.1 Ghi nhật ký đánh giá

Biện pháp quản lý

Việc ghi lại tất cả các hoạt động của người dùng, các lỗi ngoại lệ và các sự kiện an toàn thông tin cần phải được thực hiện và duy trì trong một khoảng thời gian theo thỏa thuận nhằm trợ giúp việc điều tra và giám sát điều khiển truy cập sau này.

Hướng dẫn triển khai

Các nhật ký đánh giá cần bao gồm:

a) các ID của người dùng;

b) ngày tháng, thời gian, và các chi tiết về các sự kiện quan trọng, ví dụ đăng nhập và thoát ra;

c) vị trí hoặc nhận dạng cuối cùng nếu có thể;

d) các báo cáo về những truy cập thành công và bị từ chối;

e) các báo cáo về dữ liệu truy cập thành công và bị từ chối và những lần truy cập các nguồn tài nguyên khác;

f) những thay đổi về cấu hình hệ thống;

g) sử dụng đặc quyền;

h) sử dụng các ứng dụng và các tiện ích hệ thống;

i) các tệp được truy cập và loại truy cập;

j) các địa chỉ và giao thức mạng;

k) các cảnh báo từ hệ thống điều khiển truy cập;

l) việc kích hoạt và giải kích hoạt các hệ thống bảo vệ, ví dụ như các hệ thống chống virut và các hệ thống phát hiện xâm nhập.

Thông tin khác

Các nhật ký đánh giá có thể chứa dữ liệu cá nhân bí mật. Cần thực hiện các biện pháp bảo vệ riêng phù hợp (xem thêm 14.1.4). Nếu có thể thì những người quản trị hệ thống không được phép xóa bỏ hoặc giải kích hoạt các nhật ký về các hoạt động riêng của họ (xem 9.1.3).

9.10.2 Giám sát sử dụng hệ thống

Biện pháp quản lý

Các thủ tục giám sát việc sử dụng các phương tiện xử lý thông tin cần được thiết lập và thường xuyên xem xét lại kết quả giám sát.

Hướng dẫn triển khai

Mức độ giám sát yêu cầu đối với từng thiết bị cần được xác định bằng đánh giá rủi ro. Tổ chức cần tuân thủ tất cả các yêu cầu pháp lý liên quan áp dụng cho các hoạt động giám sát. Các phạm vi giám sát cần được quan tâm bao gồm:

a) truy cập được phép, bao gồm các thông tin chi tiết như:

1) ID của người dùng;

2) ngày tháng và thời gian của các sự kiện quan trọng;

3) các loại sự kiện;

4) các tệp được truy cập;

5) các chương trình/tiện ích được sử dụng;

b) tất cả các hoạt động được ưu tiên, như:

1) sử dụng các tài khoản ưu tiên, ví dụ người giám sát, gốc, người quản trị;

2) khởi động và dừng hệ thống;

3) cắm/tháo thiết bị I/O;

c) những nỗ lực truy cập trái phép, như:

1) các hành động bị lỗi hoặc bị từ chối của người dùng;

2) các hành động bị lỗi hoặc bị từ chối liên quan đến dữ liệu và các nguồn tài nguyên khác;

3) những vi phạm chính sách truy cập và những thông báo đối với các cổng và bức tường lửa của mạng;

4) các cảnh báo từ các hệ thống phát hiện xâm nhập riêng;

d) các cảnh báo hoặc lỗi hệ thống như:

1) các cảnh báo hoặc thông điệp từ bảng điều khiển;

2) những ngoại lệ trên nhật ký hệ thống;

3) các cảnh báo về quản lý mạng;

4) các cảnh báo từ các hệ thống điều khiển truy cập;

e) những thay đổi đối với, hoặc những nỗ lực thay đổi các cài đặt và biện pháp quản lý an toàn hệ thống.

Tần suất soát xét các kết quả của hoạt động giám sát cần dựa trên các rủi ro liên quan. Các yếu tố rủi ro cần được lưu ý bao gồm:

a) tầm quan trọng của các quy trình ứng dụng;

b) giá trị, độ nhạy cảm, và tầm quan trọng của thông tin liên quan;

c) các trường hợp xâm nhập và lạm dụng trước đây, và tần suất điểm yếu bị khai thác;

d) phạm vi của kết nối hệ thống (đặc biệt là các mạng công cộng);

e) phương tiện ghi nhật ký đang bị giải kích hoạt.

Thông tin khác

Các thủ tục giám sát sử dụng rất cần thiết nhằm đảm bảo rằng người dùng chỉ đang thực hiện các hoạt động đã được cấp phép.

Việc soát xét lại nhật ký sẽ giúp hiểu được những mối đe dọa mà hệ thống phải đối mặt và phương thức xuất hiện của chúng. 12.1.1 sẽ đưa ra những ví dụ về các sự kiện có thể yêu cầu phải điều tra thêm trong trường hợp có các sự cố an toàn thông tin.

9.10.3 Bảo vệ các thông tin nhật ký

Biện pháp quản lý

Các chức năng ghi nhật ký và thông tin nhật ký cần được bảo vệ khỏi sự giả mạo và truy cập trái phép.

Hướng dẫn triển khai

Các biện pháp cần hướng tới việc bảo vệ khỏi những thay đổi trái phép và các vấn đề về sử dụng chức năng ghi nhật ký, bao gồm:

a) những thay đổi đối với các loại thông điệp đã được ghi lại;

b) các tệp nhật ký đã bị chỉnh sửa hoặc xóa bỏ;

c) dung lượng lưu trữ của phương tiện ghi nhật ký đang bị vượt, dẫn đến lỗi đối với các sự kiện đã ghi được hoặc ghi đè lên các sự kiện đã ghi trước đây.

Một số nhật ký đánh giá có thể được yêu cầu như một phần của chính sách lưu giữ các báo cáo hoặc do các yêu cầu phải thu thập và lưu giữ chứng cứ (xem thêm 12.2.3).

Thông tin khác

Các nhật ký hệ thống thường chứa một lượng lớn thông tin, phần lớn trong số chúng lại không liên quan đến việc giám sát an toàn. Để dễ dàng nhận diện các sự kiện quan trọng cho các mục đích giám sát an toàn thì cần quan tâm đến việc tự động sao chép lại các loại thông điệp phù hợp vào một nhật ký thứ hai, và/hoặc sử dụng các tiện ích hệ thống phù hợp hoặc các công cụ đánh giá nhằm thực hiện điều tra và hợp lý hóa tệp.

Các nhật ký hệ thống cần được bảo vệ, vì nếu dữ liệu có thể bị sửa đổi hoặc dữ liệu trong nhật ký bị xóa bỏ thì sự tồn tại của chúng có thể gây ra lỗi an toàn thông tin.

9.10.4 Nhật ký của người điều hành và người quản trị

Biện pháp

Các hoạt động của người quản trị và người điều hành hệ thống cần được ghi vào nhật ký.

Hướng dẫn triển khai

Các nhật ký cần bao gồm các thông tin sau:

a) thời gian xảy ra sự kiện (dù thành công hay thất bại);

b) thông tin về sự kiện (ví dụ các tệp được xử lý) hoặc sự cố (ví dụ lỗi xảy ra và hoạt động sửa lỗi đã được thực hiện);

c) tài khoản nào và người quản trị hoặc người điều hành nào tham gia;

d) các hoạt động nào đã được thực hiện.

Cần thường xuyên soát xét lại các nhật ký của người điều hành và quản trị hệ thống.

Thông tin khác

Bên cạnh việc kiểm soát những người quản trị và điều hành, có thể sử dụng thêm hệ thống phát hiện xâm nhập nhằm giám sát hệ thống và các hoạt động quản trị mạng cần tuân thủ.

9.10.5 Ghi nhật ký lỗi

Biện pháp

Các lỗi cần được ghi lại, được phân tích và có các hoạt động xử lý cần thiết.

Hướng dẫn triển khai

Những lỗi được thông báo bởi người dùng hoặc bởi các chương trình hệ thống liên quan đến các hệ thống truyền thông hoặc xử lý thông tin cần được ghi vào nhật ký. Cần thiết lập các quy tắc rõ ràng nhằm xử lý các lỗi được thông báo, bao gồm:

a) soát xét lại các nhật ký lỗi nhằm đảm bảo rằng các lỗi này đã được giải quyết thỏa đáng;

b) soát xét lại các biện pháp sửa lỗi nhằm đảm bảo rằng các biện pháp này vẫn hiệu quả, và hành động đã thực hiện là hoàn toàn được phép.

Cần đảm bảo rằng chức năng ghi nhật ký lỗi đã được kích hoạt nếu chức năng này đã sẵn sàng.

Thông tin khác

Việc ghi nhật ký lỗi và sự cố có thể ảnh hưởng đến chất lượng của hệ thống. Ghi nhật ký lỗi cần được thực hiện bởi một nhân viên có kỹ năng, và mức độ ghi nhật ký được yêu cầu đối với các hệ thống cũng cần được xác định bằng đánh giá rủi ro, trong đó cần quan tâm đến sự suy giảm chất lượng hệ thống.

9.10.6 Đồng bộ thời gian

Biện pháp quản lý

Đồng hồ trên các hệ thống xử lý thông tin trong tổ chức hoặc trong một phạm vi an toàn cần được đồng bộ với một nguồn thời gian chính xác đã được đồng ý lựa chọn.

Hướng dẫn triển khai

Nếu một máy tính hoặc thiết bị truyền thông có khả năng điều khiển một đồng hồ thời gian thực thì đồng hồ này cần được đặt về một chuẩn theo thỏa thuận, ví dụ UTC hoặc thời gian chuẩn nội bộ. Vì một số đồng hồ thường bị trôi thời gian nên cần có thủ tục kiểm tra và hiệu chỉnh đồng hồ.

Cách hiển thị định dạng ngày/giờ rất quan trọng trong việc đảm bảo phản ánh đúng thời gian thực. Cần lưu ý các đặc điểm có tính chất địa phương (như thay đổi giờ theo mùa...).

Thông tin khác

Đặt các đồng hồ máy tính một cách chính xác là vấn đề quan trọng nhằm đảm bảo tính chính xác của các nhật ký đánh giá, các nhật ký đánh giá này có thể cần cho việc điều tra hoặc là bằng chứng trong các trường hợp vi phạm pháp luật hoặc kỷ luật. Các nhật ký đánh giá không chính xác có thể gây trở ngại cho các cuộc điều tra và làm ảnh hưởng đến độ tin cậy của các bằng chứng. Đồng hồ được liên kết đến một chương trình phát thanh vô tuyến từ một đồng hồ nguyên tử quốc gia có thể được sử dụng như đồng hồ chủ đối với các hệ thống ghi nhật ký. Có thể sử dụng một giao thức thời gian mạng để giữ cho tất cả các đồng hồ tớ đều đồng bộ với đồng hồ chủ.

10 Quản lý truy cập.

10.1 Yêu cầu nghiệp vụ đối với quản lý truy cập

Mục tiêu: Quản lý các truy cập thông tin
Truy cập thông tin, các phương tiện xử lý thông tin, và các quy trình nghiệp vụ cần được kiểm soát trên cơ sở các yêu cầu về nghiệp vụ và an toàn thông tin.
Các quy tắc quản lý truy cập cần lưu ý các chính sách về phổ biến và cấp phép.

10.1.1 Chính sách quản lý truy cập

Biện pháp quản lý

Chính sách quản lý truy cập cần được thiết lập, ghi thành văn bản và soát xét dựa trên các yêu cầu nghiệp vụ và an toàn đối với các truy cập.

Hướng dẫn triển khai

Các quyền và nguyên tắc quản lý truy cập đối với mỗi người dùng hoặc nhóm người dùng cần được công bố rõ ràng trong chính sách quản lý truy cập. Các biện pháp quản lý truy cập phải bao gồm cả về mặt logic và vật lý (xem trong điều 8) và chúng phải được xem xét đồng thời. Các nhà cung cấp dịch vụ và người dùng cần được tuyên bố rõ ràng về các yêu cầu nghiệp vụ phải được đáp ứng bởi với các biện pháp quản lý truy cập.

Chính sách quản lý truy cập cần quan tâm đến các vấn đề sau:

a) các yêu cầu về an toàn thông tin của các ứng dụng nghiệp vụ riêng;

b) nhận diện tất cả các thông tin liên quan tới các ứng dụng nghiệp vụ và các rủi ro đối với thông tin.

c) các chính sách về cấp phép và phổ biến thông tin, ví dụ nhu cầu phải biết về nguyên tắc và các mức độ an toàn thông tin và phân loại thông tin (xem 6.2);

d) sự thống nhất các chính sách quản lý truy cập và phân loại thông tin của các mạng và các hệ thống khác nhau;

e) quy định của pháp luật và các nghĩa vụ thỏa thuận bất kỳ liên quan đến việc bảo vệ truy cập dữ liệu hoặc các dịch vụ (xem 14.1)

f) các hồ sơ truy cập chuẩn của người dùng đối với các vai trò nhiệm vụ chung trong tổ chức;

g) việc quản lý các quyền truy cập trong một môi trường nối mạng và phân tán, môi trường này nhận ra tất cả các dạng kết nối sẵn có;

h) việc phân tách các vai trò quản lý truy cập, ví dụ yêu cầu truy cập, việc cấp phép truy cập, quản trị truy cập;

i) các yêu cầu đối với việc cấp phép chính thức cho các yêu cầu truy cập (xem 10.2.1);

j) các yêu cầu đối với việc soát xét định kỳ những biện pháp quản lý truy cập;

k) loại bỏ các quyền truy cập (xem 7.3.3).

Thông tin khác

Cần quan tâm tới các vấn đề sau khi xác định các quy tắc quản lý truy cập:

a) phân biệt giữa các quy tắc luôn phải tuân theo và các hướng dẫn có tính chất lựa chọn hoặc điều kiện;

b) thiết lập các quy tắc dựa trên tiêu chí "mọi thứ đều bị cấm trừ khi được công bố cho phép"

c) những thay đổi trong các nhãn thông tin (xem 6.2) được khởi tạo tự động bởi các phương tiện xử lý thông tin và do ý muốn của một người dùng;

d) những thay đổi về việc cho phép người dùng được khởi tạo tự động bởi hệ thống thông tin và bởi một người quản trị hệ thống;

e) các quy tắc đòi hỏi hoặc không đòi hỏi phải được chấp thuận trước khi ban hành.

Các quy tắc quản lý truy cập cần được hỗ trợ bởi các thủ tục chính thức và các trách nhiệm đã được xác định rõ (ví dụ, xem 5.1.3; 10.3; 9.4.1; 10.6)

10.2Quản lý truy cập người dùng

Mục đích: Nhằm đảm bảo người dùng hợp lệ được truy cập và ngăn chặn những người dùng không hợp lệ truy cập trái phép tới các hệ thống thông tin.

Các thủ tục chính thức phải được thực hiện nhằm quản lý việc cấp phát quyền truy cập các hệ thống và dịch vụ thông tin.

Các thủ tục cần bao hàm tất cả các giai đoạn trong quá trình truy cập của người dùng, từ việc đăng ký khởi tạo những người dùng mới tới việc hủy bỏ đăng ký của những người dùng không còn yêu cầu truy cập tới các hệ thống và dịch vụ thông tin. Nếu thích hợp thì cần chú ý đến nhu cầu quản lý cấp phát các đặc quyền truy cập, tức là quyền cho phép người dùng bỏ qua các biện pháp quản lý hệ thống.

10.2.1 Đăng ký người dùng

Biện pháp quản lý

Cần thiết phải có một thủ tục chính thức về đăng ký và hủy đăng ký người dùng để thực hiện cấp phát hoặc thu hồi quyền truy cập đến tất cả các hệ thống và dịch vụ thông tin.

Hướng dẫn triển khai

Thủ tục quản lý truy cập cho đăng ký hoặc hủy đăng ký người dùng cần bao gồm những điều sau:

a) sử dụng các ID người dùng duy nhất nhằm cho phép nhiều người dùng có thể được liên kết tới và giữ trách nhiệm đối với các hoạt động của họ; việc sử dụng các ID nhóm chỉ được cho phép nếu chúng cần thiết cho các lý do điều hành hoặc nghiệp vụ, và cần được phê duyệt và ghi vào văn bản.

b) kiểm tra xem người dùng đã được chủ sở hữu hệ thống cấp phép sử dụng hệ thống hoặc dịch vụ thông tin chưa; có thể cũng phù hợp nếu phê chuẩn riêng các quyền truy cập từ ban quản lý;

c) kiểm tra xem mức độ truy cập được cấp có phù hợp với mục đích nghiệp vụ (xem 10.1) và phù hợp với chính sách an ninh của tổ chức không, ví dụ nó không gây ảnh hưởng tới việc phân tách nhiệm vụ (xem 9.1.3)

d) cấp cho người dùng một tờ thông báo về các quyền truy cập của họ;

e) yêu cầu người dùng ký vào các tờ thông báo rằng họ đã hiểu các điều kiện truy cập;

f) đảm bảo rằng các nhà cung cấp dịch vụ không cung cấp truy cập cho tới khi đã hoàn tất các thủ tục cấp phép;

g) duy trì một hồ sơ chính thức về tất cả những người đã đăng ký sử dụng dịch vụ;

h) lập tức loại bỏ hoặc chặn các quyền truy cập của những người dùng đã thay đổi vai trò hoặc công việc hoặc nghỉ việc;

i) kiểm tra định kỳ, loại bỏ hoặc chặn các ID người dùng và các tài khoản thừa (xem 10.2.4);

j) đảm bảo rằng các ID thừa không được cấp cho những người dùng khác.

Thông tin khác

Cần quan tâm đến việc thiết lập các vai trò truy cập của người dùng dựa trên các yêu cầu nghiệp vụ, các yêu cầu này tóm tắt nhiều quyền truy cập thành các hồ sơ truy cập riêng của người dùng. Các yêu cầu và các soát xét truy cập (xem 10.2.4) sẽ được quản lý dễ dàng ở cấp độ vai trò hơn ở cấp các quyền cụ thể.

Cần quan tâm đến các điều khoản của các hợp đồng cá nhân và hợp đồng dịch vụ trong đó nói đến các hình phạt đối với các truy cập trái phép thực hiện bởi cá nhân hoặc các phòng dịch vụ (xem thêm 5.1.5, 7.1.3 và 8.2.3)

10.2.2 Quản lý đặc quyền

Biện pháp quản lý

Việc cấp phát và sử dụng các đặc quyền cần phải được giới hạn và kiểm soát.

Hướng dẫn triển khai

Những hệ thống nhiều người dùng có yêu cầu bảo vệ trước các truy cập trái phép cần được quản lý cấp phát đặc quyền thông qua một quy trình cấp phép chính thức. Những bước dưới đây cần được quan tâm:

a) cần xác định các đặc quyền truy cập gắn liền với mỗi sản phẩm hệ thống, ví dụ hệ điều hành, hệ thống quản lý cơ sở dữ liệu và mỗi ứng dụng, và những người dùng cần được phân bổ quyền truy cập;

b) các đặc quyền cần được phân bổ cho những người dùng dựa trên cơ sở cần - sử dụng và trên cơ sở từng sự kiện phù hợp với chính sách quản lý truy cập (10.1.1), nghĩa là yêu cầu tối thiểu đối với vai trò chức năng của họ chỉ khi được yêu cầu;

c) cần duy trì một quy trình cấp phép và một hồ sơ các đặc quyền đã được phân bổ. Không được cấp phép các đặc quyền cho đến khi quá trình cấp phép đã hoàn tất;

d) cần đẩy mạnh phát triển và sử dụng các thủ tục hệ thống để tránh phải cấp phép các đặc quyền cho người dùng;

e) cần đẩy mạnh phát triển và sử dụng các chương trình không cần chạy cùng với các đặc quyền;

f) các đặc quyền phải được gán cho một ID người dùng khác với các ID người dùng được sử dụng cho mục đích nghiệp vụ thông thường.

Thông tin khác

Việc sử dụng không phù hợp các đặc quyền quản trị hệ thống (tính năng hay tiện ích bất kỳ của hệ thống thông tin cho phép người dùng bỏ qua các biện pháp kiểm soát hệ thống hoặc ứng dụng) có thể là một yếu tố chính gây ra các lỗi hay các lỗ hổng hệ thống.

10.2.3 Quản lý mật khẩu người dùng

Biện pháp quản lý

Việc cấp phát mật khẩu người dùng cần được kiểm soát thông qua một quy trình quản lý chính thức.

Hướng dẫn triển khai

Quá trình quản lý mật khẩu người dùng cần bao hàm những yêu cầu sau:

a) người dùng cần được yêu cầu ký vào một tờ in sẵn để giữ bí mật các mật khẩu cá nhân và giữ các mật khẩu nhóm chỉ trong nội bộ các thành viên của nhóm; bản ký này có thể nằm trong các điều khoản và điều kiện tuyển dụng (xem 7.1.3);

b) khi người dùng được yêu cầu duy trì các mật khẩu riêng của mình, ban đầu họ cần phải được cung cấp một mật khẩu an toàn tạm thời (xem 10.3.1), mật khẩu này sau đó sẽ buộc phải được thay đổi ngay;

c) thiết lập các thủ tục nhằm xác minh danh tính của người dùng trước khi cung cấp một mật khẩu mới, mật khẩu thay thế hoặc mật khẩu tạm thời;

d) các mật khẩu tạm thời phải được trao cho người dùng một cách an toàn; việc sử dụng của bên thứ ba hoặc các thông điệp thư điện tử không được bảo vệ cần được tránh;

e) các mật khẩu tạm thời phải là duy nhất đối với mỗi cá nhân và không thể đoán được;

f) người dùng cần có kiến thức về việc nhận các mật khẩu;

g) không được lưu mật khẩu trên các hệ thống máy tính ở định dạng không được bảo vệ;

h) các mật khẩu mặc định của nhà cung cấp cần được thay đổi ngay sau khi cài đặt hệ thống và phần mềm.

Thông tin khác

Mật khẩu là phương tiện phổ biến trong việc xác minh danh tính của người dùng trước khi truy cập tới các hệ thống thông tin hay các dịch vụ. Các công nghệ khác để nhận dạng và xác thực người dùng, chẳng hạn như sinh trắc học, ví dụ như kiểm tra dấu vân tay, xác minh chữ ký, và sử dụng thẻ phần cứng, ví dụ thẻ thông minh, cần được sẵn sàng và cần được quan tâm nếu thích hợp.

10.2.4 Soát xét các quyền truy cập của người dùng

Biện pháp quản lý

Ban quản lý cần định kỳ soát xét các quyền truy cập của người dùng theo một quy trình chính thức.

Hướng dẫn triển khai

Việc soát xét các quyền truy cập cần quan tâm đến các hướng dẫn sau đây:

a) các quyền truy cập của người dùng cần được soát xét định kỳ, ví dụ chu kỳ 6 tháng, và khi có những thay đổi bất kỳ, ví dụ được đề bạt, bị giáng chức, hoặc kết thúc công việc (xem 10.2.1);

b) các quyền truy cập của người dùng cần được soát xét và phân bổ lại khi người dùng chuyển từ công việc này sang công việc khác trong tổ chức;

c) các cấp phép cho các đặc quyền truy cập đặc biệt cần được soát xét thường xuyên hơn, ví dụ chu kỳ 3 tháng;

d) các phân bổ đặc quyền cũng phải được kiểm tra định kỳ nhằm đảm bảo rằng những đặc quyền chưa được cấp phép thì không được sử dụng;

e) những thay đổi của các tài khoản đặc quyền cần được ghi vào nhật ký soát xét định kỳ.

Thông tin khác

Cần soát xét định kỳ các quyền truy cập của người dùng nhằm duy trì kiểm soát hiệu quả các truy cập tới các dữ liệu và dịch vụ thông tin.

10.3Các trách nhiệm của người dùng

Mục tiêu: Nhằm ngăn chặn người dùng trái phép truy cập, làm tổn hại hoặc lấy cắp thông tin cũng như các phương tiện xử lý thông tin.

Sự hợp tác của những người dùng đã được cấp phép rất cần thiết để đạt được hiệu quả an toàn thông tin.

Người dùng cần nhận thức được các trách nhiệm của mình trong việc duy trì các biện pháp quản lý truy cập hiệu quả, đặc biệt phải quan tâm đến việc sử dụng các mật khẩu và sự an toàn của trang thiết bị người dùng.

Cần triển khai chính sách màn hình sạch và bàn làm việc sạch nhằm giảm thiểu rủi ro truy cập trái phép hoặc làm hư hại văn bản giấy tờ, phương tiện và các phương tiện xử lý thông tin.

10.3.1 Sử dụng mật khẩu

Biện pháp quản lý

Người dùng phải được yêu cầu tuân thủ quy tắc thực hành an toàn tốt trong việc lựa chọn và sử dụng mật khẩu.

Hướng dẫn triển khai

Tất cả những người dùng cần được tư vấn:

a) giữ bí mật các mật khẩu;

b) tránh giữ hồ sơ (ví dụ giấy, tập tin phần mềm hoặc thiết bị cầm tay) của các mật khẩu, trừ khi hồ sơ này có thể được lưu trữ an toàn và phương pháp lưu trữ đã được phê duyệt;

c) thay đổi mật khẩu bất cứ khi nào có bất kỳ dấu hiệu về tổn hại hệ thống hoặc mật khẩu;

d) chọn mật khẩu chất lượng với độ dài tối thiểu mà:

   1) dễ nhớ;

   2) không dựa trên bất cứ điều gì mà người khác có thể dễ dàng đoán hoặc có được nhờ các thông tin có liên quan tới cá nhân đó, ví dụ như tên, số điện thoại, và ngày tháng năm sinh...

   3) không dễ bị tổn hại bởi những tấn công dò tìm mật khẩu thông qua từ điển (tức là không chứa các từ có trong từ điển);

   4) không phải là dạng các ký tự hay các số giống nhau liên tiếp.

e) thay đổi mật khẩu theo định kỳ hay dựa trên số lần truy cập (mật khẩu cho các tài khoản đặc quyền cần thay đổi mật khẩu thường xuyên hơn bình thường), và tránh sử dụng lại mật khẩu cũ hoặc quay vòng các mật khẩu cũ;

f) thay đổi mật khẩu tạm thời ở lần truy cập đầu tiên;

g) không đưa mật khẩu vào thủ tục đăng nhập tự động, ví dụ được lưu trữ trong chương trình macro hay khóa chức năng;

h) không chia sẻ mật khẩu người dùng cá nhân;

i) không sử dụng chung một mật khẩu cho tất cả các mục đích nghiệp vụ và không phải nghiệp vụ.

Nếu người dùng cần truy cập nhiều dịch vụ, hệ thống hay nền tảng chương trình và được yêu cầu phải duy trì nhiều mật khẩu riêng thì họ phải được tư vấn rằng họ có thể sử dụng một mật khẩu chất lượng, duy nhất (xem phần d) ở trên) cho tất cả các dịch vụ mà người dùng được bảo đảm rằng mức độ bảo vệ hợp lý đã được thiết lập đối với việc lưu trữ mật khẩu trong mỗi dịch vụ, hệ thống hay nền tảng chương trình.

Thông tin khác

Việc quản lý hệ thống hỗ trợ để giải quyết các mật khẩu bị mất hoặc quên cần được đặc biệt quan tâm vì đây cũng có thể là một phương tiện tấn công hệ thống mật khẩu.

10.3.2 Thiết bị người dùng khi không sử dụng

Biện pháp quản lý

Người dùng cần đảm bảo rằng thiết bị phải được bảo vệ thích hợp khi không sử dụng.

Hướng dẫn triển khai

Mọi người dùng cần được trang bị kiến thức về các yêu cầu và thủ tục an toàn thông tin trong việc bảo vệ thiết bị khi không sử dụng, cũng như trách nhiệm của họ trong việc thực hiện bảo vệ. Người dùng cần được tư vấn về:

a) đóng các phiên làm việc khi đã hoàn tất, trừ khi chúng có thể được bảo vệ an toàn bằng một cơ chế chặn thích hợp, ví dụ trình bảo vệ màn hình được bảo vệ bằng mật khẩu;

b) thoát các máy tính lớn, các máy chủ, và các máy tính văn phòng khi buổi làm việc kết thúc (nghĩa là không chỉ tắt màn hình hay thiết bị đầu cuối);

c) khi không sử dụng thì cần bảo vệ an toàn cho các máy tính PC hay thiết bị đầu cuối khỏi việc sử dụng trái phép bằng một khóa có chìa hoặc một biện pháp bảo vệ tương đương, ví dụ như: truy cập qua mật khẩu (xem thêm 10.3.3).

Thông tin khác

Thiết bị được lắp đặt trong phạm vi của người dùng, ví dụ các máy trạm hoặc các máy chủ tệp tin, có thể yêu cầu bảo vệ riêng trước sự truy cập trái phép khi không được dùng tới trong thời gian dài.

10.3.3 Chính sách màn hình sạch và bàn làm việc sạch

Biện pháp quản lý

Chính sách bàn làm việc sạch không có giấy và các phương tiện lưu trữ di động và chính sách màn hình sạch cho các phương tiện xử lý thông tin phải được thực hiện.

Hướng dẫn triển khai

Chính sách màn hình sạch và bàn làm việc sạch cần lưu ý đến việc phân loại thông tin (xem 6.2), các yêu cầu pháp lý và yêu cầu hợp đồng (xem 14.1), các rủi ro tương ứng và các khía cạnh văn hóa của việc tổ chức. Những hướng dẫn sau đây cần được quan tâm:

a) thông tin nghiệp vụ quan trọng hoặc nhạy cảm, ví dụ trên giấy tờ hay trên các thiết bị lưu trữ điện tử, cần được khóa lại (lý tưởng là được giữ trong két sắt, tủ hoặc các phương tiện an toàn khác) khi không cần dùng tới, đặc biệt là khi phòng làm việc bị bỏ trống;

b) máy tính và các thiết bị đầu cuối cần được thoát hoặc được bảo vệ bằng màn hình bảo vệ hoặc cơ chế khóa bàn phím bằng mật khẩu, thẻ hoặc cơ chế xác thực người dùng tương tự khi không sử dụng nữa;

c) các đầu mối thư đến và đi và các máy fax khi không sử dụng cũng cần được bảo vệ;

d) việc sử dụng trái phép các máy chụp và các kỹ thuật sao chép khác (ví dụ các máy quét, máy ảnh kỹ thuật số) phải được ngăn chặn;

e) các tài liệu chứa thông tin nhạy cảm hay thông tin đã được phân loại cần được lấy khỏi máy in ngay lập tức.

Thông tin khác

Chính sách màn hình/bàn làm việc sạch sẽ giảm thiểu các rủi ro do truy cập trái phép, mất cắp, và hư hại thông tin trong và ngoài giờ làm việc. Các két sắt hay các phương tiện chứa an toàn khác cũng có thể bảo vệ thông tin trước các thảm họa như cháy nổ, động đất, lụt lội.

Cần quan tâm sử dụng các máy in có chức năng mã khóa, khi đó chỉ những người đã tạo mã mới có thể vận hành máy.

10.4 Quản lý truy cập mạng

Mục tiêu: Nhằm ngăn chặn truy cập trái phép tới các dịch vụ mạng.

Truy cập tới các dịch vụ kết nối mạng trong nội bộ hay ra bên ngoài mạng đều cần được quản lý.

Truy cập của người dùng tới các mạng và các dịch vụ mạng không được làm tổn hại đến sự an toàn của các dịch vụ mạng nếu bảo đảm:

a) các giao diện phù hợp giữa mạng của tổ chức và các mạng thuộc sở hữu của các tổ chức khác, và các mạng công cộng;

b) các cơ chế xác thực phù hợp được áp dụng cho mọi người dùng và thiết bị;

c) quản lý truy cập người dùng tới các dịch vụ thông tin là yêu cầu bắt buộc.

10.4.1 Chính sách sử dụng các dịch vụ mạng

Biện pháp quản lý

Người dùng chỉ được cung cấp quyền truy cập đến các dịch vụ mà họ đã được cho phép.

Hướng dẫn triển khai

Cần xây dựng chính sách về sử dụng mạng và các dịch vụ mạng. Chính sách này cần bao hàm:

a) các mạng và dịch vụ mạng đã được cho phép truy cập;

b) các thủ tục cấp phép nhằm xác định ai đã được phép truy cập tới các mạng và dịch vụ mạng nào;

c) các thủ tục và các biện pháp quản lý nhằm bảo vệ truy cập tới các kết nối mạng và dịch vụ mạng;

d) các phương thức được sử dụng để truy cập tới các mạng và dịch vụ mạng (ví dụ các điều kiện để cho phép truy cập bằng quay số tới một nhà cung cấp Internet hoặc hệ thống từ xa).

Chính sách về việc sử dụng các dịch vụ mạng cần phù hợp với chính sách quản lý truy cập nghiệp vụ (xem 10.1).

Thông tin khác

Các kết nối trái phép và không an toàn tới các dịch vụ mạng có thể ảnh hưởng tới toàn bộ tổ chức. Biện pháp quản lý này đặc biệt quan trọng cho các kết nối mạng tới các ứng dụng nghiệp vụ quan trọng hoặc nhạy cảm hoặc tới người dùng ở các vị trí có mức rủi ro cao, ví dụ như các khu vực bên ngoài hay khu vực công cộng mà nằm ngoài sự kiểm soát và quản lý an toàn của tổ chức.

10.4.2 Xác thực người dùng cho các kết nối bên ngoài

Biện pháp quản lý

Các biện pháp xác thực thích hợp cần được sử dụng để quản lý truy cập bởi các người dùng từ xa.

Hướng dẫn triển khai

Việc xác thực người dùng từ xa có thể được được thực hiện bằng, ví dụ, kỹ thuật mật mã, thẻ bài cứng, hoặc một giao thức thách thức/đáp ứng. Một số hình thức triển khai của các kỹ thuật như vậy có thể tìm thấy trong giải pháp mạng riêng ảo (VPN). Có thể sử dụng các đường truyền riêng chuyên dụng để đảm bảo nguồn của các kết nối.

Các thủ tục và các biện pháp quản lý quay số lại, ví dụ sử dụng các modem quay số lại, có thể cung cấp bảo vệ chống lại các kết nối trái phép và không mong muốn tới các phương tiện xử lý thông tin của tổ chức. Biện pháp quản lý này sẽ xác thực những người dùng đang cố gắng thiết lập kết nối đến mạng của tổ chức từ các vị trí xa. Khi sử dụng biện pháp quản lý này, tổ chức không nên sử dụng các dịch vụ mạng bao gồm cả chuyển tiếp cuộc gọi, hoặc nếu họ có sử dụng thì họ cần khóa các tính năng đó để tránh những điểm yếu liên quan đến chuyển tiếp cuộc gọi. Thủ tục gọi lại cần đảm bảo rằng hiện

phía tổ chức đã ngắt kết nối. Nếu không, người dùng ở xa có thể giữ đường kết nối mở giả như việc kiểm tra đối với cuộc gọi về đã được thực hiện. Các thủ tục và các biện pháp quản lý cuộc gọi lại cần được kiểm tra kỹ khả năng này.

Xác thực nút có thể đóng vai trò như một biện pháp khác thay thế xác thực nhóm những người dùng từ xa có kết nối tới một thiết bị máy tính dùng chung và an toàn. Các kỹ thuật mật mã, ví dụ dựa trên các chứng nhận máy móc, có thể được sử dụng để xác thực nút. Đây là một bộ phận của một số giải pháp dựa trên VPN.

Cần triển khai thêm các biện pháp quản lý bằng xác thực để quản lý truy cập tới các mạng không dây. Đặc biệt, cần quan tâm đặc biệt đến việc lựa chọn các biện pháp quản lý các mạng không dây vì chúng có nhiều khả năng bị xâm phạm và chèn thêm lưu lượng mạng mà không bị phát hiện.

Thông tin khác

Các kết nối bên ngoài tiềm tàng sự truy cập trái phép tới thông tin nghiệp vụ, ví dụ truy cập bằng các phương pháp quay số. Có nhiều phương pháp xác thực khác nhau, một số trong số chúng có mức bảo vệ cao hơn so với những phương pháp khác, ví dụ: phương pháp dựa trên các kỹ thuật mật mã có thể đạt được hiệu quả xác thực mạnh. Việc xác định mức độ bảo vệ qua đánh giá rủi ro là rất quan trọng. Điều này rất cần để có thể lựa chọn được một phương thức xác thực phù hợp.

Một phương tiện hỗ trợ kết nối tự động đến một máy tính từ xa cũng có thể là một cách để có thể có được truy cập trái phép tới một ứng dụng nghệp vụ. Và càng đặc biệt quan trọng nếu kết nối sử dụng một mạng nằm ngoài sự quản lý của ban quản lý an toàn thông tin của tổ chức.

10.4.3 Định danh thiết bị trong các mạng

Biện pháp quản lý

Định dạng thiết bị tự động cần được xem xét như một biện pháp để xác thực các kết nối từ những vị trí và thiết bị cụ thể.

Hướng dẫn triển khai

Định danh thiết bị có thể được sử dụng nếu sự truyền thông chỉ có thể được khởi tạo từ một vị trí hoặc thiết bị cụ thể. Có thể sử dụng một bộ định danh tích hợp hoặc được gắn vào thiết bị để chỉ ra xem liệu thiết bị này có được phép kết nối tới mạng không. Những bộ định danh này cần chỉ rõ mạng mà thiết bị được phép kết nối tới nếu có nhiều mạng đang tồn tại và nhất là khi các mạng này có độ nhạy cảm khác nhau. Có thể cũng cần chú ý tới vấn đề bảo vệ vật lý của thiết bị nhằm duy trì sự an toàn cho bộ định danh thiết bị.

Thông tin khác

Biện pháp quản lý này có thể được sử dụng kết hợp với các kỹ thuật khác để xác thực người dùng thiết bị (xem 10.4.2).Ngoài ra, định danh thiết bị có thể cũng được áp dụng để hỗ trợ xác thực người dùng.

10.4.4 Chuẩn đoán từ xa và bảo vệ cổng cấu hình

Biện pháp quản lý

Các truy cập vật lý và logic tới các cổng dùng cho việc cấu hình và chuẩn đoán cần được kiểm soát.

Hướng dẫn triển khai

Các biện pháp quản lý tiềm năng đối với truy cập tới các cổng cấu hình và chuẩn đoán bao gồm sử dụng khóa có chìa và các thủ tục hỗ trợ kiểm soát truy cập vật lý tới cổng. Một ví dụ của các thủ tục hỗ trợ là đảm bảo rằng các cổng cấu hình và chuẩn đoán chỉ có thể được truy cập nếu có sự dàn xếp giữa người quản lý dịch vụ máy tính và nhân viên bảo trì phần cứng/phần mềm có yêu cầu truy cập.

Các cổng, dịch vụ, và các tính năng tương tự được cài đặt trên một máy tính hay thiết bị mạng mà không đặc biệt cần thiết cho chức năng nghiệp vụ, cần bị vô hiệu hóa hoặc loại bỏ.

Thông tin khác

Nhiều hệ thống máy tính, hệ thống mạng và hệ thống truyền thông được cài đặt tính năng chuẩn đoán hoặc cấu hình từ xa để các kỹ sư bảo dưỡng sử dụng. Nếu không được bảo vệ thì các cổng chuẩn đoán này cũng sẽ là một phương tiện truy cập trái phép.

10.4.5 Phân tách trên mạng

Biện pháp quản lý

Các nhóm người dùng, dịch vụ và hệ thống thông tin cần được phân tách trên các mạng.

Hướng dẫn triển khai

Một phương pháp kiểm soát an toàn cho các mạng lớn là phân tách chúng thành các vùng mạng logic, ví dụ các vùng mạng bên trong và các vùng mạng bên ngoài của tổ chức, mỗi vùng được bảo vệ bởi một vành đai an toàn xác định. Một bộ các biện pháp quản lý tăng tiến có thể được áp dụng trong các vùng mạng logic khác nhau để tiếp tục phân tách tiếp các môi trường an ninh mạng, ví dụ các hệ thống truy cập công cộng, các mạng nội bộ và các tài sản quan trọng. Các vùng cần được xác định dựa trên quá trình đánh giá rủi ro và các yêu cầu an toàn thông tin khác nhau trong từng lĩnh vực.

Một vành đai mạng như vậy có thể được triển khai khi cài đặt một cổng an toàn giữa hai mạng kết nối với nhau để quản lý truy cập và luồng thông tin giữa hai miền. Cổng an toàn này cần được cấu hình để lọc lưu lượng giữa các miền này (xem 10.4.6 và 10.4.7) và chặn truy cập trái phép theo quy định của chính sách quản lý truy cập của tổ chức (xem 10.1). Tường lửa là một ví dụ của cổng an toàn. Một phương pháp phân tách các miền logic khác là hạn chế truy cập mạng bằng cách sử dụng mạng riêng ảo cho các nhóm người dùng trong tổ chức.

Các mạng cũng có thể được phân tách nhờ tính năng của thiết bị mạng, ví dụ chuyển mạch IP. Khi đó các miền phân tách có thể được triển khai khi quản lý các luồng dữ liệu mạng bằng các năng lực định tuyến/chuyển mạch, ví dụ tính năng danh sách quản lý truy cập.

Tiêu chí phân tách mạng cần dựa trên chính sách quản lý truy cập và các yêu cầu truy cập (xem 9.1), và cũng cần xem xét chi phí tương đối và ảnh hưởng của định tuyến mạng hợp lý hoặc công nghệ cổng lên chất lượng mạng (xem 10.4.6 và 10.4.7).

Hơn nữa, việc phân tách mạng cũng cần dựa trên giá trị và sự phân loại thông tin được lưu trữ hoặc được xử lý trong mạng, các mức độ tin cậy hoặc các giới hạn nghiệp vụ để làm giảm ảnh hưởng tổng thể của việc phân tách dịch vụ.

Cần quan tâm đến việc phân tách các mạng không dây khỏi các mạng nội bộ và mạng cá nhân. Nếu không xác định được các vành đai mạng của mạng không dây thì cần thực hiện đánh giá rủi ro để xác định các biện pháp quản lý (ví dụ xác thực mạnh, các phương pháp mã hóa, và lựa chọn tần số) để duy trì sự phân tách mạng.

Thông tin khác

Mạng càng ngày càng có xu hướng mở rộng ra ngoài ranh giới của tổ chức, vì các quan hệ đối tác kinh doanh được hình thành có thể yêu cầu kết nối hoặc chia sẻ các phương tiện mạng và phương tiện xử lý thông tin. Các mạng mở rộng có thể làm tăng nguy cơ truy cập trái phép vào các hệ thống thông tin hiện đang sử dụng mạng, một số mạng mở rộng có thể đòi hỏi phải được bảo vệ trước những người dùng mạng khác vì tính chất quan trọng hay độ nhạy cảm của các mạng này.

10.4.6 Quản lý kết nối mạng

Biện pháp quản lý

Đối với các mạng chia sẻ, đặc biệt là các mạng mở rộng ra ngoài tổ chức, số người dùng có thể kết nối vào mạng phải được giới hạn, phù hợp với các chính sách quản lý truy cập và các yêu cầu trong ứng dụng nghiệp vụ (xem 10.1)

Hướng dẫn triển khai

Các quyền truy cập mạng của người dùng cần được duy trì và cập nhật theo yêu cầu của chính sách quản lý truy cập (xem 10.1).

Khả năng kết nối của người dùng cần được hạn chế thông qua các cổng mạng, cổng mạng này lọc lưu lượng bằng các luật hoặc các bảng đã xác định trước. Dưới đây là các ví dụ của các ứng dụng cần áp dụng hạn chế truy cập:

a) Thông điệp, ví dụ thư điện tử;

b) truyền tệp;

c) truy cập tương tác;

d) truy cập ứng dụng.

Cần quan tâm đến việc liên kết các quyền truy cập mạng vào các thời điểm nhất định trong ngày hoặc ngày.

Thông tin khác

Sự phối hợp các biện pháp quản lý nhằm hạn chế khả năng kết nối của người dùng có thể được yêu cầu bởi chính sách quản lý truy cập đối với các mạng chia sẻ, đặc biệt là những mạng mở rộng ra ngoài ranh giới của tổ chức.

10.4.7 Quản lý định tuyến mạng

Biện pháp quản lý

Quản lý định tuyến mạng cần được triển khai nhằm đảm bảo các kết nối máy tính và luồng thông tin không vi phạm chính sách quản lý truy cập của các ứng dụng nghiệp vụ.

Hướng dẫn triển khai

Các biện pháp quản lý việc định tuyến cần được dựa trên cơ chế kiểm tra địa chỉ nguồn và địa chỉ đích.

Các cổng bảo vệ cần được sử dụng nhằm xác nhận địa chỉ nguồn và địa chỉ đích tại các điểm quản lý bên trong và bên ngoài mạng nếu có các kỹ thuật chuyển đổi địa chỉ mạng và/hoặc máy trung gian được sử dụng. Những người thực hiện cần phải có sự hiểu biết về tính đầy đủ và sự thiết sót của bất kỳ cơ cấu nào được triển khai. Các yêu cầu đối với biện pháp quản lý định tuyến mạng cần dựa trên các chính sách quản lý truy cập (xem 10.1).

Thông tin khác

Các mạng có chia sẻ, đặc biệt là các mạng mở rộng ra ngoài ranh giới của tổ chức có thể yêu cầu thêm các biện pháp định tuyến. Điều này đặc biệt đúng với các mạng được chia sẻ với người dùng thuộc bên thứ ba (không thuộc tổ chức).

10.5 Quản lý truy cập hệ điều hành.

Mục tiêu: Nhằm ngăn ngừa việc truy cập trái phép tới hệ điều hành.

Các tiện ích bảo vệ cần được sử dụng để giới hạn truy cập tới hệ điều hành chỉ với những người dùng được phép. Các tiện ích này cần có những năng lực sau:

a) xác thực những người dùng đã được cấp phép, phù hợp với chính sách quản lý truy cập đã xác định;

b) ghi lại những nỗ lực xác thực hệ thống thành công và thất bại;

c) ghi lại việc sử dụng các đặc quyền của hệ thống ưu tiên;

d) đưa ra các cảnh báo khi chính sách an toàn hệ thống bị vi phạm;

e) cung cấp biện pháp xác thực thích hợp;

f) nếu thích hợp thì phải hạn chế thời gian kết nối của người dùng.

10.5.1 Các thủ tục đăng nhập an toàn

Biện pháp quản lý

Truy cập đến các hệ điều hành cần được kiểm soát bởi thủ tục đăng nhập an toàn.

Hướng dẫn triển khai

Thủ tục đăng nhập vào một hệ điều hành cần được thiết kế để tối giảm cơ hội truy cập trái phép. Vì vậy thủ tục đăng nhập cần tối giảm thông tin về hệ thống nhằm tránh phải cung cấp hỗ trợ không cần thiết cho những người dùng trái phép. Một thủ tục đăng nhập tốt cần:

a) không hiển thị những nhận dạng ứng dụng hoặc hệ thống cho tới khi quá trình đăng nhập đã được thiết lập thành công;

b) Hiển thị cảnh báo chung rằng chỉ những người dùng đã được cấp phép mới được truy cập vào máy tính;

c) không cung cấp những thông điệp giúp đỡ hỗ trợ người dùng trái phép trong thủ tục đăng nhập;

d) kiểm tra tính hợp lệ của thông tin đăng nhập chỉ khi đã hoàn tất tất cả các dữ liệu đầu vào. Nếu xuất hiện một điều kiện sai thì hệ thống không được chỉ ra phần dữ liệu đúng hoặc sai.

e) giới hạn số lần cố gắng đăng nhập không thành công được cho phép, ví dụ nhiều nhất là ba lần, và phải quan tâm tới việc:

   1) ghi lại những lần cố gắng đăng nhập thất bại và thành công;

   2) đưa ra khoảng thời gian trễ bắt buộc trước khi tiếp tục cố gắng đăng nhập tiếp hoặc từ chối các cố gắng đăng nhập tiếp mà không cần cấp phép;

   3) ngắt các kết nối liên kết dữ liệu;

   4) gửi một thông điệp cảnh báo tới bảng điều khiển hệ thống nếu số lần cố gắng đăng nhập tối đa đã hết;

   5) đặt số lần thử lại mật khẩu cùng với độ dài tối thiểu của mật khẩu và giá trị của hệ thống được bảo vệ;

f) giới hạn thời gian tối đa và tối thiểu được phép cho thủ tục đăng nhập. Nếu đã vượt qua thời gian này, hệ thông sẽ kết thúc việc đăng nhập;

g) Hiển thị thông tin dưới đây sau khi hoàn thành thủ tục đăng nhập:

   1) Ngày và giờ của lần đăng nhập thành công trước đó;

   2) Những chi tiết về các lần cố gắng đăng nhập không thành công kể từ lần đăng nhập thành công gần nhất;

h) không hiển thị mật khẩu đã được đưa vào hoặc cân nhắc tới việc ẩn các ký tự mật khẩu bằng các biểu tượng;

i) không truyền các mật khẩu dưới dạng ký tự rõ ràng trên mạng.

Thông tin khác

Nếu mật khẩu được truyền đi dưới dạng ký tự rõ ràng trong suốt quá trình đăng nhập trên mạng, chúng có thể bị bắt bởi chương trình "nghe lén" trên mạng.

10.5.2 Định danh và xác thực người dùng

Biện pháp quản lý

Tất cả những người dùng đều phải có một định danh duy nhất (định danh người dùng –User ID) để sử dụng riêng cho họ. Một kỹ thuật xác thực thích hợp cần được chọn nhằm chứng thực đặc điểm nhận dạng của người dùng.

Hướng dẫn triển khai

Biện pháp quản lý này cần được áp dụng cho tất cả các loại người dùng (bao gồm nhân viên hỗ trợ kỹ thuật, nhà điều hành, người quản trị mạng, người lập trình hệ thống, và người quản lý cơ sở dữ liệu).

Các ID của người dùng cần được sử dụng nhằm theo dõi các hoạt động cá nhân. Không được thực hiện những hoạt động của người dùng thông thường từ các tài khoản đặc quyền.

Trong những trường hợp ngoại lệ, khi có một lợi ích nghiệp vụ rõ ràng, có thể sử dụng một ID người dùng chia sẻ trong một nhóm người dùng hoặc một công việc nhất định. Sự thông qua của ban quản lý cần được ghi vào văn bản cho những trường hợp này. Các biện pháp quản lý bổ sung có thể được yêu cầu nhằm duy trì khả năng giải trình trách nhiệm.

Các ID chung được dung bởi cá nhân chỉ được cho phép nếu các chức năng đó dễ truy cập hoặc các hoạt động được thực hiện bởi ID đó không cần được theo dõi (ví dụ chỉ truy cập để đọc), hoặc nếu đã thực hiện các biện pháp quản lý (ví dụ mật khẩu cho ID chung chỉ được cấp cho một nhân viên tại một thời điểm).

Khi có yêu cầu xác thực mạnh và xác minh định danh thì các phương pháp xác thực thay thế mật khẩu, ví dụ các phương tiện mã hóa, thẻ thông minh, thẻ hoặc các phương tiện sinh trắc học hay mã thông báo, sẽ được sử dụng.

Thông tin khác

Các mật khẩu (xem 10.3.1 và 10.5.3) là cách rất phổ biến để cung cấp định danh và xác thực dựa trên một bí mật mà chỉ người dùng mới biết. Tương tự như vậy với các phương tiện mã hóa và các giao thức xác thực. Độ mạnh của định danh và xác thực phải phù hợp với độ nhạy cảm của thông tin được truy cập.

Các phương tiện khác như thẻ nhớ hoặc thẻ thông minh mà người dùng sở hữu cũng có thể được sử dụng để định danh và xác thực. Các kỹ thuật xác thực bằng sinh trắc học sử dụng các đặc điểm hoặc thuộc tính duy nhất của một cá nhân cũng có thể được sử dụng để xác thực nhận dạng cá nhân. Sự kết hợp của các kỹ thuật và các cơ chế một cách an toàn sẽ cho tính năng xác thực mạnh hơn.

10.5.3 Hệ thống quản lý mật khẩu

Biện pháp quản lý

Các hệ thống quản lý mật khẩu phải có khả năng tương tác và đảm bảo chất lượng của mật khẩu.

Hướng dẫn triển khai

Một hệ thống quản lý mật khẩu cần:

a) bắt buộc sử dụng các ID và mật khẩu cá nhân riêng để duy trì khả năng giải trình trách nhiệm;

b) cho phép người dùng chọn và thay đổi mật khẩu của họ và có thủ tục xác nhận để cho phép các lỗi đầu vào;

c) bắt buộc phải chọn các mật khẩu chất lượng (xem 10.3.1);

d) bắt buộc phải thay đổi mật khẩu (xem 10.3.1);

e) bắt buộc người dùng thay đổi các mật khẩu tạm thời ở lần đăng nhập đầu tiên (xem 10.2.3);

f) duy trì hồ sơ gồm các mật khẩu trước đó của người dùng và ngăn chặn việc sử dụng lại;

g) không hiển thị các mật khẩu trên màn hình khi nó đang được nhập vào hệ thống;

h) lưu trữ các tệp mật khẩu riêng với dữ liệu hệ thống ứng dụng;

i) lưu trữ và truyền mật khẩu theo dạng đã được bảo vệ (ví dụ ở dạng đã mã hóa hoặc hàm băm).

Thông tin khác

Mật khẩu là một trong những phương tiện cơ bản trong việc xác minh quyền của người dùng được phép truy cập tới một dịch vụ máy tính.

Một vài ứng dụng yêu cầu mật khẩu người dùng phải được ấn định bởi một cơ quan có thẩm quyền độc lập; trong trường hợp này, điểm b), d) và e) của hướng dẫn trên đây không được áp dụng. Trong hầu hết các trường hợp mật khẩu được lựa chọn và duy trì bởi người dùng. Xem phần 10.3.1 hướng dẫn về sử dụng mật khẩu.

10.5.4 Sử dụng các tiện ích hệ thống

Biện pháp quản lý

Việc sử dụng các chương trình tiện ích có khả năng ảnh hưởng đến việc quản lý hệ thống và các chương trình ứng dụng khác phải được giới hạn và kiểm soát chặt chẽ.

Hướng dẫn triển khai

Những hướng dẫn sau đây về việc sử dụng các tiện ích hệ thống cần được quan tâm:

a) sử dụng các thủ tục định danh, thẩm định và cấp phép cho các tiện ích của hệ thống;

b) phân tách các tiện ích hệ thống khỏi các ứng dụng phần mềm;

c) giới hạn sử dụng các tiện ích hệ thống chỉ trong một số lượng nhỏ nhất những người dùng tin cậy và đã được cấp phép (xem 10.2.2);

d) cấp phép sử dụng đặc biệt các tiện ích hệ thống;

e) giới hạn sự sẵn sàng của các tiện ích hệ thống, ví dụ trong khoảng thời gian có một sự thay đổi đã được cấp phép;

f) ghi lại tất cả các lần sử dụng các tiện ích hệ thống;

g) xác định và ghi vào văn bản các mức cấp phép cho các tiện ích hệ thống;

h) loại bỏ hoặc vô hiệu hóa tất cả các phần mềm hệ thống và các tiện ích dựa trên phần mềm không cần thiết;

i) không để các tiện ích hệ thống sẵn sàng cho những người dùng có truy cập vào các ứng dụng trên các hệ thống có yêu cầu phân tách nhiệm vụ.

Thông tin khác

Hầu hết các máy tính đều cài đặt một hoặc nhiều chương trình tiện ích có khả năng ảnh hưởng đến hệ thống và các biện pháp quản lý ứng dụng.

10.5.5 Thời gian giới hạn của phiên làm việc

Biện pháp quản lý

Các phiên làm việc không hoạt động cần được đóng lại sau một giới hạn thời gian không hoạt động xác định.

Hướng dẫn triển khai

Chức năng tạm ngừng phải xóa màn hình của phiên và nếu có thể thì sau đó phải đóng ứng dụng và các phiên làm việc của mạng sau một giới hạn thời gian không hoạt động xác định. Khoảng thời gian tạm ngừng cần phản ánh những rủi ro an toàn của khu vực đó, phân loại thông tin đang được xử lý và các ứng dụng hiện đang sử dụng, và các rủi ro liên quan tới người dùng thiết bị.

Một vài hệ thống lại được cung cấp chức năng tạm ngừng giới hạn, chức năng này xóa màn hình và ngăn chặn truy cập trái phép nhưng không đóng hẳn các phiên làm việc của ứng dụng hay mạng.

Thông tin khác

Biện pháp quản lý này đặc biệt quan trọng trong những vị trí có độ rủi ro cao, bao gồm những khu vực công cộng hoặc nằm ngoài sự quản lý an toàn của tổ chức. Các phiên làm việc cần được đóng lại để ngăn chặn truy cập trái phép và chặn các cuộc tấn công dịch vụ.

10.5.6 Giới hạn thời gian kết nối

Biện pháp quản lý

Cần hạn chế thời gian kết nối để làm tăng độ an toàn cho các ứng dụng có mức rủi ro cao.

Hướng dẫn triển khai

Biện pháp quản lý thời gian kết nối cần được quan tâm cho các ứng dụng máy tính nhạy cảm, đặc biệt ở các vị trí có độ rủi ro cao, ví dụ các khu vực công cộng hoặc các khu vực nằm ngoài phạm vi quản lý an toàn của tổ chức. Dưới đây là các ví dụ về biện pháp quản lý hạn chế thời gian kết nối:

a) sử dụng những khe thời gian đã được xác định trước, ví dụ cho việc truyền tệp tin, hoặc các phiên làm việc tương tác thường xuyên có thời gian ngắn;

b) hạn chế thời gian kết nối chỉ trong giờ làm việc bình thường nếu không có yêu cầu làm thêm giờ hay làm ngoài giờ;

c) xem xét xác thực lại vào những thời điểm đã định.

Thông tin khác

Việc hạn chế thời gian kết nối tới các dịch vụ máy tính sẽ làm giảm cơ hội cho truy cập trái phép. Việc hạn chế thời gian của phiên làm việc sẽ ngăn chặn người dùng giữ các phiên mở để tránh phải xác thực lại.

10.6 Điều khiển truy cập thông tin và ứng dụng

Mục tiêu: Nhằm ngăn chặn các truy cập trái phép đến thông tin lưu trong các hệ thống ứng dụng.

Các tiện ích an toàn cần được sử dụng để hạn chế truy cập tới và trong các hệ thống ứng dụng.

Truy cập logic tới thông tin và phần mềm ứng dụng cần được hạn chế chỉ với những người dùng đã được cấp phép. Các hệ thống ứng dụng cần:

a) kiểm soát truy cập người dùng tới các chức năng hệ thống ứng dụng và thông tin, phù hợp với chính sách quản lý truy cập đã xác định;

b) cung cấp bảo vệ khỏi sự truy cập trái phép bởi các thực thể, phần mềm hệ điều hành, và phần mềm độc hại có khả năng làm ảnh hưởng đến hệ thống hoặc các biện pháp quản lý ứng dụng;

c) không làm tổn hại tới các hệ thống có chia sẻ nguồn thông tin khác.

10.6.1 Hạn chế truy cập thông tin.

Biện pháp quản lý

Truy cập của người dùng và nhân viên hỗ trợ tới thông tin và các chức năng của hệ thống ứng dụng cần được hạn chế phù hợp với chính sách quản lý truy cập đã xác định.

Hướng dẫn triển khai

Những hạn chế truy cập cần dựa trên các yêu cầu ứng dụng nghiệp vụ cụ thể. Chính sách quản lý truy cập cũng cần phù hợp với chính sách truy cập của tổ chức (xem 10.1).

Cần xem xét áp dụng các hướng dẫn sau nhằm hỗ trợ các yêu cầu hạn chế truy cập:

a) cung cấp các lựa chọn quản lý truy cập tới các chức năng hệ thống ứng dụng;

b) quản lý các quyền truy cập của người dùng, ví dụ. đọc, viết, xóa và thực thi;

c) quản lý các quyền truy cập của các ứng dụng khác;

d) đảm bảo rằng đầu ra của hệ thống ứng dụng xử lý thông tin nhạy cảm chỉ gồm thông tin liên quan tới việc sử dụng đầu ra và chỉ được gửi tới các vị trí hay thiết bị đầu cuối đã được phép; cần bao gồm việc soát xét định kỳ các đầu ra nhằm đảm bảo rằng thông tin thừa đều bị loại bỏ.

10.6.2 Cách ly hệ thống nhạy cảm

Biện pháp quản lý

Các hệ thống nhạy cảm cần có môi trường máy tính cách ly.

Hướng dẫn triển khai

Cần quan tâm đến các điểm sau đây trong việc cách ly hệ thống nhạy cảm:

a) độ nhạy cảm của hệ thống ứng dụng cần được người sở hữu ứng dụng xác định rõ và lập thành văn bản (xem 6.1.2);

b) nếu một ứng dụng nhạy cảm sẽ hoạt động trong môi trường chia sẻ thì các hệ thống ứng dụng có chia sẻ các nguồn tài nguyên với ứng dụng đó và những rủi ro liên quan cần được xác định và được chấp nhận bởi người sở hữu ứng dụng nhạy cảm đó.

Thông tin khác

Một số hệ thống ứng dụng rất nhạy cảm với sự mất mát tiềm ẩn, do vậy chúng đòi hỏi phải được xử lý đặc biệt.

Độ nhạy cảm có thể cho thấy rằng hệ thống ứng dụng đó:

a) cần hoạt động trên một máy tính chuyên dụng; hoặc

b) chỉ chia sẻ tài nguyên với các hệ thống ứng dụng đáng tin cậy.

Sự cách ly có thể đạt được bằng các phương pháp logic và vật lý (xem thêm 10.4.5).

10.7Tính toán di động và làm việc từ xa

Mục tiêu: Nhằm đảm bảo an toàn thông tin khi sử dụng các phương tiện tính toán di động và làm việc từ xa.

Sự bảo vệ được yêu cầu phải tương xứng với các rủi ro mà các cách làm việc đặc biệt này gây nên. Khi sử dụng tính toán di động thì phải quan tâm đến các rủi ro do làm việc trong môi trường không được bảo vệ và áp dụng biện pháp bảo vệ thích hợp. Trong trường hợp làm việc từ xa, tổ chức phải áp dụng bảo vệ với địa điểm làm việc và đảm bảo đã thực hiện các phương thức bảo vệ phù hợp cho cách làm việc này.

10.7.1 Tính toán và truyền thông qua thiết bị di động

Biện pháp kiểm soát

Một chính sách chính thức cần được chuẩn bị và các biện pháp an toàn thông tin thích hợp cần được chấp nhận nhằm bảo vệ khỏi các rủi ro khi sử dụng tính toán và truyền thông di động.

Hướng dẫn triển khai

Khi sử dụng các thiết bị tính toán và truyền thông di động, ví dụ sổ ghi chép, máy tính xách tay, thẻ thông minh, và điện thoại di động, cần quan tâm đặc biệt đến chúng nhằm đảm bảo rằng thông tin nghiệp vụ không bị tổn hại. Chính sách về việc tính toán qua thiết bị di động cần quan tâm đến những rủi ro do làm việc với thiết bị tính toán di động trong những môi trường không được bảo vệ.

Chính sách về việc tính toán qua thiết bị di động cần bao gồm các yêu cầu cho các biện pháp quản lý truy cập, bảo vệ vật lý, các kỹ thuật mã hóa, các bản sao lưu, và việc bảo vệ chống vi rút. Chính sách này cũng cần bao gồm các quy tắc và hướng dẫn kết nối các thiết bị di động tới các mạng và hướng dẫn sử dụng các thiết bị này tại nơi công cộng.

Cũng cần quan tâm khi sử dụng các thiết bị tính toán di động ở những nơi công cộng, phòng họp và các khu vực không được bảo vệ khác nằm ngoài trụ sở của tổ chức. Việc bảo vệ nên phù hợp để tránh truy nhập trái phép tới hoặc tiết lộ thông tin được lưu trữ và được xử lý bởi các thiết bị này, ví dụ sử dụng kỹ thuật mật mã (xem 11.3).

Người sử dụng các thiết bị tính toán di động tại những nơi công cộng nên lưu ý đến việc tránh rủi ro do những cá nhân không được phép. Các thủ tục chống lại các phần mềm độc hại cần sẵn sàng và được cập nhật (xem 9.4).

Cần định kỳ sao chép lại các thông tin nghiệp vụ quan trọng. Thiết bị cần sẵn sàng để cho phép sao lưu thông tin nhanh chóng và dễ dàng. Các bản sao lưu này cần được bảo vệ phù hợp chống lại, ví dụ sự đánh cắp hay mất mát thông tin.

Việc sử dụng các thiết bị di động được kết nối mạng cũng cần được bảo vệ phù hợp. Truy cập từ xa qua mạng công cộng tới thông tin nghiệp vụ bằng các thiết bị tính toán di động chỉ được thực hiện sau khi nhận dạng và xác thực thành công, và có áp dụng các cơ chế quản lý truy nhập phù hợp (xem 10.4).

Các thiết bị tính toán di động cũng phải được bảo vệ vật lý chống lại trộm cắp đặc biệt khi được để, ví dụ, trong ô tô hoặc các phương tiện vận tải khác, phòng khách sạn, trung tâm hội nghị, và các nơi hội họp. Một thủ tục cụ thể về các yêu cầu pháp lý, bảo hiểm và các yêu cầu an toàn khác của tổ chức cần được thiết lập đối với những trường hợp bị mất cắp hoặc làm mất thiết bị tính toán di động. Thiết bị mang thông tin nghiệp vụ quan trọng, nhạy cảm, và/hoặc trọng yếu không được để tự do, và nếu có thể phải được để ở nơi có khóa, hoặc sử dụng các loại khóa đặc biệt để bảo vệ thiết bị (xem 8.2.5).

Cần thu xếp đào tạo các nhân viên sử dụng tính toán di động để làm tăng nhận thức của họ về những rủi ro của cách làm việc này và triển khai các biện pháp quản lý.

Thông tin khác

Các kết nối không dây trong mạng di động cũng tương tự như các dạng kết nối mạng khác, nhưng có các điểm khác biệt quan trọng cần được lưu ý khi xác định các biện pháp quản lý. Các điểm khác biệt gồm:

a) một số giao thức an toàn trong mạng không dây vẫn chưa hoàn thiện và được coi là các điểm yếu;

b) thông tin lưu trữ trên các máy tính di động có thể không được sao lưu do băng tần mạng hạn chế và/hoặc do thiết bị di động có thể không được kết nối tại các những thời điểm đã được lập lịch để thực hiện sao lưu.

10.7.2 Làm việc từ xa

Biện pháp kiểm soát

Một chính sách, các kế hoạch điều hành và các thủ tục cần được phát triển và triển khai cho các hoạt động làm việc từ xa.

Hướng dẫn triển khai

Các tổ chức chỉ được cấp phép cho các hoạt động làm việc từ xa nếu chúng thỏa mãn các điều kiện sau: đã triển khai công tác chuẩn bị và các biện pháp quản lý an toàn phù hợp, công tác chuẩn bị và các biện pháp quản lý an toàn này đã tuân thủ các chính sách an toàn của tổ chức.

Cần thực thi bảo vệ thích hợp ở vị trí làm việc từ xa nhằm chống lại, ví dụ, sự mất cắp thiết bị và thông tin, tiết lộ thông tin trái phép, truy cập từ xa trái phép đến các hệ thống bên trong tổ chức hoặc lạm dụng các thiết bị. Các hoạt động làm việc từ xa cần được ban quản lý cho phép và quản lý, và cũng cần đảm bảo rằng những chuẩn bị phù hợp đã được thực hiện cho cách làm việc này.

Những vấn đề sau cần được quan tâm:

a) sự an toàn mức vật lý hiện tại của vị trí làm việc từ xa, trong đó cần lưu ý đến sự an toàn vật lý của các tòa nhà và môi trường bên trong;

b) môi trường vật lý dự kiến cho hoạt động làm việc từ xa;

c) các yêu cầu an toàn truyền thông, trong đó cần lưu ý nhu cầu truy cập từ xa tới các hệ thống bên trong tổ chức, thông tin nhạy cảm sẽ được truy cập và đi qua liên kết truyền thông và sự nhạy cảm của hệ thống bên trong;

d) mối đe dọa từ việc truy cập trái phép tới thông tin hoặc các nguồn tài nguyên từ những người sống cùng khác, ví dụ gia đình và bạn bè;

e) việc sử dụng các mạng gia đình, các yêu cầu hoặc các hạn chế đối với việc cấu hình các dịch vụ mạng không dây;

f) các chính sách và thủ tục phòng ngừa tranh chấp liên quan đến các quyền sở hữu trí tuệ được phát triển trên thiết bị thuộc sở hữu cá nhân;

g) truy nhập tới thiết bị thuộc sở hữu cá nhân (để kiểm tra sự an toàn của thiết bị hoặc khi điều tra), loại truy cập này có thể được ngăn chặn bằng quy định pháp lý;

h) những thỏa thuận đăng ký bản quyền phần mềm quy định trách nhiệm pháp lý của tổ chức trong việc đăng ký bản quyền phần mềm khách trên các máy trạm thuộc sở hữu của các nhân viên, người của các nhà thầu hoặc bên thứ ba;

i) các yêu cầu bảo vệ chống virut và tường lửa.

Các hướng dẫn và bố trí sau cần được quan tâm:

a) cung cấp trang bị lưu trữ và thiết bị phù hợp cho các hoạt động làm việc từ xa nếu việc sử dụng thiết bị thuộc sở hữu cá nhân không chịu sự quản lý của tổ chức là không được phép;

b) xác định công việc được phép, giờ làm việc, phân loại thông tin có thể được lấy, và các hệ thống bên trong và dịch vụ mà người làm việc từ xa được phép truy cập;

c) cung cấp thiết bị truyền thông phù hợp, gồm các phương pháp đảm bảo an toàn cho việc truy cập từ xa;

d) đảm bảo an toàn mức vật lý;

e) các quy tắc và hướng dẫn cho gia đình và khách truy cập tới thiết bị và thông tin;

f) cung cấp hỗ trợ và bảo trì phần cứng và phần mềm;

g) cung cấp các hợp đồng bảo hiểm;

h) các thủ tục sao lưu và đảm bảo sự liên tục của hoạt động nghiệp vụ;

i) đánh giá và giám sát an toàn;

j) thu hồi các cấp phép và quyền truy cập, và hoàn trả thiết bị khi chấm dứt các hoạt động làm việc từ xa.

Thông tin khác

Làm việc từ xa sử dụng công nghệ truyền thông để cho phép các cá nhân làm việc từ xa từ một vị trí cố định bên ngoài tổ chức của họ.

11 Tiếp nhận, phát triển và duy trì các hệ thống thông tin

11.1Yêu cầu đảm bảo an toàn cho các hệ thống thông tin

Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin là một phần không thể thiếu của các hệ thống thông tin.

Các hệ thống thông tin bao gồm hệ điều hành, cơ sở hạ tầng, các ứng dụng nghiệp vụ, các sản phẩm mua có sẵn, các dịch vụ và các ứng dụng do người dùng phát triển. Việc thiết kế và triển khai của hệ thống thông tin để hỗ trợ quá trình nghiệp vụ quyết định đến sự an toàn thông tin. Các yêu cầu an toàn cần được xác định và chấp thuận trước khi phát triển và/hoặc triển khai các hệ thống thông tin.

Tất cả các yêu cầu an toàn cần được xác định tại giai đoạn xác định yêu cầu của một dự án và được điều chỉnh, chấp thuận và được ghi vào văn bản như một phần của toàn bộ tình huống nghiệp vụ cho một hệ thống thông tin.

11.1.1 Phân tích và đặc tả các yêu cầu về an toàn

Biện pháp quản lý

Các thông báo về yêu cầu nghiệp vụ đối với các hệ thống thông tin mới hoặc được cải tiến từ các hệ thống thông tin có sẵn cần chỉ rõ các yêu cầu về biện pháp quản lý an toàn thông tin.

Hướng dẫn triển khai

Việc xác định các yêu cầu cho các biện pháp quản lý cần quan tâm tới các biện pháp quản lý tự động được phối hợp trong hệ thống thông tin, và nhu cầu hỗ trợ các biện pháp quản lý thủ công. Cần lưu ý tương tự khi đánh giá các gói phần mềm, dù là dạng được phát triển hay được mua, cho các ứng dụng nghiệp vụ.

Các yêu cầu và biện pháp quản lý an toàn cần phản ánh giá trị nghiệp vụ của các tài sản thông tin liên quan (xem 6.2) và những thiệt hại nghiệp vụ tiềm ẩn có thể xảy ra do lỗi hoặc do sự thiếu an toàn.

Các yêu cầu hệ thống về an toàn thông tin và các quy trình triển khai an toàn cần được tích hợp trong các giai đoạn trước của các dự án hệ thống thông tin. Việc triển khai và duy trì các biện pháp quản lý ở giai đoạn thiết kế thường rẻ hơn nhiều so với triển khai và duy trì trong hoặc sau khi triển khai.

Nếu sản phẩm được mua thì cần tuân theo quy trình kiểm tra và tiếp nhận chính thức. Các hợp đồng với nhà cung cấp cần tập trung vào các yêu cầu an toàn đã xác định. Nếu các chức năng an toàn trong một sản phẩm không đáp ứng các yêu cầu quy định thì cần xem xét các biện pháp quản lý rủi ro liên quan trước khi mua sản phẩm. Trong trường hợp có cung cấp thêm tính năng và gây ra rủi ro an toàn thì tính năng này cần được vô hiệu hóa hoặc cơ cấu kiểm soát đã được đề xuất cần được soát xét lại để xác định xem liệu có nên loại bỏ tính năng cải tiến này không.

Thông tin khác

Nếu được quan tâm thích hợp, ví dụ vì các lý do giá cả, ban quản lý có thể mong muốn sử dụng các sản phẩm đã được chứng nhận và được đánh giá một cách độc lập. Thông tin chi tiết hơn về chỉ tiêu

đánh giá các sản phẩm an toàn IT có thể tìm thấy trong ISO/IEC 15408 hoặc các tiêu chuẩn đánh giá hoặc chứng nhận khác.

ISO/IEC TR 13335-3 đưa ra hướng dẫn sử dụng các quy trình quản lý rủi ro nhằm xác định các yêu cầu đối với các biện pháp quản lý rủi ro.

11.2Xử lý đúng trong các ứng dụng

Mục tiêu: Nhằm ngăn ngừa các lỗi, mất mát, sửa đổi hoặc sử dụng trái phép thông tin trong các ứng dụng.
Các biện pháp quản lý thích hợp cần được thiết kế vào các ứng dụng, bao gồm cả các ứng dụng được người dùng phát triển để đảm bảo việc xử lý chính xác. Các biện pháp quản lý này cần bao gồm xác nhận dữ liệu đầu vào, xử lý nội bộ và xuất ra dữ liệu.
Các biện pháp quản lý bổ sung có thể được yêu cầu đối với các hệ thống xử lý hoặc có ảnh hưởng đến thông tin nhạy cảm, có giá trị hoặc quan trọng. Các biện pháp quản lý như vậy phải được xác định trên cơ sở các yêu cầu an toàn và đánh giá rủi ro.

11.2.1 Kiểm tra tính hợp lệ của dữ liệu đầu vào

Biện pháp quản lý

Dữ liệu nhập vào các ứng dụng cần được kiểm tra tính hợp lệ nhằm đảm bảo các dữ liệu này là chính xác và thích hợp.

Hướng dẫn triển khai

Việc kiểm tra cần được áp dụng cho thông tin đầu vào của các giao dịch nghiệp vụ, dữ liệu hiện tại (ví dụ, tên và địa chỉ, hạn mức tín dụng, số tham chiếu khách hàng), và các bảng tham số (ví dụ giá bán, tỷ giá chuyển đổi tiền tệ, mức thuế suất). Các hướng dẫn sau đây cần được xem xét:

a) kiểm tra ngẫu nhiên dữ liệu đầu vào hoặc sử dụng các hình thức kiểm tra dữ liệu đầu vào khác, ví dụ kiểm tra biên hoặc giới hạn các trường vào các dải dữ liệu đầu vào nhất định, để phát hiện các lỗi sau:
   1) các giá trị ngoài vùng;
   2) những ký tự không hợp lệ trong trường dữ liệu;
   3) dữ liệu lỗi hoặc không đầy đủ;
   4) vượt quá giới hạn độ lớn dữ liệu lớn nhất và thấp nhấp;
   5) dữ liệu quản lý trái phép hoặc không nhất quán;
b) soát xét định kỳ nội dung các trường chính hoặc các tệp dữ liệu nhằm xác nhận tính toàn vẹn và hợp lệ của chúng;

c) kiểm tra các tài liệu đầu vào dạng in sẵn để tìm những thay đổi trái phép (tất cả những thay đổi đối với tài liệu đầu vào đều phải được cho phép);

d) *các thủ tục cho việc xử lý các lỗi vi phạm tính hợp lệ;*

e) các thủ tục cho việc kiểm tra tính hợp lệ của dữ liệu đầu vào;

f) xác định trách nhiệm của toàn bộ những cá nhân liên quan trong quá trình xử lý dữ liệu đầu vào;

g) ghi vào nhật ký các hoạt động liên quan đến quá trình xử lý dữ liệu đầu vào (xem 9.10.1).

Thông tin khác

Nếu có thể thì cần xem xét kiểm tra và xác nhận tính hợp lệ của dữ liệu đầu vào một cách tự động nhằm giảm thiểu rủi ro của các lỗi và nhằm ngăn chặn các tấn công chuẩn bao gồm cả tấn công làm tràn bộ đệm và chèn mã.

11.2.2 Kiểm soát việc xử lý nội bộ

Biện pháp quản lý

Việc kiểm tra tính hợp lệ cần được tích hợp trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi có chủ ý.

Hướng dẫn triển khai

Việc thiết kế và triển khai các ứng dụng cần đảm bảo rằng các rủi ro do các lỗi xử lý gây ra sự mất tính toàn vẹn đều được giảm thiểu. Các vấn đề cần được quan tâm gồm:

a) sử dụng các chức năng chèn, sửa và xóa để thực hiện thay đổi dữ liệu;

b) các thủ tục nhằm ngăn ngừa chương trình chạy sai hoặc chạy sau lỗi của lần xử lý trước (xem thêm 9.1.1);

c) sử dụng các chương trình thích hợp để phục hồi sau lỗi nhằm đảm bảo việc xử lý dữ liệu chính xác;

d) bảo vệ chống lại những tấn công làm tràn/vượt quá dung lượng bộ đệm.

Một danh sách kiểm tra thích hợp cần được chuẩn bị, các hoạt động kiểm tra được ghi vào tài liệu, và các kết quả cần được cất giữ an toàn. Dưới đây là các ví dụ về các đối tượng cần kiểm tra:

a) các biện pháp quản lý theo phiên hoặc lô, nhằm điều hòa các chênh lệch của tệp dữ liệu sau các cập nhật;

b) cân nhắc các biện pháp quản lý, nhằm kiểm tra các chênh lệch đầu phiên so với các chênh lệch cuối phiên, cụ thể là:

   1) các biện pháp quản lý hoạt động – tới – hoạt động;

   2) tổng số cập nhật tệp tin;

3) các biện pháp quản lý chương trình – tới – chương trình;

c) kiểm tra tính hợp lệ của dữ liệu đầu vào mà hệ thống tạo ra (xem 11.2.1);

d) kiểm tra tính toàn vẹn, tính xác thực hay các thuộc tính an toàn khác của dữ liệu hoặc phần mềm được tải về, hoặc tải lên, giữa các máy tính trung tâm và các máy tính ở xa;

e) tổng số hàm băm của các tệp tin và hồ sơ;

f) kiểm tra nhằm đảm bảo rằng các chương trình đang chạy với đồng hồ đúng;

g) kiểm tra nhằm đảm bảo rằng các chương trình đang chạy theo đúng lệnh và kết thúc trong trường hợp có lỗi, và tạm dừng xử lý cho tới khi vấn đề được giải quyết;

h) thiết lập một nhật ký các hoạt động đã thực hiện trong quá trình xử lý (xem 9.10.1).

Thông tin khác

Dữ liệu đã được nhập đúng có thể bị sửa đổi do lỗi phần cứng, lỗi xử lý hoặc do các hoạt động cố ý. Việc kiểm tra tính hợp lệ được yêu cầu sẽ phụ thuộc vào tính chất của ứng dụng và tác động nghiệp vụ từ sự sửa đổi dữ liệu.

11.2.3 Tính toàn vẹn thông điệp

Biện pháp quản lý

Các yêu cầu đảm bảo tính xác thực và bảo vệ sự toàn vẹn thông điệp trong các ứng dụng cần được xác định. Bên cạnh đó, các biện pháp quản lý phù hợp cũng cần được xác định và triển khai.

Hướng dẫn triển khai

Việc đánh giá các rủi ro an toàn cần được thực hiện nhằm xác định xem tính toàn vẹn của thông điệp có được yêu cầu không và xác định phương pháp triển khai thích hợp nhất.

Thông tin khác

Các kỹ thuật mã hóa (xem 10.3) có thể được sử dụng như một phương tiện triển khai xác thực thông điệp phù hợp.

11.2.4 Kiểm tra tính hợp lệ của dữ liệu đầu ra

Biện pháp quản lý

Dữ liệu xuất ra từ một ứng dụng cần được kiểm tra tính hợp lệ nhằm đảm bảo rằng quá trình xử lý thông tin chính xác và thích hợp trong mọi trường hợp.

Hướng dẫn triển khai

Kiểm tra tính hợp lệ đầu ra có thể gồm:

a) các kiểm tra tính phù hợp nhằm kiểm tra xem dữ liệu đầu ra là có phù hợp không;

b) điều hòa các biện pháp quản lý nhằm đảm bảo xử lý tất cả dữ liệu;

c) cung cấp đầy đủ thông tin cho người đọc hoặc hệ thống xử lý tiếp theo nhằm xác định tính chính xác, tính đầy đủ, tính rõ ràng, và phân loại thông tin;

d) các thủ tục để xử lý tiếp khi có kết quả của các kiểm tra tính hợp lệ đầu ra;

e) xác định trách nhiệm của tất cả các cá nhân liên quan trong quá trình xử lý dữ liệu ra;

f) thiết lập một nhật ký các hoạt động trong quá trình kiểm tra tính hợp lệ của dữ liệu đầu ra.

Thông tin khác

Thông thường, các hệ thống và ứng dụng được xây dựng trên giả định rằng nếu được kiểm tra tính hợp lệ, thẩm tra và kiểm tra phù hợp thì đầu ra sẽ luôn chính xác. Tuy nhiên, giả định này không phải lúc nào cũng đúng; tức là, các hệ thống đã được kiểm tra vẫn có thể đưa ra đầu ra không chính xác trong một vài trường hợp.

11.3 Quản lý mã hóa

Mục tiêu: Nhằm bảo vệ tính bí mật, xác thực hoặc toàn vẹn của thông tin bằng các biện pháp mã hóa. Một chính sách về việc sử dụng các biện pháp quản lý bằng mã hóa cần được phát triển. Cần có sự quản lý nhằm hỗ trợ sử dụng các kỹ thuật mã hóa.

11.3.1 Chính sách sử dụng các biện pháp quản lý mã hóa

Biện pháp quản lý

Một chính sách về việc sử dụng các biện pháp quản lý mã hóa để bảo vệ thông tin cần được xây dựng và triển khai.

Hướng dẫn triển khai

Khi xây dựng chính sách mã hóa cần lưu ý những điều sau đây:

a) phương thức quản lý về việc sử dụng các biện pháp quản lý mật mã trên toàn tổ chức, bao gồm các nguyên tắc chung mà theo đó thông tin nghiệp vụ cần được bảo vệ (xem 4.1.1);

b) dựa trên quá trình đánh giá rủi ro, mức bảo vệ yêu cầu cần được xác định có lưu ý đến loại, năng lực và chất lượng của thuật toán mã hóa được yêu cầu;

c) sử dụng mã hóa để bảo vệ thông tin nhạy cảm được truyền bởi các thiết bị, phương tiện di động hoặc phương tiện có thể di dời, hoặc qua các đường truyền thông;

d) phương thức quản lý khóa, bao gồm các phương pháp bảo vệ khóa mã hóa và khôi phục thông tin đã được mã hóa trong trường hợp bị mất, bị tổn hại hoặc hỏng khóa;

e) các vai trò và trách nhiệm, ví dụ ai phải chịu trách nhiệm về:

1) triển khai chính sách;

2) quản lý khóa, bao gồm cả tạo khóa (xem thêm 11.3.2);

f) các tiêu chuẩn sẽ được chấp nhận để triển khai hiệu quả trên toàn tổ chức (giải pháp nào sẽ được sử dụng cho các quy trình nghiệp vụ nào);

g) ảnh hưởng của việc sử dụng thông tin mã hóa lên các biện pháp quản lý dựa trên điều tra nội dung (ví dụ phát hiện virus).

Khi triển khai chính sách mã hóa của tổ chức thì cần quan tâm đến các quy định và những hạn chế của quốc gia có thể áp dụng cho việc sử dụng các kỹ thuật mã hóa ở các khu vực khác nhau trên thế giới và áp dụng đối với các vấn đề về luồng thông tin mã hóa qua biên giới giữa các quốc gia (xem thêm 14.1.6)

Các biện pháp quản lý bằng mã hóa có thể được sử dụng để đạt được các mục tiêu an toàn khác nhau, ví dụ:

a) tính bí mật: sử dụng mã hóa thông tin để bảo vệ thông tin nhạy cảm hoặc quan trọng khi lưu trữ hoặc truyền đi;

b) tính toàn vẹn/tính xác thực: sử dụng chữ ký số hoặc mã xác thực thông điệp để bảo vệ tính xác thực và tính toàn vẹn của thông tin nhạy cảm hoặc quan trọng được lưu trữ hay truyền đi,.

c) tính không thể chối bỏ: sử dụng kỹ thuật mã hóa để thu chứng cứ về sự có mặt hoặc không có mặt của một sự kiện hoặc một hoạt động.

Thông tin khác

Việc đưa ra quyết định xem một giải pháp mã hóa nào đó có phù hợp không cần được xem như là một phần của quá trình đánh giá rủi ro và lựa chọn biện pháp quản lý rộng hơn. Vì vậy, sự đánh giá này có thể được sử dụng để xác định xem một biện pháp quản lý mã hóa có phù hợp không, loại biện pháp quản lý nào cần được sử dụng và được sử dụng cho mục đích và quá trình nghiệp vụ nào.

Một chính sách về việc sử dụng các biện pháp quản lý mã hóa là cần thiết nhằm tối đa lợi ích và giảm thiểu rủi ro khi sử dụng kỹ thuật mã hóa, và tránh việc sử dụng không chính xác hoặc không thích hợp. Khi sử dụng chữ ký số, cần quan tâm đến các quy định pháp lý liên quan, cụ thể là các quy định mô tả những điều kiện ràng buộc về mặt pháp lý của chữ ký số (xem 14.1).

Cần tìm tư vấn của các chuyên gia khi xác định mức bảo vệ thích hợp và khi xác định các chỉ tiêu kỹ thuật phù hợp sẽ cung cấp sự bảo vệ cần thiết và hỗ trợ việc triển khai hệ thống quản lý khóa an toàn (xem thêm 11.3.2).

ISO/IEC JTC1 SC27 đã phát triển một số tiêu chuẩn liên quan tới các biện pháp quản lý mã hóa. Thông tin sâu hơn cũng có thể tìm thấy trong IEEE1363 và các hướng dẫn của OECD về mã hóa.

11.3.2 Quản lý khóa

Biện pháp quản lý

Việc quản lý khóa cần sẵn sàng để hỗ trợ cho các kỹ thuật mã hóa được sử dụng trong tổ chức.

Hướng dẫn triển khai

Tất cả các khóa mật mã cần được bảo vệ nhằm khỏi sự sửa đổi, mất cắp và phá hoại. Hơn nữa, các khóa bí mật và khóa an toàn cần được bảo vệ khỏi sự tiết lộ trái phép. Thiết bị được sử dụng để tạo, lưu trữ và lấy được các khóa cần được bảo vệ vật lý.

Hệ thống quản lý khóa phải dựa trên bộ các tiêu chuẩn, thủ tục, và phương thức an toàn đã được chấp thuận nhằm:

a) tạo các khóa cho các hệ thống mã hóa khác nhau và các ứng dụng khác nhau;

b) tạo và nhận được các chứng chỉ khóa công khai;

c) phân phối mã khóa tới những người dùng nhất định, bao gồm cả cách kích hoạt khóa khi nhận được khóa;

d) lưu trữ khóa, bao gồm cả cách thức để những người dùng đã được cấp phép có thể truy cập tới khóa;

e) thay đổi hoặc cập nhật khóa bao gồm các nguyên tắc về thời gian phải đổi khóa và cách đổi khóa;

f) xử lý các khóa bị xâm phạm;

g) thu hồi khóa bao gồm cách thu hồi hoặc làm ngừng hoạt động khóa, ví dụ: khi khóa đã bị xâm phạm hoặc khi người dùng không làm việc cho tổ chức nữa (trường hợp nào khóa cần được lưu lại);

h) khôi phục lại các khóa bị mất hoặc bị sửa đổi như một phần của việc quản lý tính liên tục của nghiệp vụ, ví dụ cho việc khôi phục thông tin đã được mật mã;

i) Lưu trữ các khóa, ví dụ cho thông tin đã được lưu trữ hoặc sao lưu;

j) phá hủy khóa;

k) ghi nhật ký và đánh giá các hoạt động có liên quan đến việc quản lý khóa.

Để giảm khả năng xảy ra bị tổn hại thì ngày kích hoạt và giải kích hoạt các khóa cần được xác định sao cho các khóa có thể chỉ được sử dụng trong một khoảng thời gian giới hạn. Khoảng thời gian này phải tùy thuộc vào các trường hợp sử dụng biện pháp quản lý mã và các rủi ro được nhận biết.

Bên cạnh việc quản lý an toàn các khóa riêng và bí mật thì cũng cần quan tâm đến tính xác thực của khóa công cộng. Quá trình xác thực có thể được thực hiện bằng cách sử dụng các chứng chỉ khóa công cộng được phát hành bởi một cơ quan có thẩm quyền, cơ quan này phải là một tổ chức được công nhận có các biện pháp và thủ tục quản lý phù hợp nhằm cung cấp mức độ tin cậy được yêu cầu.

Nội dung của các thỏa thuận hoặc hợp đồng về mức dịch vụ với những nhà cung cấp các dịch vụ mã hóa bên ngoài, ví dụ với cơ quan cấp chứng chỉ, cần bao hàm các vấn đề về nghĩa vụ pháp lý, độ tin cậy của các dịch vụ và thời gian đáp ứng cung cấp dịch vụ (xem 5.2.3).

Thông tin khác

Quản lý khóa mã hóa cần thiết để sử dụng các kỹ thuật mã hóa một cách hiệu quả. ISO/IEC 11770 cung cấp thông tin sâu hơn về quản lý khóa. Có hai loại kỹ thuật mã hóa:

a) các kỹ thuật khóa bí mật, trường hợp này sẽ có hai hoặc nhiều bên cùng sử dụng chung một khóa và khóa này được sử dụng để mã hóa và giải mã thông tin; khóa này phải được giữ an toàn vì bất kỳ ai có thể truy cập tới khóa thì đều có khả năng giải mã tất cả các thông tin đã được mã hóa với khóa đó, hoặc sử dụng khóa đó để đưa ra thông tin trái phép;

b) các kỹ thuật khóa công khai, trường hợp này mỗi người sẽ sử dụng có một cặp khóa, một khóa công khai (khóa này có thể được tiết lộ) và một khóa riêng (khóa này được giữ bí mật); các kỹ thuật khóa công khai có thể được sử dụng để mã hóa và sản xuất chữ ký số (xem thêm ISO/IEC 9796 và ISO/IEC 14888).

Vẫn có khả năng giả mạo chữ ký số bằng cách thay khóa công khai của người dùng. Vấn đề này sẽ được giải quyết nếu sử dụng chứng chỉ khóa công khai.

Các kỹ thuật mã hóa có thể còn được sử dụng để bảo vệ các khóa mã hóa. Có thể còn cần các thủ tục để xử lý các yêu cầu pháp lý đối với truy cập tới các khóa mã hóa, ví dụ thông tin mã hóa có thể cần phải sẵn sàng ở dạng chưa được mã hóa với vai trò là bằng chứng trong các phiên toà.

11.4 An toàn cho các tệp tin hệ thống

Mục tiêu: Nhằm đảm bảo an toàn cho các tệp tin hệ thống.
Truy cập tới các tệp tin hệ thống và chương trình mã nguồn cần được quản lý, và các dự án IT và các hoạt động hỗ trợ phải được tiến hành một cách an toàn. Cần lưu ý tránh tiết lộ các dữ liệu nhạy cảm trong các môi trường kiểm tra thử.

11.4.1 Quản lý các phần mềm điều hành

Biện pháp quản lý

Cần phải có các thủ tục sẵn sàng cho việc quản lý quá trình cài đặt các phần mềm trên hệ thống vận hành.

Hướng dẫn triển khai

Để giảm thiểu rủi ro do sửa đổi các hệ thống vận hành, các hướng dẫn sau đây cần được quan tâm trong việc quản lý các thay đổi:

a) việc cập nhật phần mềm điều hành, các ứng dụng và các thư viện chương trình chỉ được thực hiện bởi những nhân viên quản trị đã được đào tạo theo quyền hạn quản lý phù hợp (xem 11.4.3);

b) các hệ thống vận hành chỉ được giữ mã thi hành đã được chấp nhận, và không được giữ mã phát triển hoặc các trình biên dịch;

c) các ứng dụng và phần mềm hệ thống điều hành chỉ được triển khai sau khi đã kiểm tra mở rộng và thành công; việc kiểm tra bao gồm các kiểm tra về tính tiện dụng, tính an toàn, các tác động lên các hệ thống khác và sự thân thiện với người dùng, và cần được thực hiện trên các hệ thống riêng biệt (xem thêm 9.1.4); cũng cần đảm bảo rằng tất cả các thư viện nguồn chương trình đều đã được cập nhật;

d) một hệ thống quản lý cấu hình cần được sử dụng để quản lý tất cả phần mềm đã được triển khai cũng như tài liệu hệ thống;

e) chiến lược hoàn trả cần được thực hiện trước khi triển khai các thay đổi;

f) nhật ký đánh giá cần được duy trì đối với mọi cập nhật về các thư viện chương trình điều hành;

g) các phiên bản trước đây của phần mềm ứng dụng cần được giữ lại với vai trò là một biện pháp phòng ngừa bất trắc;

h) các phiên bản cũ của phần mềm cũng cần được lưu lại cùng với tất cả thông tin và tham số, các thủ tục, cấu hình chi tiết, và phần mềm hỗ trợ được yêu cầu miễn sao dữ liệu vẫn được lưu lại.

Phần mềm do nhà cung cấp hỗ trợ được sử dụng trong các hệ thống vận hành cần được duy trì tại một mức được hỗ trợ bởi nhà cung cấp đó. Qua thời gian, các nhà cung cấp phần mềm sẽ ngừng hỗ trợ các phiên bản phần mềm cũ. Tổ chức cần quan tâm tới các rủi ro do phải sử dụng phần mềm không được hỗ trợ.

Các quyết định nâng cấp lên phiên bản mới đều phải xem xét các yêu cầu nghiệp vụ đối với sự thay đổi đó, và tính an toàn của phiên bản, tức là phải quan tâm đến các tính năng an toàn mới hoặc số lượng và mức độ nghiêm trọng của các vấn đề an toàn ảnh hưởng đến phiên bản này. Các bản vá phần mềm cũng cần được áp dụng nếu chúng có thể giúp loại bỏ hoặc giảm các điểm yếu an toàn (xem thêm 11.6.1).

Truy cập vật lý và logic chỉ được cấp phép cho các nhà cung cấp với các mục đích hỗ trợ khi cần thiết, và phải được sự chấp thuận của ban quản lý. Các hoạt động của nhà cung cấp cần được giám sát.

Phần mềm máy tính có thể dựa trên modun và phần mềm được cung cấp từ bên ngoài, chúng cần được giám sát và quản lý để ngăn chặn các thay đổi trái phép gây ra các điểm yếu về an toàn thông tin.

Thông tin khác

Hệ điều hành chỉ được nâng cấp khi có yêu cầu, ví dụ, khi phiên bản hiện tại của hệ điều hành không thể tiếp tục hỗ trợ các yêu cầu nghiệp vụ. Không được thực hiện các nâng cấp chỉ vì đã có phiên bản mới của hệ điều hành. Các phiên bản mới của hệ điều hành phiên bản có thể kém an toàn, ít ổn định và ít được hiểu rõ hơn hệ thống hiện tại.

11.4.2 Bảo vệ dữ liệu kiểm tra hệ thống

Biện pháp quản lý

Dữ liệu kiểm tra cần được lựa chọn, kiểm soát và bảo vệ một cách thận trọng.

Hướng dẫn triển khai

Việc sử dụng các cơ sở dữ liệu điều hành chứa các thông tin cá nhân hay bất kỳ thông tin nhạy cảm nào khác cho các mục đích kiểm tra cần phải được ngăn chặn. Nếu thông tin cá nhân hay thông tin nhạy cảm khác được sử dụng cho các mục đích kiểm tra thì tất cả các thông tin chi tiết và nội dung nhạy cảm phải được xóa bỏ hoặc sửa đổi đến khi không còn nhận ra được trước khi được đưa vào sử dụng. Các hướng dẫn sau đây cần được áp dụng để bảo vệ dữ liệu điều hành khi chúng được sử dụng cho các mục đích kiểm tra:

a) các thủ tục quản lý truy cập áp dụng cho các hệ thống ứng dụng điều hành cũng phải được áp dụng để kiểm tra các hệ thống ứng dụng;

b) cần được chấp thuận mỗi khi thông tin điều hành được sao chép vào một hệ thống ứng dụng kiểm tra;

c) thông tin điều hành cần được xóa khỏi hệ thống ứng dụng kiểm tra ngay khi việc kiểm tra đã hoàn tất;

d) việc sao chép và sử dụng thông tin điều hành cần được ghi vào nhật ký để cung cấp truy vết.

Thông tin khác

Việc kiểm tra hệ thống và chấp thuận thường yêu cầu lượng dữ liệu kiểm tra lớn gần tương đương với dữ liệu điều hành.

11.4.3 Quản lý truy cập đến mã nguồn chương trình

Biện pháp quản lý

Việc truy cập đến mã nguồn của chương trình cần được giới hạn chặt chẽ.

Hướng dẫn triển khai

Truy cập tới mã nguồn chương trình và các thông tin liên quan (ví dụ các thiết kế, các chỉ tiêu kỹ thuật, các kế hoạch thẩm tra và các kế hoạch kiểm tra tính hợp lệ) cần được quản lý chặt chẽ, nhằm ngăn chặn việc đưa thêm chức năng trái phép và tránh những thay đổi không cố ý. Mã nguồn chương trình có thể được quản lý nếu được lưu trữ tập trung, tốt nhất là trong các thư viện nguồn chương trình. Những hướng dẫn sau đây cần được quan tâm (xem thêm 10) trong việc quản lý truy cập tới các thư viện nguồn chương trình nhằm làm giảm khả năng sửa đổi các chương trình máy tính:

a) nếu có thể thì không được để các thư viện nguồn chương trình trong các hệ thống vận hành;

b) mã nguồn chương trình và các thư viện nguồn chương trình cần được quản lý theo với các thủ tục đã được thiết lập;

c) nhân viên hỗ trợ không được có truy cập không hạn chế tới các thư viện nguồn chương trình;

d) việc cập nhật các thư viện nguồn chương trình và các thông tin liên quan, và công bố các nguồn chương trình tới lập trình viên chỉ được thực hiện sau khi đã được cho phép;

e) các danh sách chương trình cần được giữ trong môi trường an toàn (xem 9.7.4);

f) nhật ký đánh giá cần được duy trì cho tất cả các truy cập tới các thư viện nguồn hệ thống;

g) việc duy trì và sao chép các thư viện nguồn chương trình phải tuân theo các thủ tục quản lý thay đổi (xem 11.5.1).

Thông tin khác

Mã nguồn chương trình là mã được viết bởi các lập trình viên, mã này được biên dịch (và được liên kết) để tạo nên các chương trình chạy được. Các ngôn ngữ lập trình hiện tại không chính thức phân biệt giữa mã nguồn và các chương trình chạy được vì các chương trình chạy được được tạo ra tại thời điểm chúng được kích hoạt.

Các tiêu chuẩn ISO 10007 và ISO/IEC 12207 cung cấp thêm thông tin về quản lý cấu hình và quy trình vòng đời của phần mềm.

11.5 Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển

Mục tiêu: Nhằm duy trì an toàn của thông tin và các phần mềm hệ thống ứng dụng.

Các môi trường dự án và hỗ trợ cần được quản lý chặt chẽ.

Các nhà quản lý chịu trách nhiệm về các hệ thống ứng dụng cũng phải chịu trách nhiệm về sự an toàn của môi trường dự án hoặc hỗ trợ. Họ cần đảm bảo rằng tất cả những thay đổi đề xuất của hệ thống đều đã được soát xét để chắc chắn rằng họ không làm tổn hại đến sự an toàn của hệ thống và môi trường hoạt động.

11.5.1 Các thủ tục quản lý thay đổi

Biện pháp quản lý

Việc thực thi các thay đổi phải được quản lý bằng việc áp dụng các thủ tục quản lý thay đổi chính thức.

Hướng dẫn triển khai

Các thủ tục quản lý thay đổi chính thức cần được lập thành văn bản và bắt buộc thi hành để giảm thiểu thiệt hại cho các hệ thống thông tin. Việc đề xuất các hệ thống mới và những thay đổi quan trọng cho hệ thống hiện tại cần tuân theo một quy trình chính thức về lập văn bản, đặc tả, kiểm tra, quản lý chất lượng và triển khai dưới sự quản lý.

Quy trình này cần bao gồm đánh giá rủi ro, phân tích những ảnh hưởng của các thay đổi, và đặc tả các biện pháp quản lý an toàn cần thiết. Quy trình này cũng phải đảm bảo rằng các thủ tục quản lý và an toàn hiện tại không bị ảnh hưởng, các lập trình viên hỗ trợ chỉ được phép truy cập đến các bộ phận hệ

thống cần thiết cho công việc của họ, phải tuân theo và các thay đổi đều phải được chấp thuận và phê chuẩn chính thức.

Nếu khả thi thì các thủ tục quản lý thay đổi ứng dụng và điều hành cần được tích hợp (xem thêm 9.1.2). Các thủ tục thay đổi cần bao gồm:

a) duy trì hồ sơ về các mức cấp phép đã được chấp thuận;

b) đảm bảo các thay đổi đều được thực thi bởi những người dùng được phép;

c) soát xét các biện pháp quản lý và toàn bộ các thủ tục nhằm đảm bảo rằng chúng sẽ không bị ảnh hưởng bởi các thay đổi;

d) xác định tất cả phần mềm, thông tin, các cơ sở dữ liệu, và phần cứng có yêu cầu sửa đổi;

e) có được sự phê chuẩn chính thức cho các đề xuất chi tiết trước khi triển khai;

f) đảm bảo rằng những người dùng hợp pháp chấp nhận các thay đổi trước khi triển khai;

g) đảm bảo rằng bộ tài liệu hệ thống được cập nhật mỗi khi hoàn tất từng thay đổi và tài liệu cũ được lưu trữ hoặc bị loại bỏ;

h) duy trì việc quản lý phiên bản đối với tất cả các cập nhật phần mềm;

i) duy trì truy vết của tất cả các yêu cầu thay đổi;

j) đảm bảo rằng văn bản vận hành (xem 9.1.1) và các thủ tục người dùng được thay đổi khi cần thiết để duy trì sự phù hợp;

k) đảm bảo rằng việc triển khai các thay đổi diễn ra đúng thời điểm và không làm ảnh hưởng đến các quá trình nghiệp vụ liên quan.

Thông tin khác

Việc thay đổi phần mềm có thể ảnh hưởng tới môi trường điều hành.

Kiểm nghiệm thực tiễn tốt sẽ bao hàm việc kiểm tra phần mềm mới trong một môi trường tách biệt với môi trường sản xuất và môi trường phát triển (xem thêm 9.1.4). Đó cũng là một cách để quản lý phần mềm mới và cho phép bảo vệ sâu thêm các thông tin điều hành được sử dụng cho các mục đích kiểm tra. Các đối tượng cần bảo vệ bao gồm các bản vá, các gói dịch vụ và bản cập nhật khác. Không được sử dụng các cập nhật tự động trên các hệ thống quan trọng vì một số cập nhật có thể gây lỗi trên các ứng dụng quan trọng (xem 11.6).

11.5.2 Soát xét kỹ thuật các ứng dụng sau thay đổi của hệ điều hành

Biện pháp quản lý

Khi hệ điều hành thay đổi, các ứng dụng nghiệp vụ quan trọng cần được soát xét và kiểm tra lại nhằm đảm bảo không xảy ra các ảnh hưởng bất lợi tới hoạt động cũng như an toàn của tổ chức.

Hướng dẫn triển khai

Quá trình này cần bao gồm:

a) soát xét biện pháp quản lý ứng dụng và toàn bộ các thủ tục nhằm đảm bảo rằng chúng không bị ảnh hưởng bởi các thay đổi của hệ điều hành;

b) đảm bảo rằng kế hoạch hỗ trợ và ngân sách hàng năm sẽ dành cho cả hoạt động soát xét và kiểm tra hệ thống sau các thay đổi của hệ điều hành;

c) đảm bảo rằng thông báo về các thay đổi hệ điều hành được đưa ra đúng thời điểm để cho phép thực hiện các kiểm tra và soát xét phù hợp trước khi triển khai;

d) đảm bảo rằng những thay đổi phù hợp được triển khai cho các kế hoạch về sự liên tục của hoạt động nghiệp vụ (xem 13).

Cần giao trách nhiệm cho một nhóm hoặc một cá nhân cụ thể trong việc giám sát các điểm yếu và các phiên bản của các bản vá và phần mềm của nhà cung cấp (xem 11.6).

11.5.3 Hạn chế thay đổi các gói phần mềm

Biện pháp quản lý

Việc sửa đổi các gói phần mềm là không được khuyến khích, cần hạn chế và chỉ thực hiện đối với các thay đổi rất cần thiết. Trong trường hợp này, mọi thay đổi cần phải được quản lý chặt chẽ.

Hướng dẫn triển khai

Miễn là có thể và khả thi, các gói phần mềm được nhà cung cấp hỗ trợ phải được sử dụng mà không bị sửa đổi. Nếu một gói phần mềm cần được sửa đổi thì phải quan tâm tới các vấn đề sau đây:

a) rủi ro của các biện pháp quản lý được cài đặt sẵn và toàn bộ các quy trình đang bị ảnh hưởng;

b) liệu có nhận được sự cho phép của nhà cung cấp không;

c) khả năng nhận được các thay đổi được yêu cầu từ nhà cung cấp dưới dạng các cập nhật chương trình chuẩn;

d) tác động nếu tổ chức phải có trách nhiệm trong việc bảo hành phần mềm trong tương lai do xảy ra các thay đổi.

Nếu những thay đổi là cần thiết thì phần mềm gốc cần được lưu lại và những thay đổi phải được thực hiện trên một bản sao đã được xác định rõ. Một quy trình quản lý cập nhật phần mềm cần được thực hiện nhằm đảm bảo các bản vá đã được chấp thuận cập nhật gần nhất và các bản cập nhật ứng dụng đã được cài đặt cho tất cả phần mềm đã được cấp phép (xem 11.6). Tất cả các thay đổi cần được kiểm tra đầy đủ và được lập thành tài liệu để chúng có thể được áp dụng lại nếu cần thiết cho các nâng cấp phần mềm trong tương lai. Nếu được yêu cầu, các thay đổi phải được kiểm tra và được xác nhận bởi một tổ chức đánh giá độc lập.

11.5.4 Sự rò rỉ thông tin

Biện pháp quản lý

Các điều kiện có thể gây rò rỉ thông tin cần phải được ngăn chặn.

Hướng dẫn triển khai

Cần quan tâm đến những vấn đề sau để hạn chế rủi ro rò rỉ thông tin, ví dụ do sử dụng và lợi dụng các kênh ngầm:

a) việc quét các phương tiện và kênh truyền thông bên ngoài để tìm các thông tin ẩn;

b) ngụy trang và điều chỉnh hệ thống và phương thức truyền thông nhằm giảm khả năng bên thứ ba có thể luận ra thông tin từ phương thức truyền thông đó;

c) tận dụng các hệ thống và phần mềm được xem là có tính toàn vẹn cao, ví dụ sử dụng các sản phẩm đã được đánh giá (xem ISO/IEC 15408);

d) giám sát thường xuyên các hoạt động của hệ thống và cá nhân nếu được cho phép và tuân theo các yêu cầu của quy định và pháp lý hiện hành;

e) giám sát việc sử dụng tài nguyên trong hệ thống máy tính.

Thông tin khác

Các kênh ngầm là tuyến không dùng để mang các luồng thông tin, tuy nhiên chúng vẫn có thể tồn tại trong hệ thống hoặc mạng. Ví dụ, việc điều khiển các bit trong các gói giao thức truyền thông có thể được sử dụng như một phương thức báo hiệu ẩn. Do bản chất của chúng mà rất khó có thể ngăn chặn sự tồn tại của tất cả các các kênh ngầm, nếu không nói là không thể. Tuy nhiên, các kênh này thường được mã Trojan lợi dụng (xem thêm 9.4.1). Việc thực thi các biện pháp quản lý ngăn chặn mã Trojan vì vậy sẽ làm giảm rủi ro từ việc lợi dụng các kênh ngầm.

Việc ngăn ngừa truy cập mạng trái phép (xem 10.4), cũng như các chính sách và thủ tục nhằm ngăn ngừa các cá nhân lạm dụng các dịch vụ thông tin (xem 14.1.5), sẽ giúp bảo vệ trước các kênh ngầm.

11.5.5 Phát triển phần mềm thuê khoán

Biện pháp quản lý

Việc phát triển các phần mềm thuê khoán cần được quản lý và giám sát bởi tổ chức.

Hướng dẫn triển khai

Trường hợp quá trình phát triển phần mềm thuê khoán thì cần quan tâm tới các điểm sau đây:

a) các vấn đề liên quan đến bản quyền, quyền sở hữu mã, và quyền sở hữu trí tuệ (xem 14.1.2);

b) việc cấp chứng nhận về chất lượng và độ chính xác của công việc cần thuê khoán;

c) các thỏa thuận giao kèo trong trường hợp có lỗi của bên thứ ba;

d) các quyền truy cập để đánh giá chất lượng và độ chính xác của công việc đã thực hiện;

e) các yêu cầu theo hợp đồng về chất lượng và chức năng an toàn của mã;

f) việc kiểm thử trước khi cài đặt nhằm phát hiện mã độc hại và mã Trojan.

11.6 Quản lý các điểm yếu kỹ thuật

Mục tiêu: Nhằm giảm thiểu các mối nguy hiểm xuất phát từ việc tin tặc lợi dụng các điểm yếu kỹ thuật đã được công bố.

Việc quản lý các điểm yếu kỹ thuật cần được triển khai theo một phương thức hiệu quả, có hệ thống và lặp lại với các biện pháp được thực hiện nhằm xác nhận hiệu quả của nó. Những đối tượng cần quan tâm phải bao gồm cả các hệ điều hành, và các ứng dụng khác đang được sử dụng.

11.6.1 Quản lý các điểm yếu về kỹ thuật

Biện pháp quản lý

Thông tin kịp thời về các điểm yếu kỹ thuật của các hệ thống thông tin đang được sử dụng cần phải được thu thập. Tổ chức cần công bố đánh giá về các điểm yếu này và thực hiện các biện pháp thích hợp để giải quyết các rủi ro liên quan.

Hướng dẫn triển khai

Việc kiểm kê các tài sản hiện có và bổ sung (xem 6.1) là một điều kiện tiên quyết để có được sự quản lý các điểm yếu kỹ thuật hiệu quả. Các thông tin cụ thể cần để hỗ trợ quản lý các điểm yếu kỹ thuật bao gồm nhà cung cấp phần mềm, số lượng phiên bản, trạng thái triển khai hiện tại (ví dụ phần mềm nào hiện đang được cài đặt trong các hệ thống nào), và những cá nhân trong tổ chức chịu trách nhiệm về phần mềm đó.

Hoạt động thích hợp, kịp thời cần được thực hiện nhằm định danh các điểm yếu kỹ thuật tiềm ẩn. Cần tuân theo các hướng dẫn sau để thiết lập được một quy trình quản lý các điểm yếu kỹ thuật hiệu quả:

a) tổ chức cần xác định và thiết lập các nguyên tắc và trách nhiệm liên quan đến việc quản lý các điểm yếu kỹ thuật, gồm việc giám sát các điểm yếu, đánh giá rủi ro của các điểm yếu, vá, theo dõi tài sản, và các trách nhiệm phối hợp bất kỳ được yêu cầu;

b) các tài nguyên thông tin sẽ được sử dụng để định danh các điểm yếu kỹ thuật liên quan và để duy trì mối quan tâm về chúng cũng cần được xác định đối với phần mềm và các công nghệ khác (dựa trên danh sách kiểm kê tài sản, xem 6.1.1); những tài nguyên thông tin này cần được cập nhật khi có những thay đổi trong bảng kiểm kê, hoặc khi tìm ra các nguồn tài nguyên mới hoặc hữu dụng;

c) cần xác định thời hạn phản ứng lại mỗi khi có các thông báo về các điểm yếu kỹ thuật tiềm ẩn;

d) mỗi khi có một điểm yếu kỹ thuật tiềm ẩn được xác định, tổ chức cần xác định các rủi ro liên quan và các hoạt động cần thực hiện; hoạt động đó có thể chỉ là vá các hệ thống bị tổn hại và/hoặc sử dụng các biện pháp quản lý khác;

e) tùy thuộc sự khẩn cấp cần giải quyết các điểm yếu kỹ thuật mà hoạt động đã được xác định phải được thực hiện theo các biện pháp quản lý liên quan tới việc quản lý sự thay đổi (xem 11.5.1) hoặc bằng cách tuân theo các thủ tục đối phó với sự cố an toàn thông tin (xem 12.2);

f) nếu bản vá có sẵn thì các rủi ro liên quan tới việc cài đặt bản vá cần được đánh giá (các rủi ro xuất phát từ điểm yếu đó cần được so sánh với rủi ro do cài đặt bản vá);

g) các bản vá cần được kiểm tra và đánh giá trước khi chúng được cài đặt nhằm đảm bảo sự hiệu quả và không dẫn tới những tác dụng phụ quá sức chịu đựng của hệ thống; nếu không có bản vá nào sẵn sàng thì cần quan tâm đến các biện pháp quản lý khác, ví dụ:

   1) tắt các dịch vụ hoặc các khả năng có liên quan tới điểm yếu;

   2) sửa lại hoặc đưa thêm các biện pháp quản lý truy cập, ví dụ đặt các bức tường lửa tại các biên giới mạng (xem 10.4.5);

   3) tăng cường giám sát nhằm phát hiện hoặc ngăn chặn các tấn công thực sự;

   4) nâng cao nhận thức về điểm yếu;

h) duy trì một nhật ký đánh giá đối với tất cả các thủ tục đã thực hiện;

i) quá trình quản lý các yếu điểm kỹ thuật cần được giám sát và đánh giá định kỳ nhằm đảm bảo ảnh hưởng và hiệu quả của nó;

j) các hệ thống có mức rủi ro cao cần được tập trung xử lý trước tiên.

Thông tin khác

Thực hiện chức năng chỉnh sửa của quy trình quản lý các điểm yếu kỹ thuật của tổ chức là vấn đề then chốt đối với nhiều tổ chức và vì vậy cần được giám sát định kỳ. Việc kiểm kê tài sản chính xác cũng rất cần thiết để có thể đảm bảo được rằng các điểm yếu kỹ thuật liên quan tiềm ẩn đều được xác định.

Việc quản lý các điểm yếu kỹ thuật có thể được coi như là một chức năng phụ của việc quản lý sự thay đổi và vì thế nó có thể tận dụng được các thủ tục và các quy trình quản lý sự thay đổi (xem 9.1.2 và 11.5.1).

Các nhà cung cấp thường phải chịu áp lực lớn trong việc ban hành các bản vá càng sớm sàng tốt. Vì vậy, một bản vá có thể không giải quyết được vấn đề một cách thỏa đáng và có thể gây ra những ảnh hưởng tiêu cực. Hơn nữa, trong một số trường hợp, việc gỡ các bản vá có thể lại không dễ dàng nếu bản vá đã được áp dụng.

Nếu không thể kiểm tra các bản vá một cách thỏa đáng, ví dụ do chi phí hoặc do thiếu tài nguyên, thì cũng có thể cân nhắc đến việc trì hoãn vá để đánh giá các rủi ro liên quan dựa trên kinh nghiệm đã được báo cáo bởi những người dùng khác.

12 Quản lý các sự cố an toàn thông tin

12.1Báo cáo về các sự kiện an toàn thông tin và các điểm yếu

Mục tiêu: Nhằm đảm bảo các sự kiện an toàn thông tin và các điểm yếu liên quan tới các hệ thống thông tin được trao đổi để các hành động khắc phục được tiến hành kịp thời.

Cần thực hiện việc báo cáo chính thức về các sự kiện và các thủ tục nâng dần cấp xử lý. Tất cả các nhân viên, người của nhà thầu và bên thứ ba phải nhận thức được các thủ tục báo cáo các loại sự kiện và điểm yếu khác nhau có thể ảnh hưởng tới sự an toàn các tài sản của tổ chức. Họ cần được yêu cầu báo cáo về điểm yếu và các sự kiện an toàn thông tin tới các điểm liên hệ xác định theo cách nhanh nhất có thể.

12.1.1 Báo cáo các sự kiện an toàn thông tin

Biện pháp quản lý

Các sự kiện an toàn thông tin cần được báo cáo thông qua các kênh quản lý thích hợp theo cách nhanh nhất có thể.

Hướng dẫn triển khai

Thủ tục báo cáo các sự kiện an toàn thông tin chính thức cần được thiết lập, cùng với thủ tục nâng dần cấp xử lý và phản ứng trước sự cố an toàn thông tin, thiết lập nên hoạt động cần thực hiện mỗi khi nhận được báo cáo về một sự kiện an toàn thông tin. Một điểm liên hệ cần được thiết lập để báo cáo các sự kiện an toàn thông tin. Cũng cần đảm bảo rằng điểm liên hệ này đều được biết đến trên toàn tổ chức, luôn sẵn sàng và có khả năng phản ứng một cách thỏa đáng và đúng lúc.

Toàn bộ nhân viên, những người thuộc các nhà thầu và bên sử dụng thứ ba đều phải nhận thức được các trách nhiệm của họ trong việc báo cáo các sự kiện an toàn thông tin theo cách nhanh nhất có thể. Họ cũng cần nhận thức được thủ tục báo cáo các sự kiện an toàn thông tin và điểm liên lạc. Các thủ tục báo cáo cần bao gồm:

a) các quy trình phản hồi phù hợp nhằm rằng đảm bảo các sự kiện an toàn thông tin được báo cáo đó đều được thông báo kết quả sau khi vấn đề đã được xử lý và loại bỏ;

b) các hình thức báo cáo các sự kiện an toàn thông tin nhằm hỗ trợ hoạt động báo cáo, và giúp người báo cáo ghi nhớ tất cả những hoạt động cần thiết trong trường hợp có sự kiện an toàn thông tin;

c) cách xử lý cần được thực hiện trong trường hợp có sự kiện an toàn thông tin, tức là:

   1) lập tức thông báo về tất cả các chi tiết quan trọng (ví dụ, dạng vi phạm hoặc không tuân thủ, sự cố hoạt động sai chức năng, các thông điệp trên màn hình, các bất thường);

   2) không tự ý thực hiện bất kỳ hoạt động nào, mà ngay lập tức báo cáo đến đầu mối liên hệ;

d) tham khảo quy trình kỷ luật chính thức đã xác lập đối với các nhân viên, người của các nhà thầu hoặc bên thứ ba đã vi phạm an toàn thông tin.

Trong các môi trường có độ rủi ro cao thì phải bắt buộc đưa ra cảnh báo về các sự cố có độ rủi ro cao. Các thủ tục phản ứng với các cảnh báo bắt buộc cần phản ánh tình trạng rủi ro cao mà các cảnh báo chỉ ra.

Thông tin khác

Dưới đây là những ví dụ về các sự kiện và sự cố an toàn thông tin:

a) mất dịch vụ, thiết bị hoặc các tiện ích,

b) các trục trặc hệ thống hoặc quá tải hệ thống,

c) các lỗi do con người,

d) không tuân thủ các chính sách hoặc các hướng dẫn,

e) vi phạm các vấn đề an toàn vật lý,

f) những thay đổi hệ thống không được quản lý,

g) các sự cố về phần cứng hoặc phần mềm,

h) các vi phạm truy cập.

Nếu quan tâm đầy đủ đến các khía cạnh bảo mật thì các sự cố an toàn thông tin có thể được sử dụng trong việc đào tạo nhận thức của người dùng (xem 7.2.2) với vai trò là các ví dụ về những vấn đề có thể xảy ra, cách phản ứng với các sự cố như vậy, và cách phòng tránh chúng trong tương lai. Để có thể giải quyết được các sự cố và sự kiện an toàn thông tin một cách thỏa đáng, có thể cũng cần thu thập chứng cứ sớm nhất có thể ngay sau khi chúng xảy ra (xem 12.2.3).

Các trục trặc hoặc các bất thường khác của hệ thống có thể là một chỉ báo của một tấn công hoặc một lỗ hổng an toàn thực tế và do đó cần luôn được thông báo như là sự kiện an toàn thông tin.

Thông tin chi tiết hơn về thông báo về các sự kiện an toàn thông tin và quản lý các sự cố an toàn thông tin đã được trình bày trong ISO/IEC TR 18044.

12.1.2 Báo cáo các điểm yếu về an toàn thông tin

Biện pháp quản lý

Mọi nhân viên, nhà thầu và bên thứ ba của các dịch vụ và hệ thống thông tin cần được yêu cầu ghi lại và báo cáo bất kỳ điểm yếu nào về an toàn đã thấy hoặc cảm thấy nghi ngờ trong các hệ thống hoặc dịch vụ.

Hướng dẫn triển khai

Tất cả các nhân viên, nhà thầu và người dùng thuộc bên thứ ba đều phải báo cáo về những vấn đề này tới ban quản lý hoặc trực tiếp tới nhà cung cấp dịch vụ của họ theo cách nhanh nhất có thể nhằm

ngăn chặn các sự cố an toàn thông tin. Cơ cấu báo cáo cần phải dễ dàng, tiện dụng, và sẵn sàng tới mức có thể. Trong mọi trường hợp, họ cần được thông báo rằng họ không được cố gắng chứng minh về điểm yếu bị nghi ngờ.

Thông tin khác

Các nhân viên, nhà thầu và người dùng thuộc tổ chức thứ ba cần được tư vấn không được cố gắng chứng minh về các điểm yếu bị nghi ngờ. Việc kiểm tra các điểm yếu có thể được hiểu như một sự lạm dụng tiềm ẩn hệ thống và cũng có thể gây thiệt hại cho các hệ thống hoặc dịch vụ thông tin và dẫn đến trách nhiệm pháp lý của cá nhân thực hiện việc kiểm tra.

12.2 Quản lý các sự cố an toàn thông tin và cải tiến

Mục tiêu: Nhằm đảm bảo một cách tiếp cận hiệu quả và nhất quán được áp dụng trong việc quản lý sự cố an toàn thông tin.

Các trách nhiệm và thủ tục cần được thực hiện để xử lý các sự kiện và điểm yếu an toàn thông tin một cách hiệu quả mỗi khi chúng được báo cáo. Quá trình cải tiến liên tục cũng cần được áp dụng nhằm phản ứng, giám sát, đánh giá, và quản lý chung về các sự cố an toàn thông tin.

Trong trường hợp có yêu cầu bằng chứng thì chúng phải được thu thập để đảm bảo sự tuân thủ các yêu cầu pháp lý.

12.2.1 Các trách nhiệm và thủ tục

Biện pháp quản lý

Các thủ tục và trách nhiệm quản lý cần được thiết lập nhằm đảm bảo sự phản ứng nhanh chóng, hiệu quả, đúng trình tự khi xảy ra các sự cố an toàn thông tin.

Hướng dẫn triển khai

Bên cạnh việc báo cáo các điểm yếu và sự kiện an toàn thông tin (xem 12.1), cũng cần giám sát các hệ thống, các cảnh báo, và các điểm yếu (9.10.2) cần được sử dụng nhằm phát hiện các sự cố an toàn thông tin.

Những hướng dẫn sau đây cho các thủ tục quản lý sự cố an toàn thông tin cần được quan tâm:

a) các thủ tục cần được thiết lập nhằm xử lý các dạng sự cố an toàn thông tin khác nhau bao gồm:

   1) lỗi hệ thống thông tin và mất dịch vụ;

   2) mã độc hại (xem 9.4.1);

   3) từ chối dịch vụ;

   4) các lỗi do dữ liệu nghiệp vụ không đầy đủ hoặc không chính xác;

   5) các vi phạm về tính bí mật hoặc tính toàn vẹn;

   6) sự lạm dụng các hệ thống thông tin;

b) bên cạnh các kế hoạch đối phó với các sự kiện bất ngờ thông thường (xem 13.1.3) thì các thủ tục cũng cần bao gồm (xem 12.2.2):

1) phân tích và xác định nguyên nhân của sự cố;

2) chính sách ngăn chặn;

3) lập kế hoạch và triển khai hoạt động khắc phục nhằm ngăn ngừa tái diễn, nếu cần thiết;

4) trao đổi thông tin với những người bị ảnh hưởng hoặc có tham gia vào phục hồi sự cố;

5) báo cáo về hoạt động tới người có thẩm quyền thích hợp;

c) các truy vết và các bằng chứng tương tự phải được thu thập (xem 12.2.3) và được bảo vệ an toàn, để dùng cho việc:

1) phân tích vấn đề từ bên trong;

2) sử dụng như chứng cứ pháp lý liên quan tới việc vi phạm hợp đồng hoặc yêu cầu pháp lý hoặc trong các trường hợp xảy ra kiện cáo dân sự hoặc hình sự, ví dụ lạm dụng chức năng của máy tính hoặc làm sai luật bảo vệ dữ liệu;

3) thương lượng bồi thường từ những nhà cung cấp dịch vụ và phần mềm;

d) hoạt động nhằm khôi phục lại sau khi xảy ra các lỗ hổng an toàn và hiệu chỉnh các lỗi hệ thống cần được quản lý thận trọng và chính thức; các thủ tục cần đảm bảo rằng:

1) chỉ cá nhân được phép và đã được chỉ định rõ mới được phép truy cập vào dữ liệu và hệ thống đang hoạt động (xem 5.2 phần truy cập từ bên ngoài);

2) mọi hoạt động khẩn cấp đã được thực hiện đều phải được ghi vào văn bản một cách chi tiết;

3) hoạt động khẩn cấp phải được báo cáo với ban quản lý và được soát xét một cách có trình tự;

4) tính toàn vẹn của các hệ thống nghiệp vụ và các biện pháp quản lý cần được chứng thực với độ trễ tối thiểu.

Các mục tiêu của việc quản lý sự cố an toàn thông tin cần được ban quản lý thông qua, và cũng cần đảm bảo rằng những người có trách nhiệm trong việc quản lý sự cố an toàn thông tin đều hiểu rõ quyền ưu tiên của tổ chức đối với việc xử lý các sự cố an toàn thông tin.

Thông tin khác

Các sự cố an toàn thông tin có thể nằm ngoài ranh giới của tổ chức và ranh giới quốc gia. Để phản ứng lại các sự cố như vậy cần nâng cao yêu cầu phối hợp ứng cứu và chia sẻ thông tin về các sự cố với các tổ chức bên ngoài một cách phù hợp.

12.2.2 Rút bài học kinh nghiệm từ các sự cố an toàn thông tin

Biện pháp quản lý

Cần có các cơ chế sẵn sàng nhằm cho phép các lượng hóa và giám sát các kiểu, số lượng và chi phí của các sự cố an toàn thông tin.

Hướng dẫn triển khai

Thông tin thu được từ quá trình đánh giá các sự cố an toàn thông tin phải được sử dụng để xác định các sự cố có tính chu kỳ hoặc có ảnh hưởng lớn.

Thông tin khác

Việc đánh giá các sự cố an toàn thông tin có thể chỉ ra sự cần thiết phải áp dụng các biện pháp quản lý tăng cường hoặc bổ sung nhằm hạn chế tần suất, thiệt hại và chi phí của các sự cố trong tương lai, hoặc phải xem xét sử dụng quá trình soát xét chính sách an toàn (xem 4.1.2).

12.2.3 Thu thập chứng cứ

Biện pháp quản lý

Khi một hành động nhằm chống lại một người hay một tổ chức sau khi có một sự cố an toàn thông tin xảy ra, liên quan đến pháp luật (có thể là dân sự hoặc hình sự), thì chứng cứ cần được thu thập, giữ lại, và được trình bày sao cho phù hợp với quy định pháp lý.

Hướng dẫn triển khai

Các thủ tục nội bộ cần được phát triển và tuân thủ trong quá trình thu thập và trình bày các chứng cứ cho các mục đích của xử lý kỷ luật trong nội bộ tổ chức.

Nhìn chung, các quy tắc đối với chứng cứ bao gồm:

a) khả năng chấp nhận được của chứng cứ: liệu chứng cứ có được sử dụng trong phiên toà không;

b) trọng lượng của chứng cứ: chất lượng và tính đầy đủ của chứng cứ.

Để đạt được khả năng chấp nhận của chứng cứ thì tổ chức cần đảm bảo rằng các hệ thống thông tin của họ đã tuân thủ tất cả các tiêu chuẩn hoặc quy tắc thực hành đã được ban hành trong việc lấy các chứng cứ có thể được chấp nhận.

Trọng lượng của chứng cứ được cung cấp phải tuân thủ các yêu cầu hiện hành. Để có được trọng lượng của chứng cứ thì chất lượng và tính đầy đủ của các biện pháp quản lý được sử dụng nhằm bảo vệ chứng cứ một cách phù hợp và nhất quán (tức là quy trình quản lý bằng chứng) trong suốt thời gian các chứng cứ được lưu giữ và xử lý phải được thể hiện bởi một vết chứng cứ chắc chắn. Nhìn chung, vết chứng cứ chắc chắn có thể được thiết lập theo các điều kiện sau đây:

a) đối với các tài liệu in trên giấy: bản gốc cần được giữ an toàn cùng với một hồ sơ của người đã tìm thấy tài liệu, nơi tìm thấy tài liệu, thời điểm tìm thấy tài liệu và người làm chứng cho phát hiện này; mọi cuộc điều tra đều phải đảm bảo rằng các tài liệu gốc không bị giả mạo;

b) đối với các thông tin trên thiết bị máy tính: các hình ảnh trung thực hoặc các bản sao (tùy thuộc các yêu cầu ứng dụng) của mọi phương tiện có thể di dời, thông tin trên các đĩa cứng hoặc trong bộ nhớ cần được đảm bảo tính sẵn sàng; nhật ký của mọi hoạt động trong quá trình sao chép cần được giữ lại và quá trình sao chép cần có người chứng kiến; các phương tiện gốc và nhật ký (nếu không thể thì ít nhất là hình ảnh trung thực hoặc một bản sao) phải được giữ an toàn và bí mật.

Mọi công việc có liên quan đến pháp luật đều chỉ được thực hiện trên các bản sao tài liệu chứng cứ. Tính toàn vẹn của tất cả các tài liệu chứng cứ cần được bảo vệ. Việc sao chép tài liệu chứng cứ phải được giám sát bởi một cá nhân đáng tin cậy và thông tin về thời gian và địa điểm thực hiện sao chép, người thực hiện các hoạt động sao chép, các công cụ và các chương trình nào đã được sử dụng cũng cần phải được ghi lại.

Thông tin khác

Khi một sự kiện an toàn thông tin được phát hiện lần đầu, có thể không thể xác định rõ ràng liệu sự kiện đó có phải đưa ra tòa hay không. Vì vậy, tồn tại một nguy cơ rằng chứng cứ cần thiết có thể vô tình hoặc cố ý bị phá hủy trước khi mức độ nghiêm trọng của vụ việc được nhận ra. Do vậy, nên sớm cần có một luật sư hoặc một nhân viên cảnh sát trong mọi hoạt động pháp lý được dự định thực hiện và được tư vấn về chứng cứ.

Chứng cứ có thể nằm ngoài phạm vi quyền hạn và/hoặc biên giới của tổ chức. Trong những trường hợp này, cần đảm bảo rằng tổ chức được quyền thu thập các thông tin cần thiết làm chứng cứ. Các yêu cầu về phạm vi quyền hạn pháp lý khác nhau cũng cần được xem xét nhằm tối đa hóa các cơ hội thú nhận.

13 Quản lý sự liên tục của hoạt động nghiệp vụ

13.1Các khía cạnh an toàn thông tin trong quản lý sự liên tục của hoạt động nghiệp vụ

Mục tiêu: Chống lại các gián đoạn trong hoạt động nghiệp vụ và bảo vệ các quy trình hoạt động trọng yếu khỏi các ảnh hưởng do lỗi hệ thống thông tin hay các thảm họa và đảm bảo khả năng khôi phục các hoạt động bình thường kịp thời. Quy trình quản lý sự liên tục của hoạt động nghiệp vụ cần được triển khai nhằm tối giảm ảnh hưởng lên tổ chức và khôi phục lại sau khi mất mát các tài sản thông tin (ví dụ, tài sản có thể bị mất do các thảm họa tự nhiên, các tai nạn, lỗi thiết bị, và các hoạt động cố ý) đến một mức độ có thể chấp nhận bằng cách phối hợp các biện pháp quản lý ngăn ngừa và khôi phục. Quá trình này cần xác định các quy trình nghiệp vụ có tính quyết định và kết hợp với các yêu cầu quản lý an toàn thông tin về sự liên tục của hoạt động nghiệp vụ với các yêu cầu về sự liên tục khác liên quan tới

các khía cạnh điều hành, đội ngũ nhân viên, tài liệu, vận chuyển và các phương tiện.

Hậu quả của các thảm họa, lỗi bảo mật, mất mát thiết bị, và sự sẵn sàng của dịch vụ phải là các đối tượng của quá trình phân tích ảnh hưởng lên nghiệp vụ. Các kế hoạch về sự liên tục trong hoạt động nghiệp vụ cần được phát triển và triển khai nhằm đảm bảo sự tiếp tục của các hoạt động cần thiết đúng lúc. An toàn thông tin cần phải là một phần không tách rời của quá trình đảm bảo sự liên tục của hoạt động nghiệp vụ, và các quá trình quản lý khác trong tổ chức.

Quản lý sự liên tục của hoạt động nghiệp vụ cần bao hàm các biện pháp quản lý nhằm xác định và giảm thiểu rủi ro, bên cạnh quá trình đánh giá rủi ro chung, sẽ làm hạn chế hậu quả do những sự cố phá hoại, và đảm bảo rằng thông tin được yêu cầu cho các quá trình nghiệp vụ là sẵn sàng.

13.1.1 Tính đến an toàn thông tin trong các quy trình quản lý sự liên tục của hoạt động nghiệp vụ

Biện pháp quản lý

Một quy trình được quản lý cần được xây dựng và duy trì nhằm đảm bảo các hoạt động của cơ quan/tổ chức không bị gián đoạn. Nội dung quy trình này phải đề cập các yêu cầu về an toàn thông tin cần thiết nhằm đảm bảo các hoạt động liên tục của tổ chức.

Hướng dẫn triển khai

Quy trình này phải cho các yếu tố quan trọng sau trong quản lý sự liên tục của các hoạt động nghiệp vụ:

a) hiểu về các rủi ro mà tổ chức đang đối mặt trên khía cạnh về rủi ro rất có khả năng xảy ra và ảnh hưởng của chúng một cách kịp thời, bao gồm định danh và phân loại ưu tiên các quá trình nghiệp vụ quan trọng (xem 13.1.2);

b) xác định mọi tài sản tham gia vào các quá trình nghiệp vụ quan trọng (xem 6.1.1);

c) hiểu rõ về ảnh hưởng lên hoạt động nghiệp vụ của các gián đoạn do các sự cố thông tin có khả năng xảy ra (quan trọng là các giải pháp tìm được phải giải quyết được các sự cố gây ra ảnh hưởng nhỏ, cũng như các sự cố nghiêm trọng có thể đe dọa sự tồn tại của tổ chức), và thiết lập các mục tiêu nghiệp vụ của các phương tiện xử lý thông tin;

d) *cân nhắc đến việc mua bảo hiểm phù hợp, việc này có thể là một phần trong quy trình quản lý* sự liên tục của hoạt động nghiệp chung, và cũng là một phần trong quá trình quản lý rủi ro hoạt động;

e) xác định và quan tâm tới việc triển khai thêm các biện pháp quản lý phòng ngừa và giảm nhẹ thiệt hại;

f) xác định các nguồn tài nguyên về tài chính, tổ chức, kỹ thuật và môi trường thỏa đáng để có thể xử lý được các yêu cầu an toàn thông tin đã xác định;

g) đảm bảo sự an toàn cho nhân viên và sự bảo vệ các phương tiện xử lý thông tin và tài sản của tổ chức;

h) lập và lập thành tài liệu các kế hoạch quản lý sự liên tục của hoạt động nghiệp vụ trong đó giải quyết các yêu cầu an toàn thông tin tuân theo chiến lược quản lý sự liên tục về hoạt động nghiệp vụ đã được thông qua (xem 13.1.3);

i) kiểm tra và cập nhật định kỳ các kết hoạch và các quy trình cần thực hiện (xem 13.1.5);

j) đảm bảo rằng việc quản lý sự liên tục của hoạt động nghiệp vụ được phối hợp trong cơ cấu và các quy trình của tổ chức, trách nhiệm về quá trình quản lý sự liên tục của hoạt động nghiệp vụ cần được phân ở mức độ phù hợp trong tổ chức (xem 5.1.1).

13.1.2 Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức

Biện pháp quản lý

Các sự kiện có thể gây ra gián đoạn sự gián đoạn của hoạt động của tổ chức cần được xác định cùng với xác suất, ảnh hưởng cũng như hậu quả của chúng đối với an toàn thông tin.

Hướng dẫn triển khai

Các khía cạnh an toàn thông tin của sự liên tục của hoạt động nghiệp vụ cần dựa trên việc xác định các sự kiện (hoặc chuỗi sự kiện) có thể gây ra sự gián đoạn các quá trình nghiệp vụ của tổ chức, ví dụ sự cố thiết bị, lỗi do con người, mất cắp, cháy, các thảm họa tự nhiên và các hoạt động khủng bố. Sau đó cần đánh giá rủi ro nhằm xác định khả năng xảy ra và ảnh hưởng của những gián đoạn đó, về mặt thời gian, mức độ thiệt hại và thời gian khôi phục.

Các đánh giá rủi ro đối với sự liên tục của các hoạt động nghiệp vụ cần được thực hiện với sự tham gia đầy đủ của các chủ sở hữu các quá trình và các nguồn tài nguyên nghiệp vụ. Việc đánh giá này cần xem xét mọi quá trình nghiệp vụ và không được giới hạn chỉ với các phương tiện xử lý thông tin, nhưng phải cho các kết quả cụ thể về an toàn thông tin. Điều quan trọng là phải liên kết các khía cạnh rủi ro khác nhau với nhau để có được một bức tranh hoàn chỉnh về các yêu cầu về sự liên tục của hoạt động nghiệp vụ của tổ chức. Việc đánh giá cần xác định, định lượng, và phân loại ưu tiên các rủi ro dựa trên tiêu chí và các mục tiêu của tổ chức, trong đó phải bao hàm các nguồn tài nguyên quan trọng, những ảnh hưởng của sự gián đoạn, thời gian gián đoạn cho phép, và các ưu tiên khôi phục.

Tùy thuộc vào các kết quả của quá trình đánh giá rủi ro, một chiến lược về sự liên tục của hoạt động nghiệp vụ cần được phát triển nhằm xác định cách tiếp cận chung đối với sự liên tục của hoạt động nghiệp vụ. Một khi chiến lược này đã được thiết lập thì ban quản lý cần thông qua, và một kế hoạch đã được thiết lập và thông qua để triển khai chiến lược này.

13.1.3 Xây dựng và triển khai các kế hoạch về tính liên tục, trong đó bao gồm vấn đề đảm bảo an toàn thông tin

Biện pháp quản lý

Các kế hoạch phải được phát triển và triển khai nhằm duy trì hoặc khôi phục các hoạt động điều hành và đảm bảo tính sẵn sàng của thông tin ở mức độ yêu cầu và đáp ứng yêu cầu về thời gian xử lý các gián đoạn và hư hỏng trong các quá trình nghiệp vụ quan trọng.

Hướng dẫn triển khai

Quá trình lên kế hoạch về tính liên tục về nghiệp vụ cần quan tâm tới những điều sau:

a) xác định và thông qua mọi trách nhiệm và thủ tục về tính liên tục của hoạt động nghiệp vụ;

b) xác định độ mất mát thông tin và dịch vụ ở mức chấp nhận được;

c) triển khai các thủ tục cho phép khôi phục và phục hồi các hoạt động nghiệp vụ và tính sẵn sàng của thông tin theo thang thời gian yêu cầu; cần đưa ra các yêu cầu chú ý đặc biệt đến việc đánh giá những phụ thuộc về nghiệp vụ trong nội bộ và bên ngoài và các bản hợp đồng đang có hiệu lực;

d) các thủ tục vận hành cho đến khi hoàn tất việc khôi phục và phục hồi;

e) tài liệu về các quy trình và thủ tục;

f) đào tạo phù hợp đội ngũ nhân viên về các quá trình và thủ tục đã được thông qua, gồm cả việc quản lý khủng hoảng;

g) kiểm tra và cập nhật các kế hoạch.

Quá trình lập kế hoạch cần tập trung vào các mục tiêu nghiệp vụ được yêu cầu, ví dụ việc khôi phục các dịch vụ truyền thông cụ thể cho khách hàng trong khoảng thời gian có thể chấp nhận. Các dịch vụ và nguồn tài nguyên hỗ trợ quá trình này cũng cần được xác định, bao gồm đội ngũ nhân viên, các nguồn tài nguyên xử lý không phải dạng thông tin, cũng như các dàn xếp về phương tiện xử lý thông tin dự phòng. Các dàn xếp như vậy có thể bao hàm cả các dàn xếp với các bên thứ ba dưới hình thức là các thỏa thuận giữa hai bên, hoặc các dịch vụ thuê bao thương mại.

Các kế hoạch về sự liên tục của hoạt động nghiệp vụ cần tập trung vào các điểm yếu của tổ chức và vì *vậy có thể chứa các thông tin nhạy cảm cần được bảo vệ thích hợp. Các bản sao của các kế hoạch về* sự liên tục của hoạt động nghiệp vụ cần được lưu trữ tại một địa điểm ở xa với khoảng cách đủ để có thể không bị thiệt hại từ các thảm họa tại điểm chính. Ban quản lý cần đảm bảo các bản sao chép đó phải được cập nhật và được bảo vệ với mức an toàn như tại địa điểm chính. Các tài liệu khác cần cho việc thực hiện các kế hoạch về tính liên tục cũng cần được lưu trữ ở một vị trí ở xa.

Nếu sử dụng các vị trí thay thế tạm thời thì mức độ của các biện pháp quản lý an toàn được triển khai tại những vị trí đó phải tương đương với vị trí chính.

Thông tin khác

Cũng cần chú ý rằng các kế hoạch và các hoạt động quản lý khủng hoảng (xem 13.1.3f)) có thể khác với quản lý sự liên tục của hoạt động nghiệp vụ.

13.1.4 Khung hoạch định sự liên tục trong hoạt động nghiệp vụ

Biện pháp quản lý

Một khung hoạch định các kế hoạch đảm bảo liên tục trong hoạt động nghiệp vụ cần được duy trì để mọi kế hoạch được thực hiện một cách nhất quán và đạt được các yêu cầu về đảm bảo an toàn thông tin cũng như xác định được các mức độ ưu tiên cho việc kiểm tra và duy trì.

Hướng dẫn triển khai

Mỗi kế hoạch về sự liên tục của các hoạt động nghiệp vụ phải mô tả cách tiếp cận tính liên tục, ví dụ cách tiếp cận để đảm bảo tính sẵn sàng và sự an toàn của thông tin hoặc hệ thống thông tin. Mỗi kế hoạch cũng cần xác định rõ kế hoạch nâng dần cấp xử lý và các điều kiện thực hiện, cũng như các cá nhân có trách nhiệm thực hiện từng bộ phận của kế hoạch. Khi có các yêu cầu mới được xác định thì mọi thủ tục khẩn cấp hiện hành, ví dụ các kế hoạch di tản hoặc các dàn xếp về dự phòng, cần được bổ sung hợp lý. Các thủ tục cần nằm trong chương trình quản lý thay đổi của tổ chức để đảm bảo rằng các vấn đề về sự liên tục của hoạt động nghiệp vụ luôn được giải quyết thỏa đáng.

Mỗi kế hoạch cần có người sở hữu xác định. Các thủ tục khẩn cấp, kế hoạch dự phòng bằng nhân công, và các kế hoạch tiếp tục phải thuộc trách nhiệm của những người sở hữu các tài nguyên nghiệp vụ và các quá trình liên quan. Các dàn xếp dự phòng cho các dịch vụ kỹ thuật thay thế, chẳng hạn như các phương tiện truyền thông và xử lý thông tin, phải luôn thuộc trách nhiệm của các nhà cung cấp dịch vụ.

Khung hoạch định sự liên tục trong hoạt động nghiệp vụ cần tập trung vào các yêu cầu an toàn thông tin đã được xác định và cần quan tâm tới những điều sau:

a) các điều kiện khởi động các kế hoạch, trong đó mô tả quy trình phải thực hiện (ví dụ cách đánh giá tình hình, người tham gia) trước khi mỗi kế hoạch được khởi động;

b) các thủ tục khẩn cấp, trong đó mô tả các hoạt động cần được thực hiện khi xảy ra một sự cố gây nguy hiểm cho các hoạt động nghiệp vụ;

c) các thủ tục dự phòng trong đó mô tả các hoạt động cần được thực hiện nhằm thúc đẩy các hoạt động nghiệp vụ cần thiết hoặc hỗ trợ các dịch vụ cho các vị trí thay thế tạm thời khác, và khôi phục các quá trình nghiệp vụ theo các thang thời gian yêu cầu;

d) thủ tục vận hành tạm thời trong khi chờ đợi hoàn thành việc khôi phục;

e) các thủ tục tiếp tục lại trong đó mô tả những hoạt động cần được thực hiện để trở lại các hoạt động nghiệp vụ bình thường;

f) lịch trình bảo dưỡng trong đó quy định cách thức và thời gian kế hoạch sẽ được kiểm tra và quy trình duy trì kế hoạch;

g) các hoạt động nhận thức, giáo dục và đào tạo được thiết kế nhằm thiết lập hiểu biết về các quá trình đảm bảo sự liên tục của nghiệp vụ và đảm bảo rằng các quá trình đó vẫn tiếp tục có hiệu quả;

h) các trách nhiệm của các cá nhân, trong đó mô tả những người có trách nhiệm thực hiện thành phần nào của kế hoạch. Các lựa chọn thay thế cần được đề cử khi có yêu cầu;

i) các tài sản và nguồn tài nguyên quan trọng cần để có thể thực hiện các thủ tục khẩn cấp, dự phòng và tiếp tục lại.

13.1.5 Kiểm tra, duy trì và đánh giá lại các kế hoạch đảm bảo sự liên tục trong hoạt động nghiệp vụ

Biện pháp quản lý

Các kế hoạch về sự liên tục trong hoạt động nghiệp vụ cần được kiểm tra và cập nhật thường xuyên nhằm luôn đảm bảo tính cập nhật và hiệu quả.

Hướng dẫn triển khai

Các cuộc kiểm tra kế hoạch về sự liên tục của hoạt động nghiệp vụ cần đảm bảo rằng tất cả thành viên của nhóm khôi phục và đội ngũ nhân viên có liên quan khác đều nhận thức được về các kế hoạch và trách nhiệm của họ đối với sự liên tục của hoạt động nghiệp vụ và sự an toàn thông tin và biết được vai trò của họ khi kế hoạch được đề xuất.

Kế hoạch kiểm tra (các) kế hoạch về sự liên tục của hoạt động nghiệp vụ cần chỉ ra cách thức và thời gian kiểm tra từng thành phần của kế hoạch. Mỗi thành phần của (các) kế hoạch cần được kiểm tra thường xuyên.

Phải sử dụng nhiều kỹ thuật kiểm tra để đảm bảo rằng (các) kế hoạch sẽ vận hành trong đời sống thực tế. Các kỹ thuật này phải bao gồm:

a) kiểm tra bằng công nghệ cao các kịch bản khác nhau (trong đó thảo luận về các kịch bản khôi phục hoạt động nghiệp vụ sử dụng các gián đoạn mẫu);

b) mô phỏng (đặt biệt là trong quá trình đào tạo con người về các vai trò của họ trong việc quản lý hậu sự cố/ khủng hoảng);

c) kiểm tra việc khôi phục kỹ thuật (đảm bảo các hệ thống thông tin có thể được khôi phục thực sự);

d) kiểm tra việc khôi phục tại một vị trí khác (chạy các quy trình nghiệp vụ song song với các hoạt động khôi phục ở xa vị trí chính);

e) các cuộc kiểm tra các phương tiện và dịch vụ của nhà cung cấp (đảm bảo rằng các dịch vụ và sản phẩm được cung cấp từ bên ngoài sẽ tuân theo cam kết trong hợp đồng);

f) hoàn tất các đợt diễn tập (kiểm tra để đảm bảo rằng tổ chức, cá nhân, thiết bị, các phương tiện và các quá trình có thể đối phó được với các gián đoạn).

Những kỹ thuật này có thể được sử dụng cho mọi tổ chức. Chúng phải được áp dụng theo cách phù hợp với kế hoạch khôi phục cụ thể. Các kết quả của các cuộc kiểm tra cần được ghi lại và các hoạt động cần được thực hiện nhằm cải tiến kế hoạch nếu cần thiết.

Trách nhiệm cần được phân định trong việc thường xuyên soát xét từng kế hoạch về sự liên tục của hoạt động nghiệp vụ. Sau khi xác định những thay đổi trong các hoạt động nghiệp vụ chưa được phản ánh trong các kế hoạch về sự liên tục của hoạt động nghiệp vụ thì phải cập nhật kế hoạch một cách phù hợp. Quá trình quản lý thay đổi chính thức này cần đảm bảo rằng các kế hoạch được cập nhật đều được phân phối và củng cố bằng các soát xét về toàn bộ kế hoạch một cách thường xuyên.

Các ví dụ về những thay đổi mà việc cập nhật các kế hoạch về sự liên tục của hoạt động nghiệp vụ cần phải được quan tâm là việc thu nhận thiết bị mới, nâng cấp các hệ thống và những thay đổi về:

a) nhân sự;

b) các địa chỉ và số điện thoại;

c) chiến lược nghiệp vụ;

d) vị trí, các phương tiện và các nguồn tài nguyên;

e) quy định pháp lý;

f) các nhà thầu, nhà cung cấp và khách hàng thân thiết;

g) các quy trình, hoặc mới hoặc bị thu hồi;

h) rủi ro (điều hành và tài chính).

14 Sự tuân thủ

14.1Sự tuân thủ các quy định pháp lý

Mục tiêu: Nhằm tránh sự vi phạm pháp luật, quy định, nghĩa vụ theo các hợp đồng đã ký kết, và tránh sự vi phạm các yêu cầu về đảm bảo an toàn thông tin.

Thiết kế, điều hành, sử dụng và quản lý các hệ thống thông tin có thể phải tuân theo các yêu cầu về an toàn thông tin của luật pháp, quy định, và giao kèo.

Có thể tìm thấy những tư vấn về các yêu cầu pháp lý cụ thể từ những cố vấn pháp luật của tổ chức, hoặc những người hành nghề về luật pháp có đủ khả năng phù hợp. Các yêu cầu pháp lý của các quốc gia cũng khác nhau và có thể thay đổi nếu thông tin được tạo ra ở một quốc gia nhưng lại được truyền sang một quốc gia khác (nghĩa là luồng dữ liệu chuyển qua biên giới).

14.1.1 Xác định các điều luật hiện đang áp dụng được

Biện pháp quản lý

Tất cả các yêu cầu về pháp lý, quy định, nghĩa vụ trong hợp đồng đã ký và cách tiếp cận của tổ chức để đáp ứng những yêu cầu này phải được xác định rõ ràng, ghi thành văn bản và được cập nhật thường xuyên.

Hướng dẫn triển khai

Các biện pháp quản lý cụ thể và các trách nhiệm của cá nhân để đáp ứng các yêu cầu này phải được xác định và được lập thành văn bản.

14.1.2 Quyền sở hữu trí tuệ (IPR)

Biện pháp quản lý

Các thủ tục phù hợp cần được triển khai nhằm đảm bảo sự phù hợp với các yêu cầu pháp lý, các quy định và cam kết theo hợp đồng trong việc sử dụng các tài liệu có quyền sở hữu trí tuệ và các sản phẩm phần mềm độc quyền.

Hướng dẫn triển khai

Các hướng dẫn sau cần được quan tâm để bảo vệ mọi tài liệu có quyền sở hữu trí tuệ:

a) công bố các quyền sở hữu trí tuệ phải tuân thủ theo chính sách trong đó xác định việc sử dụng hợp pháp các sản phẩm thông tin và phần mềm;

b) chỉ lấy phần mềm qua các nguồn quen biết và đáng tin cậy, nhằm đảm bảo rằng không vi phạm bản quyền;

c) duy trì nhận thức về các chính sách bảo vệ các quyền sở hữu trí tuệ, và đưa ra lưu ý về mục đích thực hiện hoạt động kỷ luật đối với các cá nhân vi phạm các chính sách;

d) duy trì đăng ký các tài sản phù hợp, và xác định tất cả các tài sản cùng các yêu cầu bảo vệ các quyền sở hữu trí tuệ;

e) duy trì chứng minh và chứng cứ về quyền sở hữu bản quyền, các đĩa điều khiển, sách hướng dẫn...;

f) triển khai các biện pháp quản lý nhằm đảm bảo rằng không bị vượt quá số lượng người dùng tối đa được phép;

g) thực hiện các cuộc kiểm tra để đảm bảo rằng chỉ các phần mềm được cấp phép và các sản phẩm có bản quyền mới được cài đặt;

h) cung cấp một chính sách duy trì các điều kiện bản quyền thích hợp;

i) cung cấp một chính sách bố trí hoặc chuyển phần mềm cho những người khác;

j) Sử dụng các công cụ đánh giá phù hợp;

k) tuân theo các điều khoản và điều kiện đối với phần mềm và thông tin lấy được từ các mạng công cộng;

l) không nhân bản, chuyển đổi sang dạng khác hoặc lấy từ các hồ sơ thương mại (phim ảnh, tiếng nói) trừ khi đã được phép;

m) không sao chép toàn bộ hoặc từng phần các sách, báo, báo cáo hoặc các dạng tài liệu khác trừ khi được luật bản quyền cho phép.

Thông tin khác

Các quyền sở hữu trí tuệ bao gồm bản quyền phần mềm hoặc tài liệu, các quyền thiết kế, đăng ký thương mại, bằng sáng chế, và các đăng ký mã nguồn.

Các sản phẩm phần mềm có bản quyền thường được cung cấp theo một thỏa thuận đăng ký nhằm xác định các điều khoản và điều kiện đăng ký, ví dụ, giới hạn sử dụng các sản phẩm chỉ với các máy móc cụ thể hoặc giới hạn sao chép chỉ cho các mục đích tạo ra các bản sao lưu. Trạng thái IPR của phần mềm do tổ chức phát triển sẽ đòi hỏi phải được công bố rõ ràng với đội ngũ nhân viên.

Các yêu cầu pháp lý, quy định và giao kèo có thể đặt ra những giới hạn trong việc sao chép các tài liệu có bản quyền. Cụ thể là, chúng có thể yêu cầu chỉ có các tài liệu được phát triển bởi tổ chức, hoặc được đăng ký bản quyền hoặc được cung cấp bởi người phát triển cho tổ chức, mới có thể được sử dụng. Sự vi phạm bản quyền có thể dẫn đến các hoạt động pháp lý, đó có thể là các cuộc kiện cáo có tính chất hình sự.

14.1.3 Bảo vệ các hồ sơ của tổ chức

Biện pháp quản lý

Các hồ sơ quan trọng cần được bảo vệ khỏi sự mất mát, phá hủy hoặc làm sai lệch, phù hợp với pháp luật, quy định, các nghĩa vụ trong hợp đồng đã ký.

Hướng dẫn triển khai

Các hồ sơ cần được phân loại theo loại hồ sơ, ví dụ hồ sơ kế toán, hồ sơ cơ sở dữ liệu, nhật ký giao dịch, nhật ký đánh giá, và các thủ tục điều hành, mỗi hồ sơ đều có các thông tin chi tiết về các giai đoạn sử dụng và loại phương tiện lưu trữ, ví dụ giấy, phim, từ, quang. Mọi tài liệu có khóa mã hóa liên quan và các chương trình liên quan đến các văn bản được mã hóa hoặc chữ ký số (xem 11.3), cần được lưu trữ để có thể giải mã các hồ sơ.

Cần xem xét khả năng hư hỏng thiết bị được sử dụng để lưu trữ các hồ sơ. Các thủ tục lưu trữ và xử lý cần được triển khai theo các hướng dẫn của nhà sản xuất. Nếu cần lưu trữ trong thời gian dài thì nên xem xét sử dụng giấy hoặc tấm vi phim.

Trường hợp thiết bị lưu trữ điện tử được lựa chọn thì các thủ tục nhằm đảm bảo khả năng truy cập dữ liệu (cả khả năng đọc phương tiện và định dạng) trong toàn bộ quá trình lưu trữ cũng cần được đưa ra nhằm bảo vệ an toàn trước những mất mát do sự thay đổi công nghệ trong tương lai.

Các hệ thống lưu trữ dữ liệu cần được chọn lựa sao cho dữ liệu được yêu cầu có thể lấy lại định dạng và khung thời gian trong mức có thể chấp nhận được, tùy theo các yêu cầu phải thỏa mãn.

Nếu thích hợp thì hệ thống lưu trữ và xử lý cần đảm bảo định danh rõ các hồ sơ và thời gian lưu trữ chúng như đã được xác định bởi các yêu cầu pháp lý, quy định của quốc gia hoặc khu vực. Hệ thống này phải cho phép hủy bỏ các hồ sơ một cách phù hợp sau thời gian lưu trữ đó nếu chúng không cần thiết cho tổ chức nữa.

Để thỏa mãn các mục tiêu bảo vệ hồ sơ, các bước sau đây cần được thực hiện trong nội bộ tổ chức:

a) đưa ra các hướng dẫn về việc sử dụng, lưu trữ, xử lý và loại bỏ các hồ sơ và thông tin;

b) kế hoạch lưu trữ cần được phác thảo nhằm xác định các hồ sơ và khoảng thời gian lưu trữ chúng;

c) việc kiểm kê các nguồn tài nguyên của các thông tin quan trọng cần được duy trì;

d) các biện pháp quản lý phù hợp cần được triển khai nhằm bảo vệ các hồ sơ và thông tin khỏi bị mất, phá hủy và làm giả.

Thông tin khác

Một số hồ sơ có thể cần được lưu giữ an toàn để tuân thủ các yêu cầu pháp lý, quy định hoặc giao kèo, cũng như để hỗ trợ các hoạt động nghiệp vụ cần thiết. Ví dụ các hồ sơ có thể được yêu cầu là chứng cứ cho thấy tổ chức hoạt động tuân theo các quy định hoặc các yêu cầu pháp lý, nhằm đảm bảo sự phòng thủ thích đáng trước các hành động dân sự hoặc hình sự tiềm ẩn, hoặc để xác nhận tình trạng tài chính của một tổ chức trước các cổ đông, các bên liên quan, và các đánh giá viên. Khoảng thời gian và nội dung dữ liệu cần lưu trữ thông tin có thể được quy định bởi các điều luật hoặc quy tắc quốc gia.

Thông tin sâu hơn về việc quản lý các hồ sơ của tổ chức có thể tìm thấy trong ISO 15489-1.

14.1.4 Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân

Biện pháp quản lý

Việc bảo vệ dữ liệu và tính riêng tư cần được đảm bảo theo yêu cầu pháp lý, quy định, và cả các điều *khoản trong hợp đồng nếu có.*

Hướng dẫn triển khai

Chính sách về sự riêng tư và bảo vệ dữ liệu của tổ chức cần được phát triển và triển khai. Chính sách này cần được phổ biến cho tất cả các nhân viên tham gia vào việc xử lý thông tin cá nhân.

Việc tuân thủ chính sách này và tất cả các yêu cầu pháp lý và quy định về bảo vệ dữ liệu có liên quan đòi hỏi cơ cấu và biện pháp quản lý phù hợp. Thông thường cách tốt nhất để đạt được điều này là chỉ định trách nhiệm cá nhân, ví dụ chỉ định ra một nhân viên bảo vệ dữ liệu, người này phải đưa ra hướng dẫn cho những người quản lý, người dùng, và các nhà cung cấp dịch vụ trên cơ sở các trách nhiệm cá *nhân của họ và các thủ tục cần phải tuân theo. Trách nhiệm đối với việc xử lý thông tin cá nhân và đảm* bảo nhận thức về các nguyên tắc bảo vệ dữ liệu cần được đề cập phù hợp tuân theo các yêu cầu pháp

lý và các quy định. Các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ thông tin cá nhân cũng cần được triển khai.

Thông tin khác

Một số nước đã đưa ra quy định pháp lý về các biện pháp quản lý việc thu thập, xử lý, và chuyển giao dữ liệu cá nhân (nhìn chung, thông tin về những người còn sống có thể được xác định từ các thông tin đó). Tùy thuộc vào các quy định pháp lý riêng của từng quốc gia mà các biện pháp quản lý có thể áp đặt các nhiệm vụ lên những cá nhân thu thập, xử lý, và phổ biến thông tin cá nhân, và có thể hạn chế khả năng truyền dữ liệu đó tới nước khác.

14.1.5 Ngăn ngừa việc lạm dụng phương tiện xử lý thông tin

Biện pháp quản lý

Cần ngăn chặn người dùng khỏi việc sử dụng các phương tiện xử lý thông tin vào mục đích không được phép.

Hướng dẫn triển khai

Ban quản lý cần thông qua việc sử dụng các phương tiện xử lý thông tin. Mọi sự sử dụng các phương tiện này cho các mục đích phi nghiệp vụ mà chưa có sự thông qua của ban quản lý (xem 5.1.4), hoặc cho các mục đích trái phép, đều được coi là sử dụng các phương tiện một cách không phù hợp. Nếu bất kỳ hoạt động trái phép nào được xác định bởi quá trình giám sát hoặc bởi các biện pháp khác thì hoạt động này cần được đưa vào diện lưu ý của người quản lý, trong đó cần quan tâm đến biện pháp xử phạt thỏa đáng và/hoặc hoạt động pháp lý.

Cần có sự tư vấn pháp lý trước khi triển khai các thủ tục giám sát.

Mọi người dùng đều phải nhận thức được phạm vi truy cập được phép của họ và việc giám sát nhằm phát hiện sự sử dụng trái phép. Họ có thể được cấp cho một giấy phép, mà bản sao của nó sẽ được người dùng ký vào và được tổ chức lưu giữ một cách an toàn. Các nhân viên của tổ chức, người của nhà thầu và bên thứ ba cần được tư vấn là không được truy cập trừ khi truy cập đó đã được cấp phép.

Tại thời điểm đăng nhập, cần có một thông điệp cảnh báo chỉ ra rằng phương tiện xử lý thông tin đang được truy cập là thuộc quyền sở hữu của tổ chức và sự truy cập chưa được cấp phép sẽ bị cấm. Người dùng phải hiểu biết và phản ứng một cách phù hợp với thông điệp trên màn hình để tiếp tục quá trình đăng nhập (xem 10.5.1).

Thông tin khác

Các phương tiện xử lý thông tin của một tổ chức thường dành riêng và trước tiên cho các mục đích nghiệp vụ.

Các công cụ phát hiện vi phạm, kiểm tra nội dung, và các công cụ giám sát khác có thể giúp ngăn ngừa và phát hiện sự lạm dụng các phương tiện xử lý thông tin.

Rất nhiều nước đã có các quy định pháp lý trong việc bảo vệ chống lại việc lạm dụng máy tính. Đó có thể là sự vi phạm có tính chất hình sự trong việc sử dụng máy tính cho những mục đích trái phép.

Tính pháp lý của việc giám sát sự sử dụng cũng khác nhau giữa các quốc gia và có thể đòi hỏi ban quản lý phải tư vấn cho mọi người dùng về việc giám sát và/hoặc để nhận được sự chấp thuận của họ. Nếu hệ thống đang được truy cập được sử dụng cho truy cập công cộng (ví dụ dịch vụ web công cộng) và là đối tượng cần giám sát an toàn bảo mật thì cần đưa ra một thông điệp thông báo về điều đó.

14.1.6 Quy định về quản lý mã hóa

Biện pháp quản lý

Quản lý mã hóa cần được áp dụng phù hợp với các thỏa thuận, luật pháp và các quy định liên quan.

Hướng dẫn triển khai

Những vấn đề sau cần được quan tâm nhằm tuân thủ các thỏa thuận, luật pháp và quy định liên quan:

a) các hạn chế về việc nhập và/hoặc xuất phần mềm và phần cứng máy tính để thực hiện các chức năng mã hóa;

b) các hạn chế về việc nhập và/hoặc xuất phần mềm và phần cứng máy tính được thiết kế để bổ sung các chức năng mã hóa;

c) các hạn chế về việc sử dụng mã hóa;

d) các phương pháp bắt buộc hoặc tùy chọn về truy cập được thực hiện bởi các quan chức quốc gia tới thông tin được mã hóa bởi phần cứng hoặc phần mềm để có được sự bí mật về nội dung.

Cần có tư vấn pháp lý để đảm bảo sự tuân thủ các luật lệ và quy định của quốc gia. Trước khi thông tin đã mã hóa hoặc các biện pháp quản lý mã hóa được chuyển sang quốc gia khác thì cũng cần có sự tư vấn pháp lý.

14.2 Sự tuân thủ các chính sách và tiêu chuẩn an toàn, và tương thích kỹ thuật

Mục tiêu: Nhằm đảm bảo sự tuân thủ của hệ thống theo các chính sách và tiêu chuẩn an toàn của tổ chức.

Sự an toàn của các hệ thống thông tin cần được soát xét định kỳ.

Các soát xét như vậy phải được thực hiện theo các chính sách an toàn thông tin phù hợp và các nền tảng kỹ thuật, các hệ thống thông tin cần được đánh giá sự tuân thủ theo các tiêu chuẩn triển khai an toàn thông tin hiện hành và các biện pháp quản lý an toàn thông tin đã được lập thành văn bản.

14.2.1 Sự tuân thủ các tiêu chuẩn và chính sách an toàn

Biện pháp quản lý

Người quản lý cần đảm bảo rằng mọi thủ tục đảm bảo an toàn trong phạm vi trách nhiệm của mình đều được thực hiện chính xác để đạt được kết quả phù hợp với các chính sách cũng như các tiêu chuẩn an toàn.

Hướng dẫn triển khai

Ban quản lý cần soát xét định kỳ sự tuân thủ về xử lý thông tin theo các chính sách, tiêu chuẩn an toàn và các yêu cầu an toàn khác trong phạm vi trách nhiệm của mình.

Nếu khi soát xét tìm thấy bất cứ sự không tuân thủ nào thì ban quản lý cần:

a) xác định nguyên nhân của sự không tuân thủ;

b) đánh giá nhu cầu cần có các hoạt động để đảm bảo sự không tuân thủ sẽ không tái diễn;

c) xác định và triển khai hoạt động phòng ngừa thích hợp;

d) soát xét lại hoạt động phòng ngừa đã được thực hiện.

Các kết quả của việc soát xét và các hoạt động phòng ngừa đã được thực hiện bởi những người quản lý cần được ghi lại và các báo cáo này cần được lưu lại. Những người quản lý phải báo cáo các kết quả đến những người thực hiện các soát xét độc lập (xem 5.1.8) nếu việc soát xét độc lập diễn ra trong phạm vi thuộc trách nhiệm của họ.

Thông tin khác

Nội dung giám sát điều hành việc sử dụng hệ thống đã được đề cập trong 9.10.

14.2.2 Kiểm tra sự tương thích kỹ thuật

Biện pháp quản lý

Các hệ thống thông tin cần được kiểm tra thường xuyên sự tuân thủ các tiêu chuẩn thực hiện an toàn.

Hướng dẫn triển khai

Việc kiểm tra tuân thủ kỹ thuật cần được thực hiện bằng tay (nếu cần phải được hỗ trợ bởi các công cụ phần mềm phù hợp) bởi một kỹ sư hệ thống có kinh nghiệm, và/hoặc với sự hỗ trợ của các công cụ tự động, các công cụ này sẽ cung cấp một bản báo cáo kỹ thuật mà sau này sẽ được giải thích bởi một chuyên gia kỹ thuật.

Nếu thực hiện các cuộc kiểm tra thâm nhập hoặc các cuộc đánh giá điểm yếu thì cần thận trọng vì các hoạt động như vậy có thể gây tổn hại đến sự an toàn của hệ thống. Những cuộc kiểm tra này cần được lên kế hoạch, được lập thành văn bản và có thể lặp lại.

Mọi cuộc kiểm tra tuân thủ kỹ thuật đều chỉ được thực hiện bởi những người nhân viên có trình độ, có thẩm quyền, hoặc dưới sự giám sát của những nhân viên như vậy.

Thông tin khác

Kiểm tra tuân thủ kỹ thuật phải thực hiện trên các hệ thống vận hành nhằm đảm bảo rằng các biện pháp quản lý phần cứng và phần mềm đều được thực hiện đúng. Loại kiểm tra tuân thủ này đòi hỏi phải được thực hiện bởi những chuyên gia kỹ thuật thành thạo.

Kiểm tra tuân thủ cũng bao gồm, ví dụ, các cuộc kiểm tra xâm nhập và các cuộc đánh giá điểm yếu, các cuộc kiểm tra này có thể được thực hiện bởi những chuyên gia độc lập đã được ký hợp đồng thực hiện mục đích này. Cách đó có thể rất hữu ích trong việc phát hiện các điểm yếu của hệ thống và kiểm tra xem các biện pháp quản lý có hiệu quả trong việc ngăn chặn truy cập trái phép do những điểm yếu này không.

Việc kiểm tra sự xâm nhập và đánh giá các điểm yếu sẽ cung cấp đánh giá chung về hệ thống trong một trạng thái nhất định vào một thời điểm nhất định. Sự đánh giá này được giới hạn cho các phần của hệ thống thực sự đã được kiểm tra trong mọi nỗ lực xâm nhập. Việc kiểm tra xâm nhập và đánh giá điểm yếu không thể thay thế việc đánh giá rủi ro.

14.3 Xem xét việc đánh giá các hệ thống thông tin

Mục tiêu: Nhằm tối ưu hóa và giảm thiểu những ảnh hưởng xấu từ/tới quá trình đánh giá các hệ thống thông tin.
Cần có các biện pháp quản lý nhằm bảo vệ an toàn cho các hệ thống vận hành và các công cụ đánh giá trong khi đánh giá các hệ thống thông tin.
Việc bảo vệ cũng được yêu cầu nhằm bảo vệ tính toàn vẹn và ngăn ngừa sự lạm dụng các công cụ đánh giá.

14.3.1 Các biện pháp quản lý đánh giá các hệ thống thông tin

Biện pháp quản lý

Các yêu cầu và hoạt động đánh giá các hệ thống vận hành cần được hoạch định thận trọng và thống nhất nhằm hạn chế rủi ro hoặc sự đổ vỡ của các quy trình hoạt động nghiệp vụ.

Hướng dẫn triển khai

Những hướng dẫn sau cần được quan tâm:

a) các yêu cầu đánh giá cần được thông qua với ban quản lý;

b) phạm vi của các cuộc kiểm tra cần được thông qua và quản lý;

c) các cuộc kiểm tra cần được giới hạn chỉ truy cập đọc tới phần mềm và dữ liệu;

d) các truy cập khác ngoài truy cập chỉ đọc chỉ được cho phép đối với các bản sao đã được phân tách của các tệp tin hệ thống, các bản sao này phải được xóa bỏ khi việc đánh giá đã hoàn tất hoặc được bảo vệ phù hợp nếu có nghĩa vụ phải giữ lại các tệp tin đó theo các yêu cầu của hồ sơ đánh giá;

e) các nguồn tài nguyên sử dụng để thực thi các cuộc kiểm tra phải được xác định rõ và sẵn sàng;

f) các yêu cầu về xử lý đặc biệt hoặc xử lý thêm cũng cần được xác định rõ và được thông qua;

g) mọi truy cập đều phải được giám sát và ghi lại để cung cấp vết tham chiếu; việc sử dụng các *vết tham chiếu theo thời gian cần được xem xét đối với các hệ thống hoặc dữ liệu quan trọng;*

h) mọi thủ tục, yêu cầu và trách nhiệm đều phải được lập thành văn bản;

i) (những) người thực hiện đánh giá cần độc lập với các hoạt động cần đánh giá.

14.3.2 Bảo vệ các công cụ đánh giá hệ thống thông tin

Biện pháp quản lý

Truy cập tới các công cụ đánh giá hệ thống thông tin cần được bảo vệ khỏi mọi sự lạm dụng hoặc lợi dụng.

Hướng dẫn triển khai

Các công cụ đánh giá hệ thống thông tin, ví dụ, các phần mềm hoặc tệp dữ liệu, cần được cách ly với các hệ thống vận hành và phát triển và không được giữ trong các thư viện băng ghi âm hoặc các khu vực có người dùng, trừ khi được bảo vệ ở mức độ phù hợp.

Thông tin khác

Nếu công việc đánh giá có sự tham gia của các bên thứ ba thì có thể xuất hiện rủi ro do các bên thứ ba lạm dụng các công cụ đánh giá và truy cập vào thông tin. Các biện pháp quản lý như 5.2.1 (để đánh giá rủi ro) và 8.1.2 (để hạn chế truy cập vật lý) có thể cần được quan tâm để giải quyết rủi ro này và mọi hậu quả của nó, ví dụ ngay lập tức thay đổi các mật khẩu đã được tiết lộ cho các nhân viên đánh giá.

Thư mục tài liệu tham khảo

[1] ISO/IEC Guide 2:1996, Standardization and related activities -- General vocabulary

[2] ISO/IEC Guide 73:2002, Risk management -- Vocabulary -- Guidelines for use in standards

[3] ISO/IEC 13335-1:2004, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management

[4] ISO/IEC TR 13335-3:1998, Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security

[5] ISO/IEC 13888-1:1997, Information technology -- Security techniques -- Non-repudiation -- Part 1: General

[6] ISO/IEC 11770-1:1996, Information technology -- Security techniques -- Key management -- Part 1: Framework

[7] ISO/IEC 9796-2:2002, Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[8] ISO/IEC 9796-3:2000, Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms

[9] ISO/IEC 14888-1:1998, Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General

[10] ISO/IEC 15408-1:1999, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

[11] ISO/IEC TR 14516:2002, Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services

[12] BS ISO 15489-1:2001, Information and documentation - Records management – Part 1: General

[13] ISO 10007:2003, Guidelines for Configuration Management.

[14] ISO/IEC 12207:1995, Information technology -- Software life cycle processes

[15] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[16] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

[17] OECD Guidelines for Cryptography Policy, 1997

[18] IEEE P1363 – 2000, Standard Specifications for Public-Key Cryptography

[19] ISO/IEC 18028-4, Information technology -- Security techniques – IT Netwwork security - Part 4: Securing remote access

[20] ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.