TCVN TIÊU CHUẨN QUỐC GIA

TCVN 7562 : 2005
ISO/IEC 17799 : 2000

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – MÃ THỰC HÀNH QUẢN LÝ AN NINH THÔNG TIN

Information technology — Code of practice for information security management

HÀ NỘI – 2008

Mục lục Trang

Lời nói đầu

TCVN 7562 : 2005 hoàn toàn tương đương với **ISO/IEC 17799 : 2000**.

TCVN 7562 : 2005 do Ban kỹ thuật tiêu chuẩn TCVN/TC 154 *"Quá trình, các yếu tố dữ liệu và tài liệu trong thương mại, công nghiệp và hành chính"* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ ban hành.

Tiêu chuẩn này được chuyển đổi năm 2008 từ Tiêu chuẩn Việt Nam cùng số hiệu thành Tiêu chuẩn Quốc gia theo quy định tại Khoản 1 Điều 69 của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật và điểm a khoản 1 Điều 6 Nghị định số 127/2007/NĐ-CP ngày 1/8/2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

Công nghệ thông tin – Mã thực hành quản lý an ninh thông tin

Information Technology — Code of practice for information security management

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra các khuyến nghị về công tác quản lý an ninh thông tin cho những người có trách nhiệm cài đặt, thực thi hoặc duy trì an ninh trong tổ chức của họ. Tiêu chuẩn này nhằm cung cấp một cơ sở chung để xây dựng các tiêu chuẩn an ninh trong tổ chức và thực hành quản lý an ninh một cách hiệu quả và tạo tính tin cậy trong các giao dịch liên-tổ chức. Các khuyến nghị rút ra từ tiêu chuẩn này nên được lựa chọn và sử dụng phù hợp với các luật và các quy định liên quan.

2 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa sau:

2.1 An ninh thông tin

Duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin.

- **Tính bảo mật**

Đảo bảo rằng chỉ người được phép mới có thể truy cập thông tin.

- **Tính toàn vẹn**

Bảo vệ tính chính xác và đầy đủ của thông tin và các phương pháp xử lý.

- **Tính sẵn sàng**

Đảm bảo rằng người sử dụng được phép có thể truy cập thông tin và các tài sản tương ứng khi cần.

2.2 Đánh giá rủi ro

Đánh giá các mối đe dọa, những ảnh hưởng và điểm yếu của thông tin và các phương tiện xử lý thông tin cũng như khả năng có thể xảy ra.

2.3 Quản lý rủi ro

Quá trình xác định, kiểm soát và giảm thiểu hoặc loại trừ các rủi ro an ninh có thể ảnh hưởng đến các hệ thống thông tin với chi phí có thể chấp nhận được.

3 Chính sách an ninh

3.1 Chính sách an ninh thông tin

Mục tiêu: Cung cấp phương hướng quản lý và hỗ trợ an ninh thông tin. Ban quản lý nên thiết lập một phương hướng chính sách rõ ràng và công khai hỗ trợ và cam kết an ninh thông tin thông qua việc phát hành và duy trì một chính sách an ninh thông tin trong toàn tổ chức.

3.1.1 Tài liệu chính sách an ninh thông tin

Tài liệu chính sách nên được ban quản lý thông qua, được phát hành và truyền đạt cho toàn bộ nhân viên khi thích hợp. Bản chính sách này nên công bố cam kết của ban quản lý và trình bày cách tiếp cận quản lý an ninh thông tin của tổ chức một cách ngắn gọn, tối thiểu nó nên bao gồm hướng dẫn sau:

a) định nghĩa về an ninh thông tin, toàn bộ đối tượng, phạm vi của nó và tầm quan trọng của an ninh như một cơ chế tạo điều kiện cho việc chia sẻ thông tin;

b) trình bày mục đích quản lý, hỗ trợ các mục tiêu và nguyên tắc về an ninh thông tin;

c) giải thích ngắn gọn các chính sách, nguyên tắc, tiêu chuẩn an ninh và tuân thủ các yêu cầu có tầm quan trọng đặc biệt đối với tổ chức, ví dụ:

   1) tuân thủ các yêu cầu pháp lý và theo hợp đồng;

   2) các yêu cầu giáo dục an ninh;

   3) ngăn ngừa và phát hiện các virút và phần mềm gây hại khác;

   4) quản lý tính liên tục của công việc kinh doanh;

   5) các hậu quả của các vi phạm chính sách an ninh;

d) xác định các trách nhiệm chung và riêng cho việc quản lý an ninh thông tin, gồm cả việc báo cáo các sự cố an ninh;

e) tham chiếu tới tài liệu có thể hỗ trợ cho chính sách, ví dụ các chính sách và thủ tục an ninh chi tiết hơn cho các hệ thống thông tin cụ thể hoặc các quy tắc an ninh mà người sử dụng phải tuân theo.

Chính sách này nên được truyền đạt trong toàn tổ chức tới những người sử dụng ở dạng thích hợp mà người đọc có thể thu nhận và hiểu được.

3.1.2 Soát xét và đánh giá

Nên có một người chịu trách nhiệm chính trong việc duy trì và soát xét chính sách này theo một quy trình soát xét định trước. Quy trình đó nên đảm bảo rằng việc soát xét được thực hiện để đáp ứng với bất kỳ thay đổi nào ảnh hưởng tới cơ sở của sự đánh giá rủi ro ban đầu, ví dụ các sự cố an ninh đáng lưu ý, các điểm yếu hoặc các thay đổi mới đối với cơ sở hạ tầng tổ chức hoặc kỹ thuật.

Các soát xét định kỳ cũng nên lập chương trình các vấn đề sau:

a) tính hiệu lực của chính sách, được chứng tỏ bằng bản chất, số lượng và ảnh hưởng của các sự cố an ninh được ghi lại;

b) chi phí và ảnh hưởng của các kiểm soát tính hiệu quả kinh doanh;

c) tác động của các thay đổi tới công nghệ.

4 An ninh tổ chức

4.1 Hạ tầng an ninh thông tin

Mục tiêu: Quản lý an ninh thông tin trong tổ chức. Khuôn khổ quản lý nên được thiết lập để khởi đầu và kiểm soát việc thực hiện an ninh thông tin trong tổ chức. Các diễn đàn quản lý phù hợp với khả năng lãnh đạo của ban quản lý nên được thành lập để thông qua chính sách an ninh thông tin, ấn định các vai trò an ninh và phối hợp thực hiện an ninh trong toàn bộ tổ chức. Nếu cần thiết, một nguồn tài nguyên các lời khuyên chuyên môn về an ninh thông tin nên được thiết lập và sẵn dùng trong tổ chức. Nên phát triển việc cộng tác với các chuyên gia an ninh bên ngoài để theo kịp các xu hướng công nghiệp, các tiêu chuẩn giám sát, phương pháp đánh giá và cung cấp các điểm liên lạc phù hợp khi xử lý các sự cố an ninh. Nên khuyến khích sử dụng cách tiếp cận an ninh thông tin đa chiều, ví dụ bao gồm sự phối hợp và hợp tác của các nhà quản lý, người sử dụng, nhà quản trị, người thiết kế ứng dụng, kiểm toán viên và nhân viên an ninh và các chuyên gia có kỹ năng chuyên môn trong nhiều lĩnh vực như bảo hiểm và quản lý rủi ro.

4.1.1 Diễn đàn quản lý an ninh thông tin

An ninh thông tin là một trách nhiệm của doanh nghiệp được toàn bộ các thành viên của nhóm quản lý tham gia. Một diễn đàn quản lý nên được quan tâm để đảm bảo rằng có phương hướng rõ ràng và sự quản lý hữu hình hỗ trợ cho các sáng kiến an ninh. Diễn đàn đó nên thúc đẩy an ninh trong tổ chức thông qua sự cam kết thích hợp và sáng kiến tương xứng.

Diễn đàn này có thể là một phần của cơ quan quản lý. Điển hình là một diễn đàn bảo đảm trách nhiệm sau đây:

a) soát xét và phê duyệt chính sách an ninh thông tin và toàn bộ người có trách nhiệm;

b) kiểm tra các thay đổi quan trọng trong tình trạng phơi bày tài sản thông tin đối với các mối đe dọa chính;

c) soát xét và kiểm tra các sự cố an ninh thông tin;

d) phê duyệt các sáng kiến để tăng cường an ninh thông tin.

Một nhà quản lý nên có trách nhiệm đối với toàn bộ các hoạt động liên quan đến an ninh.

4.1.2 Hợp tác về an ninh thông tin

Trong một tổ chức lớn, một diễn đàn chức năng-chéo của các đại diện quản lý từ các bộ phận liên quan của tổ chức đó có thể cần thiết phối hợp thực hiện các kiểm soát an ninh thông tin. Điển hình là diễn đàn:

a) đồng ý các vai trò và trách nhiệm cụ thể đối với an ninh thông tin trên toàn bộ tổ chức;

b) đồng ý các phương pháp luận và quy trình cụ thể đối với an ninh thông tin, nghĩa là; đánh giá rủi ro, hệ thống phân loại an ninh;

c) đồng ý và hỗ trợ các sáng kiến an ninh thông tin của tổ chức mở rộng, nghĩa là; chương trình nhận thức về an ninh;

d) đảm bảo rằng an ninh một phần của quy trình lập kế hoạch thông tin;

e) đánh giá sự tương xứng và phối hợp thực hiện các kiểm soát an ninh thông tin cụ thể đối với các hệ thống hoặc dịch vụ mới;

f) soát xét các sự cố về an ninh thông tin;

g) thúc đẩy tính minh bạch của việc hỗ trợ an ninh thông tin của doanh nghiệp trong toàn bộ tổ chức.

4.1.3 Phân định trách nhiệm về an ninh thông tin

Các trách nhiệm đối với việc bảo vệ các tài sản cá nhân và tiến hành các quy trình an ninh cụ thể nên được xác định rõ ràng.

Chính sách an ninh thông tin (xem mục 3) nên cung cấp hướng dẫn chung trong việc phân định các vai trò và trách nhiệm an ninh trong tổ chức. Điều này nên được bổ sung, khi cần thiết, cùng với hướng dẫn chi tiết hơn đối với các địa điểm, hệ thống hoặc dịch vụ cụ thể. Các trách nhiệm cục bộ đối với các tài sản vật chất và thông tin cá nhân và các quá trình an ninh, như việc lập kế hoạch liên tục kinh doanh nên được xác định rõ ràng.

Trong nhiều tổ chức, một nhà quản lý an ninh thông tin sẽ được bổ nhiệm để nắm giữ toàn bộ trách nhiệm đối với việc phát triển và thực hiện an ninh và để hỗ trợ việc xác định kiểm soát.

Tuy nhiên, trách nhiệm đối với sáng kiến và thực hiện các kiểm soát thường giữ nguyên cho các nhà quản lý cá nhân. Một thực tế chung là để bổ nhiệm một người chủ sở hữu đối với mỗi tài sản thông tin thì người đó trở thành người có trách nhiệm hàng ngày đối với an ninh.

Người chủ sở hữu các tài sản thông tin có thể uỷ quyền các trách nhiệm về an ninh của họ cho các nhà quản lý cá nhân hoặc các nhà cung cấp dịch vụ. Tuy nhiên người chủ đó vẫn còn trách nhiệm đối với an ninh của tài sản đó và nên có khả năng xác nhận bất kỳ sự chịu trách nhiệm được uỷ quyền đều đã hoàn thành đúng.

Điều cần thiết là các phạm vi cho mỗi nhà quản lý là trách nhiệm được chỉ rõ; đặc biệt các sự việc sau đây xảy ra:

a) các tài sản khác nhau và các quy trình an ninh được kết hợp với mỗi hệ thống cá nhân nên được định danh và xác định rõ ràng;

b) nhà quản lý có trách nhiệm đối với mỗi tài sản hoặc quy trình an ninh nên được thỏa thuận và các chi tiết của trách nhiệm này nên được tài liệu hóa;

c) các mức cấp phép nên được xác định rõ ràng và được tài liệu hóa.

4.1.4 Quyền xử lý các phương tiện xử lý thông tin

Một quy trình cấp phép của quản lý đối với các phương tiện xử lý thông tin mới nên được thiết lập.

Nên xem xét các kiểm soát sau đây:

a) các phương tiện mới nên có sự phê chuẩn quản lý người sử dụng thích hợp, căn cứ vào mục đích và việc sử dụng của họ. Sự phê chuẩn cũng nên đạt được từ Nhà quản lý có trách nhiệm đối với việc duy trì môi trường an ninh của hệ thống thông tin cục bộ để đảm bảo rằng toàn bộ các chính sách và yêu cầu về an ninh liên quan được đáp ứng;

b) khi cần thiết, phần cứng và phần mềm nên được kiểm tra để đảm bảo rằng chúng có thể so sánh với các thành phần hệ thống khác;

CHÚ THÍCH: Có thể đòi hỏi kiểu phê chuẩn đối với các kết nối cụ thể.

c) việc sử dụng các phương tiện xử lý thông tin cá nhân đối với việc xử lý thông tin doanh nghiệp và bất kỳ các kiểm soát cần thiết nên được cấp phép;

d) việc sử dụng các phương tiện xử lý thông tin cá nhân trong nơi làm việc có thể dẫn đến các điểm dễ bị tấn công mới vì vậy nên được đánh giá và cho phép.

Các kiểm soát này đặc biệt quan trọng trong một môi trường được nối mạng.

4.1.5 Lời khuyên của chuyên gia về an ninh thông tin

Lời khuyên về an ninh của chuyên gia hầu như bị phụ thuộc bởi nhiều tổ chức. Theo lý tưởng, một cố vấn an ninh thông tin tiến hành trong một tổ chức có kinh nghiệm nên cung cấp lời khuyên. Không phải toàn bộ các tổ chức đều có thể muốn thuê một chuyên gia cố vấn. Trong các trường hợp như vậy, khuyến cáo rằng một cá nhân cụ thể được định danh để phối hợp các kiến thức và kinh nghiêm tiến hành trong tổ chức để đảm bảo tính nhất quán và cung cấp hỗ trợ trong việc tạo quyết định an ninh.

Họ cũng nên có quyền sử dụng các cố vấn phù hợp ở bên ngoài để cung cấp lời khuyên chuyên gia ngoài kinh nghiệm của chính họ.

Các cố vấn an ninh thông tin hoặc các điểm liên lạc tương đương nên được giao nhiệm vụ với việc cung cấp lời khuyên trên toàn bộ các khía cạnh của an ninh thông tin, có sử dụng hoặc của chính họ hoặc lời khuyên bên ngoài. Chất lượng của việc đánh giá các mối đe dọa an ninh và lời khuyên trên các kiểm soát sẽ xác định tính hiệu lực của an ninh thông tin của tổ chức. Để tính hiệu lực và sự tác động là tối đa thì chúng nên được phép trực tiếp có quyền sử dụng quản lý trong toàn bộ tổ chức.

Cố vấn an ninh thông tin hoặc điểm liên lạc tương đương nên được tư vấn ở giai đoạn sớm nhất có thể theo sau một vấn đề sự cố an ninh hoặc lỗ thủng an ninh khả nghi để cung cấp một nguồn hướng dẫn của chuyên gia hoặc các nguồn điều tra. Mặc dù phần lớn các điều tra an ninh nội bộ thông thường sẽ

được tiến hành dưới kiểm soát quản lý, cố vấn an ninh thông tin có thể được đề nghị đưa ra lời khuyên, hướng dẫn hoặc thực hiện cuộc điều tra đó.

4.1.6 Hợp tác giữa các tổ chức

Các liên lạc thích hợp với các ủy quyền hợp pháp, các cơ quan quy định, các nhà cung cấp dịch vụ thông tin và các nhà điều hành viễn thông nên được duy trì để đảm bảo rằng hành động thích hợp có thể được thực hiện một cách nhanh chóng và đạt được lời khuyên, trong trường hợp của một vấn đề sự cố an ninh. Tương tự, thành viên của các nhóm an ninh và các diễn đàn công nghiệp nên được xem xét.

Các trao đổi của thông tin an ninh nên được hạn chế để đảm bảo rằng thông tin bí mật của tổ chức đó không được chuyển cho các cá nhân trái phép.

4.1.7 Soát xét độc lập của an ninh thông tin

Tài liệu về chính sách an ninh thông tin (xem 3.1) trình bày chính sách và các trách nhiệm đối với an ninh thông tin. Việc thi hành nó nên được soát xét một cách độc lập để cung cấp sự bảo đảm rằng các hoạt động thực tế của tổ chức phản ánh một cách đúng đắn chính sách và nó có tính khả thi và hiệu quả (xem 12.2).

Một soát xét như vậy có thể được tiến hành bằng chức năng đánh giá nội bộ, một nhà quản lý độc lập hoặc một tổ chức thứ ba tiến hành soát xét đó. Ở đây, các ứng cử viên này có các kỹ năng và kinh nghiệm thích hợp.

4.2 Anh ninh đối với sự truy cập của bên thứ ba

Mục tiêu: Duy trì an ninh cho các phương tiện xử lý thông tin của tổ chức và các tài sản thông tin do các bên thứ ba truy cập.
Việc truy cập tới các phương tiện xử lý thông tin của tổ chức bởi các bên thứ ba nên được kiểm soát.
Ở những chỗ có nhu cầu kinh doanh với việc truy cập của bên thứ ba, đánh giá rủi ro nên được tiến hành để xác định các vấn đề liên quan đến an ninh và các yêu cầu kiểm soát. Các kiểm soát nên được thỏa thuận và xác định rõ trong hợp đồng với bên thứ ba.
Việc truy cập của bên thứ ba cũng có thể liên quan đến các bên tham gia khác. Các hợp đồng cho phép việc truy cập của bên thứ ba nên gồm việc xem xét sự chỉ định các bên tham gia có đủ tư cách khác và các điều kiện truy cập của họ.
Tiêu chuẩn này có thể được sử dụng như một cơ sở đối với các hợp đồng như vậy và khi xem xét nguồn cung cấp cho việc xử lý thông tin.

4.2.1 Xác định các rủi ro từ việc truy cập của bên thứ ba

4.2.1.1 Các kiểu truy cập

Kiểu truy cập của bên thứ ba có tầm quan trọng đặc biệt. Ví dụ, các rủi ro của việc truy cập thông qua một kết nối mạng là khác với các rủi ro truy cập vật lý.

Các kiểu truy cập nên được xem xét là:

a) truy cập vật lý, ví dụ tới các văn phòng, phòng máy tính, tủ hồ sơ;

b) truy cập logic, ví dụ tới các cơ sở dữ liệu, hệ thống thông tin của tổ chức.

4.2.1.2 Các lý do truy cập

Các bên thứ ba có thể được phép truy cập vì một số lý do. Ví dụ, các bên thứ ba cung cấp các dịch vụ cho tổ chức không tại chỗ nhưng có thể được truy cập vật lý và logic, như là:

a) nhân viên hỗ trợ phần cứng và phần mềm cần truy cập vào chức năng ứng dụng ở mức hệ thống hoặc mức cơ sở;

b) các đối tác thương mại hoặc các liên doanh có thể trao đổi thông tin, truy cập các hệ thống thông tin hoặc chia sẻ các cơ sở dữ liệu.

Thông tin có thể bị rủi ro bởi việc truy cập của các bên thứ ba nếu quản lý an ninh không thích hợp. Ở chỗ có nhu cầu kinh doanh để kết nối tới vị trí của bên thứ ba, nên tiến hành đánh giá rủi ro để xác định bất kỳ yêu cầu kiểm soát cụ thể nào. Nên tính đến kiểu truy cập, giá trị của thông tin, các kiểm soát bên thứ ba sử dụng và các vấn đề liên quan của truy cập này tới an ninh cho thông tin của tổ chức.

4.2.1.3 Các nhà thầu tại chỗ

Các bên thứ ba được đặt tại chỗ trong một khoảng thời gian như đã xác định trong hợp đồng cũng có thể làm tăng các điểm yếu an ninh. Các ví dụ bên thứ ba tại chỗ gồm:

a) nhân viên hỗ trợ và bảo trì phần cứng và phần mềm;

b) các dịch vụ vệ sinh, ăn uống, bảo vệ an ninh và các dịch vụ hỗ trợ được cung ứng khác;

c) sinh viên thực tập và các bổ nhiệm ngắn hạn ngẫu nhiên khác;

d) các cố vấn.

Điều cốt yếu là hiểu được kiểm soát nào là cần thiết để quản lý việc truy cập của bên thứ ba tới các phương tiện xử lý thông tin. Nói chung, toàn bộ các yêu cầu an ninh đối với việc truy cập của bên thứ ba hoặc các kiểm soát nội bộ nên được thể hiện trong hợp đồng của bên thứ ba (xem 4.2.2).

Ví dụ, nếu có một nhu cầu đặc biệt cho tính bảo mật của thông tin nên sử dụng các thỏa thuận không làm lộ thông tin (xem 6.1.3).

Không nên cung cấp việc truy cập thông tin và các phương tiện xử lý thông tin cho bên thứ ba cho đến khi các kiểm soát thích hợp được thực hiện và một hợp đồng được ký kết xác định các điều khoản về kết nối hoặc truy cập.

4.2.2 Các yêu cầu an ninh trong hợp đồng của bên thứ ba

Các sắp đặt liên quan tới việc truy cập của bên thứ ba tới các phương tiện xử lý thông tin của tổ chức nên được dựa trên cơ sở một hợp đồng chính thức bao gồm hoặc đề cập tới toàn bộ các yêu cầu an ninh để đảm bảo tuân thủ các chính sách và các tiêu chuẩn an ninh của tổ chức. Hợp đồng đó nên đảm bảo rằng không có sự hiểu lầm giữa tổ chức và bên thứ ba.

Các tổ chức nên tự đưa ra thông tin để đảm bảo về nhà cung cấp của họ. Các điều khoản sau đây nên được xem xét trong hợp đồng:

a) chính sách chung về an ninh thông tin;

b) bảo vệ tài sản, bao gồm:

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

   2) các thủ tục để xác định có hoặc không xảy ra bất kỳ sự làm hại nào cho các tài sản, ví dụ mất mát hoặc thay đổi dữ liệu;

   3) các kiểm soát để đảm bảo việc trả lại hoặc hủy thông tin và các tài sản vào cuối hoặc một thời điểm đã thỏa thuận trong hợp đồng;

   4) tính toàn vẹn và tính sẵn sàng;

   5) các hạn chế trong việc sao chép và làm lộ thông tin;

c) mô tả mỗi dịch vụ sẵn dùng;

d) mức chỉ tiêu của dịch vụ và các mức không chấp nhận của dịch vụ;

e) điều khoản đối với việc thuyên chuyển nhân viên thích hợp;

f) các trách nhiệm pháp lý tương ứng của các bên tham gia thỏa thuận;

g) các trách nhiệm đối với các vấn đề pháp lý, ví dụ luật bảo vệ dữ liệu, đặc biệt tính đến các hệ thống pháp lý Quốc gia khác nhau trong trường hợp hợp đồng đó liên quan đến hợp tác với các tổ chức của nhiều nước (xem 12.1);

h) các quyền sở hữu trí tuệ (IPRs) và chuyển nhượng bản quyền tác giả (xem 12.1.2) và bảo vệ bất kỳ công việc hợp tác nào (xem 6.1.3);

i) các thỏa thuận kiểm soát truy cập, bao gồm:

   1) các phương pháp truy cập được phép, việc kiểm soát và sử dụng các định danh duy nhất như các chỉ danh (ID) và mật khẩu của người sử dụng;

   2) một quy trình cấp phép đối với việc truy cập và các đặc quyền của người sử dụng;

   3) một yêu cầu duy trì danh sách các cá nhân được cấp phép sử dụng các dịch vụ sẵn có và các quyền và đặc quyền nào của họ về việc sử dụng này;

j) sự định nghĩa của các tiêu chuẩn có thể thực hiện được, sự giám sát và báo cáo của họ;

k) quyền giám sát và thu hồi, hoạt động của người sử dụng;

l) quyền kiểm tra các trách nhiệm theo hợp đồng hoặc nhờ bên thứ ba tiến hành các kiểm tra này;

m) thiết lập của một quy trình bậc thang đối với việc giải quyết vấn đề; các sắp đặt có tính liên tục cũng nên được xem xét ở những nơi thích hợp;

n) các trách nhiệm liên quan cài đặt và bảo dưỡng phần cứng và phần mềm;

o) khuôn khổ báo cáo rõ ràng và các dạng thức báo cáo đã thông qua;

p) một quy trình rõ ràng và cụ thể đối với việc quản lý sự thay đổi;

q) mọi kiểm soát và cơ chế bảo vệ vật lý được yêu cầu để đảm bảo các kiểm soát đó được làm theo;

r) đào tạo người sử dụng và nhà quản trị về các phương pháp, các thủ tục và an ninh;

s) các kiểm soát để đảm bảo chống lại phần mềm cố ý gây hại (xem 8.3);

t) các chuẩn bị cho việc báo cáo, thông báo và điều tra các sự cố an ninh và các vi phạm an ninh;

u) sự liên quan của bên thứ ba cùng với các thầu phụ.

4.3 Cung ứng bên ngoài

Mục tiêu: Duy trì an ninh thông tin khi trách nhiệm xử lý thông tin được đưa cho một tổ chức khác cung ứng.

Các sắp xếp cho việc cung ứng bên ngoài nên xác định các rủi ro, các kiểm soát và thủ tục an ninh cho các hệ thống thông tin, các mạng và/ hoặc các môi trường màn hình nền trong hợp đồng giữa các bên.

4.3.1 Các yêu cầu an ninh trong hợp đồng cung ứng

Các yêu cầu an ninh cho tổ chức cung ứng việc quản lý và kiểm soát toàn bộ hoặc một số hệ thống thông tin, các mạng và/ hoặc các môi trường màn hình nền của nó nên được định rõ trong hợp đồng chính thức giữa các bên.

Ví dụ, hợp đồng đó nên định rõ:

a) các yêu cầu pháp lý được đáp ứng như thế nào, ví dụ luật bảo vệ dữ liệu;

b) các chuẩn bị nào được sắp đặt để đảm bảo rằng toàn bộ các bên tham gia liên quan đến việc cung ứng, gồm cả các thầu phụ, nhận thức được trách nhiệm an ninh của mình;

c) tính toàn vẹn và tính bảo mật của các tài sản kinh doanh của tổ chức được duy trì và kiểm tra như thế nào;

d) các kiểm soát vật lý và logic nào sẽ được sử dụng để ngăn ngừa và hạn chế việc truy cập thông tin kinh doanh nhạy cảm của tổ chức đối với người sử dụng được phép;

e) tính sẵn sàng của các dịch vụ được duy trì trong trường hợp có tai họa như thế nào?;

f) mức an ninh vật lý nào được cung cấp cho thiết bị cung ứng;

g) quyền kiểm tra sổ sách.

Các điều khoản liệt kê ở 4.2.2 cũng nên được xem xét như một phần của hợp đồng này. Hợp đồng nên cho phép các yêu cầu và các thủ tục an ninh để được mở rộng trong một kế hoạch quản lý an ninh đã được thỏa thuận giữa hai bên.

Mặc dù các hợp đồng cung ứng có thể đưa ra một một số vấn đề an ninh phức tạp, các kiểm soát trong mã thực hành này có thể dùng như một điểm bắt đầu cho việc thỏa thuận về cấu trúc và nội dung của bản kế hoạch quản lý an ninh.

5 Phân loại và kiểm soát tài sản

5.1 Trách nhiệm giải trình các tài sản

Mục tiêu: Duy trì sự bảo vệ thích hợp các tài sản của tổ chức.

Toàn bộ các tài sản thông tin chính nên được giải trình và có người quản lý được bổ nhiệm.

Trách nhiệm giải trình các tài sản giúp cho việc đảm bảo duy trì sự bảo vệ thích hợp. Các quản lý nên được xác định đối với toàn bộ các tài sản chính và có trách nhiệm đối với việc duy trì các kiểm soát thích hợp ấn định trước. Trách nhiệm thực hiện các kiểm soát có thể được giao phó lại. Trách nhiệm giải trình nên giữ nguyên đối với người quản lý tài sản được bổ nhiệm.

5.1.1 Kiểm kê các tài sản

Các bản kiểm kê tài sản giúp đảm bảo việc bảo vệ tài sản hiệu quả được tiến hành và cũng có thể được yêu cầu cho các mục tiêu kinh doanh khác, như sức khỏe và an toàn, các lý do bảo hiểm hoặc tài chính (quản lý tài sản). Quy trình lập bản kiểm kê tài sản là một khía cạnh quan trọng của quản lý rủi ro. Một tổ chức cần có khả năng xác định các tài sản của mình cũng như giá trị và tầm quan trọng tương ứng của các tài sản này. Dựa trên thông tin này, tổ chức có thể đưa ra các mức bảo vệ tương xứng với giá trị và tầm quan trọng của các tài sản. Nên thảo ra và duy trì một bản kiểm kê đối với các tài sản quan trọng kết hợp với từng hệ thống thông tin. Mỗi tài sản nên được xác định rõ ràng cũng như được thỏa thuận và ghi chép quyền sở hữu và sự phân loại an ninh của nó (xem 5.2), cùng với vị trí hiện tại của nó (quan trọng là khôi phục các mất mát hoặc hỏng hóc). Các ví dụ về các tàI sản kết hợp với các hệ thống thông tin là:

a) các tài sản thông tin: Các tệp dữ liệu và cơ sở dữ liệu, tài liệu hệ thống, sổ tay người sử dụng, tài liệu đào tạo, thủ tục hoạt động hoặc hỗ trợ, kế hoạch liên tục, chuẩn bị dự phòng, thông tin thu được;

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

c) các tài sản vật lý: Thiết bị máy tính (các bộ vi xử lý, màn hình, máy tính xách tay, modem), thiết bị truyền thông (routers, PABXs, máy fax, máy trả lời tự động), phương tiện có từ tính (các băng từ và đĩa), các thiết bị kỹ thuật khác (máy phát điện, thiết bị điều hoà không khí), đồ đạc, văn phòng;

d) các dịch vụ: Các dịch vụ truyền thông và máy tính, thiết bị chung, ví dụ; lò sưởi, chiếu sáng, năng lượng, điều hòa.

5.2 Phân loại thông tin

Mục tiêu: Đảm bảo rằng các tài sản thông tin có một mức bảo vệ thích hợp.

Thông tin nên được phân loại để định ra nhu cầu, mức ưu tiên và mức bảo vệ. Thông tin có tính nhạy cảm và tính phê bình khác nhau. Một số mục có thể yêu cầu một mức bảo vệ bổ sung hoặc quá trình quản lý đặc biệt. Một hệ thống phân loại thông tin nên được sử dụng để xác định một loạt các mức bảo vệ thích hợp và thông báo về các biện pháp quản lý đặc biệt.

5.2.1 Các hướng dẫn phân loại

Các loại thông tin và các kiểm soát bảo vệ liên quan nên xét đến các nhu cầu chia sẻ hoặc hạn chế thông tin trong kinh doanh và các tác động kinh doanh kết hợp với các nhu cầu này, ví dụ truy cập trái phép hoặc gây hại cho thông tin đó. Nói chung, sự phân loại thông tin là một phương pháp nhanh xác định các thông tin này được quản lý và bảo vệ như thế nào.

Thông tin và các yếu tố đầu vào từ các hệ thống quản lý dữ liệu được phân loại nên được ghi nhãn theo giá trị và tính nhạy cảm của nó đối với tổ chức. Nó có thể phù hợp để ghi nhãn thông tin theo tính phê bình của nó đối với tổ chức, ví dụ; dưới dạng tính toàn vẹn và tính sẵn sàng.

Thông tin thường hết tính nhạy cảm hoặc phê bình sau một khoảng thời gian nhất định, ví dụ, khi thông tin đó đã được công bố. Nên xét đến các khía cạnh này vì sự phân loại quá kỹ có thể dẫn tới một chi phí kinh doanh thêm không cần thiết. Các hướng dẫn phân loại nên lường trước và cho phép với thực tế sự phân loại của bất kỳ hạng mục thông tin nào không nhất thiết cố định mãi và có thể thay đổi phù hợp với một số chính sách đã định trước (xem 9.1).

Nên xem xét số lượng danh mục phân loại và lợi ích đạt được từ việc sử dụng chúng. Các kế hoạch quá phức tạp có thể trở thành nặng nề và không kinh tế khi sử dụng hoặc không thực tế. Nên quan tâm đến sự thông dịch các nhãn phân loại trên các tài liệu từ các tổ chức khác mà có thể có các quy ước khác nhau đối với các nhãn tương tự hoặc cùng tên gọi.

Trách nhiệm đối với việc xác định sự phân loại của một hạng mục thông tin nên giữ nguyên người khởi tạo hoặc người quản lý được bổ nhiệm của thông tin đó, ví dụ đối với một tài liệu, bản ghi dữ liệu, tệp dữ liệu hoặc đĩa mềm và đối với việc soát xét theo định kỳ sự phân loại đó.

5.2.2 Dán nhãn và quản lý thông tin

Điều quan trọng là một loạt các thủ tục thích hợp được xác định đối với việc ghi nhãn và quản lý thông tin phù hợp với kế hoạch phân loại được tổ chức chấp nhận. Các thủ tục này cần bao trùm các tài sản thông tin dưới các dạng thức vật lý và điện tử. Đối với mỗi sự phân loại, các quy trình quản lý nên được xác định để bao gồm các kiểu hoạt động xử lý thông tin sau đây:

a) sao chép;

b) lưu trữ;

c) truyền bằng cách gửi thư, fax và thư điện tử;

d) truyền bằng lời nói, bao gồm điện thoại di động, thư thoại, máy trả lời;

e) sự phá hoại.

Dữ liệu ra từ các hệ thống chứa thông tin được phân loại theo tính nhạy cảm hoặc tính phê bình nên mang một nhãn phân loại thích hợp (trong các dữ liệu ra). Việc ghi nhãn đó nên phản ánh sự phân loại theo các quy tắc được thiết lập ở 5.2.1. Các hạng mục xem xét gồm các báo cáo in sẵn, hiển thị màn hình, phương tiện truyền thông (băng từ, đĩa, CD, băng cátsét), các thông điệp điện tử và các truyền tệp.

Các nhãn vật lý nói chung là các dạng thích hợp nhất cho dán nhãn. Tuy nhiên, một số tài sản thông tin, như các tài liệu dưới dạng điện tử, không thể được dán nhãn vật lý và nên sử dụng các phương tiện dán nhãn điện tử.

6 An ninh cá nhân

6.1 An ninh theo định nghĩa và nguồn công việc

Mục tiêu: Giảm các rủi ro do các hành vi sai sót, đánh cắp, gian lận hoặc lạm dụng các phương tiện.
Các trách nhiệm an ninh nên được định rõ vào giai đoạn tuyển nhân viên, bao gồm trong các hợp đồng và được giám sát trong thời gian làm việc của cá nhân.
Các nhân viên mới có tiềm năng nên được kiểm tra một cách thích hợp (xem 6.1.2), đặc biệt đối với các công việc nhạy cảm. Toàn bộ người sử dụng, cả nhân viên và bên thứ ba, các phương tiện xử lý thông tin nên ký kết một thỏa thuận về tính bảo mật (không làm lộ).

6.1.1 An ninh theo các trách nhiệm công việc

Các vai trò và trách nhiệm an ninh, khi được đặt trong chính sách an ninh thông tin của tổ chức (xem 3.1) nên được tài liệu hóa một cách thích hợp. Chúng nên gồm mọi trách nhiệm chung đối với việc thực hiện hoặc duy trì chính sách an ninh cũng như mọi trách nhiệm đặc biệt đối với việc bảo vệ các tài sản cụ thể hoặc đối với việc thi hành các quy trình hoặc các hoạt động an ninh cụ thể.

6.1.2 Chính sách và kiểm tra nhân sự

Việc kiểm tra các nhân viên dài hạn nên được tiến hành tại thời điểm tuyển dụng. Các kiểm soát nên bao gồm:

a) tính sẵn có của các giấy tờ dẫn chứng về các đặc điểm, ví dụ về công việc và cá nhân;

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

c) xác nhận bằng cấp được yêu cầu và phẩm chất nghề nghiệp;

d) kiểm tra nhận dạng (hộ chiếu hoặc giấy tờ tương tự).

Việc bổ nhiệm ban đầu và thăng tiến công việc liên quan đến cá nhân truy cập tới các phương tiện xử lý thông tin và đặc biệt với các thông tin nhạy cảm, ví dụ thông tin về tài chính hoặc thông tin bảo mật cao, tổ chức cũng nên tiến hành kiểm tra tín dụng. Đối với nhân viên đang giữ vị trí có thẩm quyền đáng kể thì việc kiểm tra này nên được lặp lại có định kỳ.

Quá trình kiểm tra tương tự nên được tiến hành đối với các nhà thầu và nhân viên tạm thời. Nếu các nhân viên này được cung cấp thông qua môi giới thì hợp đồng với môi giới nên quy định rõ ràng các trách nhiệm kiểm tra của môi giới và các thủ tục khai báo mà họ cần phải theo nếu việc kiểm tra không đầy đủ hoặc các kết quả gây sự nghi ngờ hoặc lo ngại.

Ban quản lý nên đánh giá việc giám sát nhân viên mới và thiếu kinh nghiệm cùng với quyền truy cập tới các hệ thống nhạy cảm. Công việc của toàn bộ nhân viên nên đạt được các quá trình soát xét và phê chuẩn định kỳ của một nhân viên cấp cao hơn.

Các nhà quản lý nên được nhận thức rằng hoàn cảnh cá nhân của các nhân viên có thể ảnh hưởng đến công việc của họ. Các vấn đề cá nhân hoặc tài chính, các thay đổi về hành vi hoặc lối sống, sự vắng mặt nhiều lần và dấu hiệu của tình trạng căng thẳng hoặc tình trạng chán nản có thể dẫn tới hành vi gian lận, ăn cắp, gây lỗi hoặc các hành vi liên quan đến vấn đề an ninh khác. Thông tin này nên được xử lý phù hợp với tất cả pháp chế thích hợp hiện có trong phạm vi pháp luật liên quan.

6.1.3 Thỏa thuận về tính bảo mật

Các thỏa thuận về tính bảo mật hoặc không làm lộ được sử dụng để đưa ra lưu ý rằng thông tin là bảo mật hoặc bí mật. Các nhân viên nên ký kết một thỏa thuận như một phần của các điều khoản và điều kiện tuyển dụng ban đầu của họ.

Nên yêu cầu những người sử dụng không chủ định, nhân viên và bên thứ ba, chưa có hợp đồng bao gồm thỏa thuận về tính bảo mật, ký kết một thỏa thuận về tính bảo mật trước khi được phép truy cập tới các phương tiện xử lý thông tin.

Các thỏa thuận về tính bảo mật nên được soát xét khi có các thay đổi về thời hạn công việc hoặc hợp đồng, cụ thể là khi những người lao động rời tổ chức hoặc các hợp đồng đã hết hạn.

6.1.4 Các điều khoản và điều kiện tuyển dụng

Các điều khoản và điều kiện tuyển dụng nên chỉ ra trách nhiệm của người lao động đối với an ninh thông tin. Nếu thích hợp, các trách nhiệm này nên tiếp tục duy trì trong một khoảng thời gian xác định sau khi hết công việc. Nếu người lao động coi thường các yêu cầu an ninh đó thì sẽ bị kiện.

Trách nhiệm và quyền lợi pháp lý của người lao động nên dễ hiểu và có trong các điều khoản và điều kiện tuyển dụng, ví dụ liên quan đến các luật bản quyền hoặc luật bảo vệ dữ liệu, đồng thời cũng nên có trách nhiệm đối với việc phân loại và quản lý dữ liệu của người lao động. Các điều khoản và điều kiện tuyển dụng nên chỉ ra rằng các trách nhiệm này được mở rộng ra bên ngoài phạm vi tổ chức và thời gian làm việc bình thường, ví dụ trong trường hợp làm việc ở nhà (Xem 7.2.5 và 9.8.1).

6.2 Đào tạo người sử dụng

Mục tiêu: Đảm bảo rằng người sử dụng nhận thức được các mối đe dọa và các vấn đề liên quan đến an ninh thông tin trang bị để hỗ trợ chính sách an ninh của tổ chức trong quá trình làm việc bình thường của họ.

Người sử dụng nên được đào tạo về các thủ tục an ninh và sử dụng đúng các phương tiện xử lý thông tin để giảm thiểu các rủi ro an ninh có khả năng xảy ra.

6.2.1 Giáo dục và đào tạo an ninh thông tin

Toàn bộ các nhân viên của tổ chức và những người sử dụng liên quan hoặc bên thứ ba nên tiếp nhận đào tạo thích hợp và các cập nhật thường xuyên về chính sách và thủ tục của tổ chức. Điều này bao gồm các yêu cầu an ninh, trách nhiệm pháp lý và các kiểm soát kinh doanh, cũng như đào tạo việc sử dụng đúng các phương tiện xử lý thông tin trước khi truy cập tới thông tin hoặc các dịch vụ được cho phép ví dụ thủ tục đăng nhập, sử dụng các gói phần mềm.

6.3 Đối phó với các sự cố và sự cố an ninh

Mục tiêu: Giảm thiểu thiệt hại từ các trục trặc và sự cố an ninh, theo dõi và rút kinh nghiệm từ các sự cố như vậy.

Các sự cố ảnh hưởng tới an ninh nên được báo cáo càng nhanh càng tốt qua các kênh quản lý phù hợp.

Toàn bộ những người lao động và các nhà thầu nên được nhận thức về các quy trình báo cáo các kiểu sự cố khác nhau có thể có tác động tới an ninh các tài sản của tổ chức (vi phạm an ninh, mối đe dọa, nhược điểm hoặc trục trặc). Họ nên được yêu cầu báo cáo bất kỳ sự cố họ thấy hoặc nghi ngờ nào càng nhanh càng tốt cho bộ phận được chỉ định. Tổ chức nên thiết lập một quy trình kỷ luật chính thức đối với việc xử lý những người lao động vi phạm an ninh. Để có thể xác định các sự cố một cách đúng đắn, cần thu thập chứng cớ càng sớm càng tốt sau khi sự việc xảy ra (xem 12.1.7).

6.3.1 Báo cáo các sự cố an ninh

Các sự cố an ninh nên được báo cáo qua các kênh quản lý phù hợp càng nhanh càng tốt.

Nên thiết lập một thủ tục báo cáo chính thức, cùng với thủ tục phản hồi lại sự cố, lập ra hành động cần thực hiện để báo cáo về sự cố. Toàn bộ những người lao động và các nhà thầu nên được nhận thức về thủ tục báo cáo các sự cố an ninh đó và nên yêu cầu báo cáo các sự cố như vậy càng nhanh càng tốt. Các quá trình phản hồi thông tin phù hợp nên được thi hành để đảm bảo rằng việc báo cáo các sự cố được thông báo kết quả sau khi sự cố đó đã được xử lý và khép lại. Các sự cố này có thể được sử dụng trong việc đào tạo nhận thức cho người sử dụng (xem 6.2) như là các ví dụ về điều có thể xảy ra, cách phản hồi lại với các sự cố đó và cách phòng tránh chúng trong tương lai (xem 12.1.7).

6.3.2 Báo cáo các điểm yếu an ninh

Người sử dụng các dịch vụ thông tin nên được yêu cầu ghi chú và báo cáo bất kỳ điểm yếu an ninh nào họ thấy hoặc nghi ngờ hoặc các mối đe dọa đối với các hệ thống hoặc các dịch vụ. Họ nên báo cáo các vấn đề này tới cả ban quản lý và trực tiếp cho nhà cung cấp dịch vụ của họ càng nhanh càng tốt. Người sử dụng nên được thông báo rằng trong bất kỳ hoàn cảnh nào, họ không nên cố gắng chứng minh một điểm yếu nghi ngờ. Điều này là để bảo vệ cho chính họ, vì việc kiểm tra các nhược điểm có thể được giải thích như sự lạm dụng hệ thống.

6.3.3 Báo cáo các sự cố an ninh

Nên thiết lập các thủ tục báo cáo các sự cố phần mềm. Các hành động sau đây nên được xem xét:

a) nên ghi chép các dấu hiệu vấn đề và thông điệp xuất hiện trên màn hình;

b) nếu có thể, máy tính nên được cô lập và ngừng sử dụng. Việc tiếp xúc thích hợp nên được cảnh báo ngay lập tức. Nên ngưng kết nối thiết bị được kiểm tra khỏi mọi mạng của tổ chức trước khi được cấp nguồn lại. Các đĩa mềm không nên được chuyển tới các máy tính khác;

c) vụ việc nên được báo cáo ngay lập tức tới nhà quản lý an ninh thông tin.

Người sử dụng không nên cố gắng gỡ bỏ phần mềm bị nghi ngờ đó trừ khi được quyền làm vậy. Nhân viên được đào tạo và có kinh nghiệm thích hợp nên tiến hành việc khôi phục.

6.3.4 Rút kinh nghiệm từ các sự cố

Nên có các cơ chế để tạo điều kiện cho việc xác định số lượng và giám sát các kiểu, dung lượng và chi phí của các sự cố và trục trặc. Thông tin này nên được sử dụng để định danh các sự cố hoặc trục trặc lặp lại nhiều lần và có ảnh hưởng lớn. Điều này có thể chỉ ra nhu cầu các kiểm soát tăng cường hoặc bổ sung để hạn chế tần suất xảy ra, sự thiệt hại và chi phí của các sự, vụ trong tương lai hoặc để đưa vào trong quy trình soát xét chính sách an ninh (xem 3.1.2).

6.3.5 Quy trình thiết lập kỷ luật

Nên có một quy trình kỷ luật chính thức đối với các nhân viên vi phạm các chính sách và các quy trình an ninh của tổ chức (xem 6.1.4 và 12.1.7 đối với sự sử dụng chứng cớ). Một quy trình như vậy có thể hoạt động như một sự ngăn chặn các nhân viên có thể có khuynh hướng coi nhẹ các quy trình an ninh. Ngoài ra, nó nên đảm bảo việc coi công bằng, đúng đắn với các nhân viên bị nghi ngờ là phạm sai lầm nghiêm trọng hoặc có các hành vi liên tục vi phạm an ninh.

7 An ninh môi trường và vật lý

7.1 Phạm vi an ninh

Mục tiêu: Ngăn ngừa việc truy cập, gây hại và can thiệp trái phép vào vùng và thông tin kinh doanh.
Các phương tiện xử lý thông tin kinh doanh có tính quy định hoặc nhạy cảm nên được đặt trong các phạm vi an ninh, được bảo vệ bởi một vành đai an ninh xác định, cùng với các hàng rào an ninh thích hợp và các kiểm soát xâm nhập. Chúng nên được bảo vệ vật lý khỏi sự truy cập, gây hại và can thiệp trái phép. Việc bảo vệ nên tương xứng với các rủi ro đã xác định. Một chính sách bàn sạch và màn hình sạch được khuyến cáo để giảm rủi ro của truy cập trái phép hoặc sự gây hại các giấy tờ, phương tin truyền thông và các phương tiện xử lý thông tin.

7.1.1 Vành đai an ninh vật lý

Sự bảo vệ vật lý có thể đạt được bằng cách tạo ra các hàng rào vật lý xung quanh vùng kinh doanh và phương tiện xử lý thông tin. Mỗi hàng rào thiết lập một vành đai an ninh, mỗi vành đai làm tăng sự bảo vệ chung. Các tổ chức nên sử dụng các vành đai an ninh để bảo vệ các khu vực chứa các phương tiện xử lý thông tin (xem 7.1.3). Một vành đai an ninh nghĩa là xây lên một hàng rào, ví dụ một bức tường, cổng vào kiểm tra thẻ hoặc bàn tiếp tân. Vị trí và sức bền của mỗi hàng rào phụ thuộc vào các kết quả đánh giá rủi ro.

Các chỉ dẫn và kiểm soát sau đây nên được xem xét và thi hành khi thích hợp:

a) vành đai an ninh nên được xác định rõ ràng;

b) vành đai an ninh của một tòa nhà hoặc nơi chứa các phương tiện xử lý thông tin nên vững chắc về mặt vật lý (nghĩa là: không nên có khoảng trống trong vành đai an ninh hoặc các khu vực có thể dễ dàng xảy ra một vụ tấn công);

c) các bức tường bên ngoài của địa điểm đó nên có cấu trúc vững chắc toàn bộ các cửa bên ngoài nên được bảo vệ phù hợp chống lại việc truy cập trái phép, ví dụ các cơ chế kiểm soát, các thanh chắn, các báo động, khóa v..v;

d) một khu vực tiếp tân do người phụ trách hoặc các phương tiện khác để kiểm soát truy cập vật lý tới khu vực này hoặc toà nhà nên được tiến hành. Truy cập tới các địa điểm và các toà nhà nên bị hạn chế, chỉ cho cá nhân được cấp phép;

e) nếu cần thiết, các hàng rào vật lý nên được mở rộng từ sàn thực tới trần thực để ngăn ngừa xâm nhập trái phép và làm ô nhiễm môi trường gây ra bởi lửa và lụt lội;

f) toàn bộ các cửa thoát hỏa trong vành đai an ninh nên được báo động và nên đóng sập lại.

7.1.2 Kiểm soát xâm nhập vật lý

Các khu vực an ninh nên được bảo vệ bởi các kiểm soát xâm nhập thích hợp để đảm bảo rằng chỉ các cá nhân được cấp phép mới được phép truy cập. Nên xem xét các kiểm soát sau đây:

a) các khách đến các khu vực an ninh nên được giám sát hoặc rà soát và ghi lại ngày giờ ra vào của họ. Họ chỉ được cho phép truy cập vì các mục đích cụ thể, được quyền và được chỉ dẫn về các yêu cầu an ninh của khu vực đó và các thủ tục khẩn cấp;

b) truy cập tới thông tin nhạy cảm và các phương tiện xử lý thông tin nên được kiểm soát và hạn chế chỉ cho các cá nhân được cấp phép. Các kiểm soát xác thực, ví dụ thẻ và PIN nên được sử dụng để cấp phép và kiểm tra tính hợp lệ toàn bộ các truy cập. Một dấu vết kiểm tra của toàn bộ các truy cập nên được duy trì một cách an toàn;

c) tất cả các cá nhân nên được yêu cầu đeo một số dạng định danh có thể trông thấy và khuyến khích nghi ngờ những người lạ không ai đi cùng và không khoác định danh có thể trông thấy;

d) các quyền truy cập tới các khu vực an ninh nên được xem xét và cập nhật một cách đều đặn.

7.1.3 An ninh văn phòng, phòng và phương tiện

Một khu vực an ninh có thể là một văn phòng hoặc một số phòng được khóa trong một vành đai an ninh vật lý, có thể được khóa và có thể bao gồm các giá hoặc các két khóa được. Việc lựa chọn và thiết kế một khu vực an ninh nên xét đến khả năng bị hư hại do lửa, lũ lụt, nổ, tình trạng náo động nội bộ và các tai họa khác do tự nhiên hoặc con người gây ra, cũng nên tính đến các quy định và tiêu chuẩn liên quan đến sức khỏe và an toàn. Việc xem xét cũng nên xem xét mọi mối đe dọa an ninh từ các vùng bên cạnh, ví dụ sự rò rỉ nước ở các khu vực khác.

Nên xem xét các kiểm soát sau đây:

a) các phương tiện chính nên được đặt ở nơi tránh sự tiếp cận của công chúng;

b) các tòa nhà nên kín đáo và biểu thị tối thiểu mục đính của chúng, không có các dấu hiệu rõ ràng xác nhận sự hiện diện của các hoạt động xử lý thông tin, cả bên ngoài và bên trong tòa nhà;

c) các chức năng và thiết bị hỗ trợ có thể chứa thông tin nên được đặt khi thích hợp trong khu vực an ninh để tránh các nhu cầu truy cập, ví dụ các máy sao chụp tài liệu, các máy fax;

d) các cửa ra vào và cửa sổ nên được khóa khi không chú ý và việc bảo vệ bên ngoài nên xem xét các cửa sổ, đặc biệt ở tầng dưới mặt đất;

e) nên thực hiện lắp đặt theo các tiêu chuẩn chuyên nghiệp và kiểm tra thường xuyên các hệ thống phát hiện xâm nhập phù hợp để bao quát được toàn bộ các cửa ra vào bên ngoài và các cửa sổ có thể xâm nhập. Các khu vực không lắp đặt được nên có báo động 24/24. Việc kiểm soát cũng nên được trang bị cho các khu vực khác, ví dụ các phòng máy tính hoặc các phòng thông tin;

f) các phương tiện xử lý thông tin do tổ chức quản lý nên được phân tách về mặt vật lý với các phương tiện xử lý thông tin do các bên thứ ba quản lý;

g) các tài liệu hướng dẫn và danh bạ điện thoại nội bộ xác định vị trí các phương tiện xử lý thông tin nhạy cảm không nên để mọi người dễ dàng truy cập được;

h) các vật liệu nguy hiểm và dễ cháy nên được lưu trữ cẩn thận với khoảng cách an toàn với khu vực an ninh. Các hàng cung cấp lớn như đồ dùng văn phòng không nên được lưu trong khu vực an ninh trừ khi được yêu cầu;

i) các thiết bị và phương tiện mang thông tin dự phòng nên được đặt ở một khoảng cách an toàn để tránh tổn thất do một tai họa nào đó tại vị trí chính.

7.1.4 Làm việc trong phạm vi an ninh

Các kiểm soát và hướng dẫn bổ xung có thể được yêu cầu để tăng cường an ninh của một khu vực an ninh.

Điều này bao gồm kiểm soát đối với nhân sự hoặc các bên thứ ba làm việc trong khu vực an ninh, cũng như các hoạt động của bên thứ ba diễn ra tại đó. Nên xem xét các kiểm soát sau đây:

a) cá nhân chỉ nên biết về sự tồn tại hoặc các hoạt động trong một khu vực an ninh ở mức cần biết cơ bản;

b) nên tránh có các công việc trong khu vực an ninh không được giám sát vì cả lý do an toàn và để ngăn ngừa các cơ hội cho các hoạt động có chủ ý gây hại;

c) các khu vực an ninh không người nên được khoá cẩn thận và kiểm tra định kỳ;

d) bên thứ ba hỗ trợ các dịch vụ cá nhân nên được hạn chế tối đa truy cập các khu vực an ninh hoặc phương tiện xử lý thông tin nhạy cảm trừ khi được yêu cầu. Việc truy cập nên được cấp phép và được giám sát. Các rào cản và vành đai bổ xung để kiểm soát truy cập vật lý là cần thiết giữa các khu vực với các yêu cầu an ninh khác nhau bên trong vành đai an ninh;

e) ảnh, băng, đĩa hoặc các thiết bị ghi lưu khác trái phép dùng, trừ khi được cho phép.

7.1.5 Các khu vực tiếp nhận và phân phối riêng biệt

Các khu vực tiếp nhận và phân phối nên được kiểm soát và nếu có thể nên tách biệt khỏi các phương tiện xử lý thông tin để tránh truy cập trái phép. Các yêu cầu an ninh cho các khu vực này nên được xác lập qua việc đánh giá rủi ro. Nên xem xét các kiểm soát sau đây:

Truy cập tới một khu vực dự trữ từ bên ngoài toà nhà nên được hạn chế cho các cá nhân được xác nhận và cho phép.

Khu vực dự trữ nên được thiết kế để các nguồn cung ứng không thể được tiếp nhận mà không có sự tiếp cận của nhân viên phân phối đến các bộ phận khác trong toà nhà.

Các cửa ra vào bên ngoài của khu vực dự trữ nên được đảm bảo an ninh khi cửa bên trong mở.

Nguyên liệu đầu vào nên được giám định kỹ các nguy hiểm tiềm tàng [xem 7.2.1 d)] trước khi được đưa từ khu vực dự trữ đến nơi sử dụng.

Nguyên liệu đầu vào nên được đăng ký ở cửa vào, nếu thích hợp (xem 5.1).

7.2 An ninh thiết bị

Mục tiêu: Ngăn ngừa sự mất mát, tổn thất hoặc làm hại các tài sản và sự gián đoạn các hoạt động kinh doanh.
Các thiết bị nên được bảo vệ về mặt vật lý khỏi các mối đe dọa an ninh và các hiểm hoạ môi trường. Sự bảo vệ các thiết bị (bao gồm cả các thiết bị không sử dụng tại chỗ) là cần thiết để giảm sự rủi ro của việc truy cập trái phép dữ liệu và để bảo vệ chống lại sự mất mát hoặc hư hại. Điều này cũng nên xem xét sự lắp đặt và tháo bỏ thiết bị. Kiểm soát đặc biệt có thể được yêu cầu để bảo vệ khỏi các nguy hiểm hoặc việc truy cập trái phép và để bảo vệ các thiết bị hỗ trợ, như thiết bị cung cấp điện và hệ thống dây cáp.

7.2.1 Chọn địa điểm đặt và bảo vệ thiết bị

Thiết bị nên được đặt và bảo vệ để giảm các rủi ro từ các mối đe dọa và nguy hiểm của môi trường và các nguy cơ truy cập trái phép. Nên xem xét các kiểm soát sau đây:

a) thiết bị nên được đặt ở nơi giảm thiểu việc truy cập không cần thiết trong khu vực làm việc;

b) các phương tiện lưu trữ và xử lý thông tin các dữ liệu nhạy cảm nên được đặt sao cho giảm sự rủi ro bỏ sót trong quá trình sử dụng;

c) các bộ phận yêu cầu bảo vệ đặc biệt nên được cô lập để giảm mức bảo vệ yêu cầu chung;

d) các kiểm soát nên được thích ứng để giảm thiểu rủi ro từ các mối đe dọa tiềm tàng gồm:

   1) hành vi ăn trộm;

   2) cháy;

   3) nổ;

   4) khói;

5) nước (hoặc lỗi cung cấp);

6) rác;

7) rung;

8) các ảnh hưởng hóa chất;

9) nhiễu nguồn điện;

10) phát xạ điện từ.

e) một tổ chức nên xem xét chính sách của mình đối với việc ăn, uống và hút thuốc trong phạm vi gần các phương tiện xử lý thông tin;

f) điều kiện môi trường nên được giám sát đối với các điều kiện có thể ảnh hưởng bất lợi cho hoạt động của các phương tiện xử lý thông tin;

g) việc sử dụng các biện pháp bảo vệ đặc biệt, như keyboard membranes nên được xem xét cho các thiết bị trong môi trường công nghiệp;

h) tác động của một hiểm hoạ xảy ra trong các nơi tiếp giáp nên được xem xét, ví dụ như cháy ở toà nhà bên cạnh, nước rò từ trên mái hoặc trong các tầng dưới tầng mặt đất hoặc một vụ nổ trên phố.

7.2.2 Các nguồn điện

Thiết bị nên được bảo vệ khi mất điện hoặc có sự bất ổn về điện khác. Nên cung cấp một nguồn điện phù hợp thích ứng với các đặc điểm kỹ thuật của nhà sản xuất thiết bị.

Các lựa chọn để có được nguồn cung cấp điện ổn định gồm:

a) có các nguồn cung cấp đa dạng để tránh bị mất điện do một nguồn cung cấp có sự cố;

b) nguồn cung cấp điện không bị gián đoạn (UPS);

c) máy phát điện dự phòng.

Thiết bị hỗ trợ cho các hoạt động kinh doanh có tính phê bình nên có UPS để hỗ trợ việc thay nhau ngừng hoặc tiếp tục hoạt động. Các kế hoạch cho sự ổn định nên tính đến cả sự hỏng hóc của UPS. Thiết bị USP nên được kiểm tra thường xuyên để đảm bảo nó có công suất thích hợp và được kiểm tra phù hợp với các khuyến cáo của nhà sản xuất.

Máy phát điện dự phòng nên được xem xét nếu quá trình hoạt động cần phải tiếp tục trong trường hợp mất điện kéo dài. Nếu được lắp đặt, máy phát điện nên được kiểm tra thường xuyên để phù hợp với hướng dẫn của nhà sản xuất. Nguồn cung cấp nhiên liệu thích hợp nên sẵn sàng để đảm bảo rằng máy phát điện có thể hoạt động trong thời gian dài.

Thêm vào đó, các công tắc điện khẩn cấp nên được đặt gần các cửa thoát khẩn cấp trong các phòng thiết bị để ngắt điện nhanh chóng trong trường hợp khẩn cấp. Đèn lối đi khẩn cấp nên được bật trong trường hợp mất nguồn điện chính. Chống sét nên được áp dụng cho toàn bộ các toàn nhà và các thiết bị chống sét nên được lắp đặt cho toàn bộ các đường truyền thông bên ngoài.

7.2.3 An ninh cho hệ thống cáp

Điện và các thiết bị truyền thông bằng cáp cung cấp dữ liệu hoặc các dịch vụ hỗ trợ thông tin nên được bảo vệ khỏi việc nghe trộm hoặc bị hư hại. Nên xem xét các kiểm soát sau đây:

a) đường điện và đường truyền thông đến các phương tiện xử lý thông tin nên được đặt ngầm ở các nơi có thể hoặc tuân theo sự bảo vệ phù hợp;

b) đường truyền mạng nên được bảo vệ khỏi sự nghe trộm trái phép hoặc sự hư hại, ví dụ sử dụng ống cáp hoặc tránh đi qua các khu vực công cộng;

c) đường điện và đường truyền thông tin nên tách riêng để ngăn ngừa sự ảnh hưởng lẫn nhau;

d) đối với các hệ thống có tính nhạy cảm hoặc phê bình cao, việc kiểm soát thêm nên gồm:

   1) dùng ống cáp bọc sắt, các phòng hoặc hộp có khoá ở các điểm giám định hoặc kiểm tra;

   2) sử dụng các đường truyền hoặc phương tiện truyền phát khác nhau;

   3) sử dụng sợi cáp quang;

   4) thiết lập các rà soát đối với các âm mưu trái phép được ghép vào cáp.

7.2.4 Bảo dưỡng thiết bị

Thiết bị nên được bảo dưỡng chuẩn để đảm bảo tính sẵn sàng và chính xác.

Nên xem xét các kiểm soát sau đây:

a) thiết bị nên được bảo dưỡng phù hợp với các đặc tính kỹ thuật và khoảng thời gian bảo dưỡng mà nhà cung cấp khuyến cáo;

b) chỉ cá nhân bảo dưỡng được cấp phép mới được tiến hành sửa chữa và bảo dưỡng thiết bị;

c) toàn bộ các lỗi nghi ngờ hoặc có thực và toàn bộ sự phòng ngừa hoặc bảo dưỡng nên được ghi chép và lưu giữ lại;

d) các kiểm soát thích hợp nên được tiến hành khi gửi thiết bị ngoại vi đi bảo dưỡng (xem thêm 7.2.6 liên quan đến dữ liệu bị tẩy, xoá hoặc chèn). Toàn bộ yêu cầu nên phù hợp với hợp đồng bảo hiểm.

7.2.5 An ninh của các thiết bị ngoại vi

Không liên quan đến quyền sở hữu, việc sử dụng bất kỳ thiết bị bên ngoài phạm vị một tổ chức nào để xử lý thông tin nên được ban quản lý cho phép. An ninh cho các thiết bị này nên được cân đối với an ninh của các thiết bị trong tổ chức có cùng mục đích tương tự và xét đến các rủi ro của công việc bên ngoài phạm vị của tổ chức đó. Thiết bị xử lý thông tin bao gồm toàn bộ các máy tính cá nhân, các người tổ chức, điện thoại di động, giấy tờ và các dạng khác, được dùng để làm việc ở nhà hoặc được mang ra ngoài các vị trí công việc thông thường.

Các hướng dẫn sau nên được xem xét.

a) thiết bị và phương tiện truyền thông ngoại vi không nên gây chú ý ở nơi công cộng. Các máy tính xách tay nên được cho vào túi xách tay và được nguỵ trang ở mức có thể khi di chuyển;

b) các hướng dẫn bảo vệ thiết bị của nhà sản xuất nên được thực thi mọi lúc, ví dụ bảo vệ khi ở trong các môi trường có điện từ lớn;

c) kểm soát làm việc ở nhà nên được xác định qua đánh giá rủi ro và áp dụng các kiểm soát phù hợp riêng, ví dụ các tủ lưu hồ sơ có khoá, "chính sách bàn sạch" và kiểm soát việc truy cập máy tính;

d) nên thực hiện các bảo hiểm thích hợp để bảo vệ cho thiết bị ngoại vi.

Các rủi ro an ninh, ví dụ hư hại, trộm cắp và nghe trộm, có thể khác nhau ở mỗi địa điểm và nên được xét đến để xác định các kiểm soát phù hợp nhất. Thông tin thêm về các khía cạnh khác của bảo vệ thiết bị di động có thể xem ở mục 9.8.1.

7.2.6 An ninh trong việc loại bỏ hoặc tái sử dụng các thiết bị

Thông tin có thể bị tổn thất bởi việc loại bỏ hoặc tái sử dụng thiết bị không cẩn thận (xem thêm 8.6.4). Các bộ phận lưu trữ chứa thông tin nhạy cảm nên được huỷ bỏ về mặt vật lý hoặc chèn đè một cách an toàn hơn là sử dụng chức năng xoá thông thường. Toàn bộ các phần của thiết bị chứa phương tiện truyền thông lưu trữ, ví dụ các đĩa cứng cố định nên được kiểm tra để đảm bảo rằng bất kỳ dữ liệu nhạy cảm và phần mềm được cấp phép phải được xoá hoặc chèn đè trước khi huỷ bỏ. Các bộ phận lưu trữ chứa thông tin nhạy cảm bị thiệt hại nên được đánh giá để xác định rủi ro nếu các bộ phận này bị huỷ, sửa chữa hoặc bỏ đi.

7.3 Kiểm soát chung

Mục tiêu: Ngăn ngừa sự làm hại hoặc đánh cắp thông tin và các phương tiện xử lý thông tin.
Thông tin và các phương tiện xử lý thông tin nên được bảo vệ khỏi bị lộ, sửa đổi hoặc đánh cắp bởi các cá nhân trái phép và kiểm soát nên được thực hiện để giảm thiểu mất mát hoặc hư hoại. Các thủ tục lưu trữ và quản lý xem ở mục 8.6.3.

7.3.1 Chính sách bàn "sạch" và màn hình "sạch"

Các tổ chức nên xem xét việc tiếp nhận một "chính sách bàn sạch" cho các giấy tờ và phương tiện truyền thông lưu trữ lưu động và "chính sách màn hình sạch" cho các phương tiện xử lý thông tin để giảm các rủi ro của việc truy cập trái phép, mất mát và thiệt hại thông tin trong và ngoài giờ làm việc chính thức. Chính sách này nên xét đến việc phân loại an ninh thông tin (xem 5.2), các rủi ro của việc áp dụng chính sách và các khía cạnh văn hoá của tổ chức.

Thông tin bị bỏ sót trên bàn cũng giống như bị thiệt hại hoặc phá huỷ trong một thảm hoạ như một vụ cháy, lụt hoặc nổ. Nên xem xét các kiểm soát sau đây:

a) KHI THÍCH HỢP, giấy tờ và các phương tiện truyền thông máy tính nên được lưu trữ trong các tủ có khoá phù hợp và/hoặc các vật chứa an toàn khác khi không sử dụng, đặc biệt ngoài giờ làm việc;

b) các thông tin doanh nghiệp có tính nhạy cảm hoặc phê bình nên được khóa an toàn (như các tủ hoặc nơi lưu an toàn chống cháy) khi không có nhu cầu, đặc biệt khi văn phòng không có người;

c) máy tính cá nhân và cổng in và các cổng khác của máy tính nên được đóng khi không dùng và nên được bảo vệ bằng các khóa mật mã, mật khẩu hoặc các kiểm soát khác khi không sử dụng;

d) các nơi thư đến hoặc đi, các máy telex, fax không hoạt động nên được bảo vệ;

e) các mày photo nên được khóa ngoài giờ làm việc chính thức (hoặc bảo đảm an toàn khỏi việc sử dụng trái phép bằng cách này cách khác);

f) thông tin nhạy cảm hoặc được phân loại, khi in xong nên được xoá ngay khỏi máy in.

7.3.2 Di chuyển tài sản

Thiết bị, thông tin hoặc phần mềm không nên mang ra ngoài nếu trái phép. Khi cần thiết và thích hợp, thiết bị nên được thoát ra và vào lại khi quay lại sử dụng. Kiểm tra tại chỗ nên được thi hành để phát hiện việc di chuyển tàl sản trái phép.

Các cá nhân nên được biết rằng các kiểm tra tại chỗ sẽ được tiến hành.

8 Quản lý truyền thông và hoạt động

8.1 Trách nhiệm và thủ tục hoạt động

Mục tiêu: Đảm bảo các phương tiện xử lý thông tin hoạt động đúng và an toàn.
Các trách nhiệm và các thủ tục đối với quản lý và vận hành toàn bộ phương tiện xử lý thông tin nên được thiết lập. Điều này bao gồm việc xây dựng các hướng dẫn vận hành thích hợp và các thủ tục đáp ứng với sự cố. Nên tiến hành phân tách trách nhiệm (xem 8.1.4), khi thích hợp, để giảm sự rủi ro do việc lạm dụng hệ thống một cách vô ý hoặc chủ tâm.

8.1.1 Thủ tục vận hành được tài liệu hóa

Các thủ tục vận hành được xác định bởi chính sách an ninh nên được tài liệu hóa và duy trì. Các thủ tục vận hành nên được coi như các tài liệu chính thức và các thay đổi phải được phép của ban quản lý.

Các thủ tục nên chỉ rõ các hướng dẫn cho việc điều hành mỗi công việc cụ thể bao gồm:

a) kiểm soát và xử lý thông tin;

b) lập kế hoạch các yêu cầu, bao gồm sự phụ thuộc với các hệ thống khác, các lần bắt đầu công việc sớm nhất và hoàn thành công việc muộn nhất;

c) các hướng dẫn xử lý các lỗi hoặc các trường hợp khác thường có thể xảy ra trong quá trình điều hành công việc, bao gồm các hạn chế trong việc sử dụng các tiện ích của hệ thống (xem 9.5.5);

d) các điểm hỗ trợ trong trường hợp gặp khó khăn về kỹ thuật hoặc vận hành không mong muốn;

e) các hướng dẫn kiểm soát dữ liệu ra đặc biệt, như là việc sử dụng đồ dùng văn phòng đặc biệt hoặc việc quản lý dữ liệu ra bảo mật, bao gồm các thủ tục đối với việc huỷ bỏ an toàn kết quả của các công việc lỗi;

f) các thủ tục khởi động lại và khôi phục lại hệ thống sử dụng trong trường hợp lỗi hệ thống.

Các thủ tục tài liệu hoá cũng nên được chuẩn bị cho các hoạt động quản lý hệ thống kết hợp với các phương tiện xử lý thông tin và truyền thông, như các thủ tục bật và tắt máy tính, sao lưu, bảo dưỡng thiết bị, quản lý và bảo vệ cho phòng máy và nơi xử lý tin.

8.1.2 Kiểm soát thay đổi hoạt động

Các thay đổi với các phương tiện xử lý thông tin và các hệ thống nên được kiểm soát. Việc kiểm soát các thay đổi đối với các phương tiện xử lý thông tin và các hệ thống không thích hợp là nguyên nhân chung của các lỗi về hệ thống và an toàn. Các trách nhiệm và các thủ tục quản lý chính thức nên được tiến hành để đảm bảo sự kiểm soát thoả đáng đối với toàn bộ các thay đổi về thiết bị, phần mềm hoặc các thủ tục. Các chương trình hoạt động nên được kiểm soát thay đổi nghiêm ngặt. Khi các chương trình bị thay đổi, một bảng kiểm toán bao gồm toàn bộ các thông tin liên quan nên được lưu lại. Các thay đổi đối với môi trường vận hành có thể ảnh hưởng đến các ứng dụng. Ở bất kỳ nơi tiến hành nào, các thủ tục kiểm soát sự thay đổi vận hành và ứng dụng nên thống nhất (xem thêm 10.5.1). Cụ thể, nên xem xét các kiểm soát sau đây:

a) định danh và lưu giữ các thay đổi quan trọng;

b) đánh giá sự ảnh hưởng tiềm ẩn của các thay đổi như vậy;

c) thủ tục chứng minh chính thức cho các thay đổi có mục đích;

d) thông tin các chi tiết thay đổi cho toàn bộ những người có liên quan;

e) thủ tục xác định các trách nhiệm bỏ qua và khôi phục các thay đổi không thành công.

8.1.3 Thủ tục quản lý sự cố

Các thủ tục và trách nhiệm quản lý sự cố nên được thiết lập để đảm bảo đáp ứng với các sự cố an ninh nhanh chóng, hiệu quả và có trình tự (xem thêm 6.3.1). Nên xem xét các kiểm soát sau đây:

a) các thủ tục nên được thiết lập đối với toàn bộ các loại sự cố an ninh tiềm ẩn, bao gồm:

   1) các sai sót của hệ thống thông tin và thiếu sót của dịch vụ;

   2) từ chối dịch vụ;

   3) lỗi do dữ liệu kinh doanh không đây đủ hoặc sai lệch;

   4) vi phạm tính bảo mật.

b) bên cạnh các kế hoạch đáp ứng với các sự bất ngờ thông thường (thiết kế để khôi phục hệ thống hoặc dịch vụ nhanh nhất có thể) các thủ tục cũng nên được xem xét (xem thêm 6.3.4):

   1) phân tích và xác định nguyên nhân của sự cố;

   2) lập kế hoạch và thực hiện các phương thức để ngăn ngừa việc tái diễn, nếu cần thiết;

   3) thu thập các dấu vết kiểm tra và chứng cớ tương tự;

   4) thông tin với các bên bị ảnh hưởng hoặc có liên quan với việc khôi phục sự cố;

   5) báo cáo hoạt động tới cấp có thẩm quyền phù hợp;

c) các dấu vết kiểm tra và chứng cớ tương tự nên được thu thập (xem 12.1.7) và duy trì hợp lý, để:

   1) phân tích các vấn đề nội bộ;

2) sử dụng làm chứng cớ có liên quan đến một vi phạm hợp đồng tiềm ẩn, vi phạm yêu cầu có tính điều chỉnh hoặc trong trường hợp các vụ kiện pháp lý hoặc phạm pháp, ví dụ lạm dụng máy tính hoặc luật bảo vệ dữ liệu;

3) đàm phán đền bù từ các nhà cung cấp phần mềm và dịch vụ;

d) hoạt động khôi phục các vi phạm an ninh và sửa chữa lỗi hệ thống nên được kiểm soát cẩn thận và đúng cách. Thủ tục này nên đảm bảo rằng:

1) chỉ nhân viên được xác nhận và có quyền rõ ràng mới được phép tiếp cận với các hệ thống và dữ liệu đang hoạt động (xem thêm 4.2.2 về việc truy cập của bên thứ ba);

2) toàn bộ các hoạt động khẩn cấp phải được ghi lại chi tiết;

3) hoạt động khẩn cấp phải được báo cáo tới ban quản lý và được giám sát một cách tuần tự;

4) tính toàn vẹn của các hệ thống và các kiểm soát kinh doanh phải được khẳng định với sự trì hoãn tối thiểu.

8.1.4 Phân tách trách nhiệm

Phân tách trách nhiệm là một biện pháp giảm rủi ro của việc lạm dụng hệ thống vô ý hoặc cố ý. Việc phân tách điều hành hoặc quản lý các nhiệm hoặc các phạm vi trách nhiệm để giảm cơ hội đối với các sửa đổi trái phép hoặc lạm dụng thông tin và dịch vụ nên được xem xét.

Các tổ chức nhỏ khó đạt kết quả với biện pháp này, nhưng nguyên tắc này nên được áp dụng triệt để có thể. Các bộ phận khó phân tách nên xét đến các kiểm soát khác như giám sát các hoạt động, dấu vết kiểm tra và giám sát quản lý. Điều quan trọng là kiểm tra an ninh phải độc lập.

Phải cẩn thận để không một cá nhân đơn lẻ nào có thể vi phạm gian lận trong các phạm vi trách nhiệm riêng mà không bị phát hiện. Khi bắt đầu một công việc nên phân tách ngay quyền hạn. Nên xem xét các kiểm soát sau đây:

a) điều quan trọng là phân tách các hoạt động yêu cầu có sự cấu kết để tránh gian lận, ví dụ việc tăng một đơn hàng mua bán và kiểm tra lại xem hàng đã được nhận chưa;

b) nếu có nguy hiểm trong sự cấu kết thì cần tạo ra các kiểm soát để tìm ra một số người liên quan để giảm khả năng của các âm mưu.

8.1.5 Phân tách về các phương tiện phát triển và hoạt động

Phân tách các phương tiện phát triển, thử nghiệm và hoạt động là việc quan trọng để đạt được thành công trong việc phân tách các vai trò có liên quan. Các quy tắc chuyển giao phần mềm từ trạng thái phát triển sang hoạt động nên được xác định và tài liệu hoá.

Các hoạt động phát triển và thử nghiệm có thể dẫn đến các vấn đề nghiêm trọng, ví dụ sự thay đổi không mong muốn các tệp tin hoặc môi trường hệ thống hoặc lỗi hệ thống. Xem xét mức độ phân tách giữa các môi trường phát triển, thử nghiệm và hoạt động là cần thiết để ngăn chặn các vấn đề khi hoạt động. Một sự phân tách tương tự cũng nên được thực hiện với các chức năng phát triển và thử nghiệm. Trong trường hợp này, cần

duy trì một môi trường quen thuộc và ổn định để việc thử nghiệm có ý nghĩa và ngăn ngừa được sự truy cập của các chuyên viên phát triển không thích hợp.

Các nơi mà nhân viên phát triển và thử nghiệm truy cập vào hệ thống hoạt động và các thông tin của nó, họ có thể đưa vào mã không được kiểm tra và trái phép hoặc thay đổi dữ liệu hoạt động. Trong một số hệ thống khả năng này có thể bị lạm dụng để phạm lỗi gian lận hoặc đưa vào mã không được kiểm tra hoặc có hại.

Mã không được kiểm tra và có hại có thể gây ra các vấn đề nghiêm trọng trong vận hành. Các chuyên viên phát triển và thử nghiệm cũng đưa ra một mối đe doạ đối với tính bảo mật của thông tin vận hành.

Các hoạt động phát triển và thử nghiệm có thể gây ra các thay đổi không định trước cho phần mềm và thông tin nếu họ cùng chia sẻ cùng một môi trường hoạt động máy tính. Vì vậy, phân tách các phương tiện phát triển, thử nghiệm và hoạt động là thoả đáng để giảm rủi ro của sự thay đổi bất ngờ hoặc việc truy cập trái phép vào phần mềm hoạt động và dữ liệu kinh doanh. Nên xem xét các kiểm soát sau đây:

a) phần mềm phát triển và hoạt động nên chạy trên các bộ vi xử lý máy tính khác nhau hoặc trong các miền hoặc thư mục khác nhau ở các nơi có thể;

b) các hoạt động phát triển và thử nghiệm nên phân tách càng xa càng tốt;

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

d) nên sử dụng các thủ tục đăng nhập khác nhau cho các hệ thống thử nghiệm và hoạt động để giảm rủi ro mắc lỗi. Người sử dụng nên được khuyến khích sử dụng các mật mã khác nhau cho các hệ thống này và các bảng chọn nên đưa ra các thông điệp xác nhận phù hợp;

e) nhân viên phát triển chỉ nên truy cập vào các mật khẩu hoạt động khi có sự kiểm soát đối với việc phát hành các mật khẩu cho việc hỗ trợ các hệ thống hoạt động. Các kiểm soát nên đảm bảo rằng các mật khẩu này được thay đổi sau khi sử dụng.

8.1.6 Quản lý các phương tiện bên ngoài

Việc sử dụng một nhà thầu bên ngoài để quản lý các phương tiện xử lý thông tin có thể dẫn đến việc lộ an ninh tiềm ẩn, như khả năng bị hại, tổn thất hoặc mất mát các dữ liệu ở các vị trí của nhà thầu. Các rủi ro này nên được xác định trước và các kiểm soát được thoả thuận với nhà thầu và được ghi trong hợp đồng (xem thêm 4.2.2 và 4.3 về hướng dẫn hợp đồng với bên thứ ba liên quan đến việc truy cập vào các phương tiện của tổ chức và các hợp đồng cung ứng).

Các vấn đề cụ thể nên được nói đến gồm:

a) xác định các ứng dụng có tính nhạy cảm hoặc phê bình tốt hơn là giữ trong một nhóm;

b) đạt được sự chấp nhận của các chủ sở hữu ứng dụng kinh doanh;

c) thực hiện các kế hoạch liên tục trong kinh doanh;

d) các tiêu chuẩn an ninh phải được xác định rõ và quá trình dự liệu sự tuân thủ;

e) sự phân bổ các trách nhiệm và thủ tục cụ thể để kiểm soát hiệu quả toàn bộ các hoạt động an ninh có liên quan;

f) các trách nhiệm và thủ tục báo cáo và xử lý các sự cố an ninh (xem 8.1.3).

8.2 Lập kế hoạch hệ thống và sự công nhận

Mục tiêu: Giảm thiểu rủi ro về lỗi hệ thống.
Yêu cầu lập kế hoạch và chuẩn bị trước để đảm bảo khả năng sẵn sàng của năng lực và các nguồn lực phù hợp.
Đặt các kế hoạch cho các yêu cầu năng lực trong tương lai để giảm rủi ro quá tải hệ thống.
Các yêu cầu vận hành của hệ thống mới nên được thiết lập, tài liệu hoá và kiểm tra trước khi tiếp nhận và sử dụng.

8.2.1 Lập kế hoạch về năng lực

Các nhu cầu năng lực nên được giám sát và lập kế hoạch cho các yêu cầu trong tương lai để đảm bảo rằng việc cung cấp nguồn lực và dự trữ thích hợp luôn sẵn sàng. Các kế hoạch này nên tính đến các hoạt động kinh doanh mới và yêu cầu của hệ thống cũng như xu hướng hiện tại và được lập kế hoạch trong quá trình xử lý thông tin của tổ chức.

Các máy tính lớn đòi hỏi sự chú ý riêng biệt, vì giá thành rất lớn và thời gian thay thế, nâng cấp lâu. Các nhà quản lý các dịch vụ chính nên kiểm soát việc sử dụng các nguồn hệ thống trọng yếu, bao gồm bộ vi xử lý, lưu trữ miền, tệp, cổng in và các cổng ra khác và các hệ thống truyền tin. Họ nên xác định xu hướng trong cách sử dụng, đặc biệt trong mối quan hệ với các ứng dụng kinh doanh và các công cụ quản lý hệ thống thông tin.

Các nhà quản lý nên sử dụng thông tin này để xác định và phòng ngừa các khả năng nút cổ chai có thể gây ra mối đe doạ cho an ninh hệ thống hoặc các dịch vụ cho người sử dụng và nên lập kế hoạch hoạt động ứng phó thích hợp.

8.2.2 Chấp nhận hệ thống

Tiêu chuẩn chấp nhận các hệ thống thông tin mới, nâng cấp và các phiên bản mới nên được thiết lập và các cuộc kiểm tra phù hợp của hệ thống nên được tiến hành trước khi tiếp nhận. Các nhà quản lý nên đảm bảo rằng các yêu cầu và tiêu chuẩn tiếp nhận các hệ thống mới phải được xác định rõ ràng, được chấp nhận, được tài liệu hoá và được kiểm tra. Nên xem xét các kiểm soát sau đây:

a) việc thực hiện và các yêu cầu năng lực máy tính;

b) khôi phục lỗi và thủ tục khởi động lại và các kế hoạch đáp ứng với sự bất ngờ;

c) chuẩn bị và kiểm tra thủ tục hoạt động thông thường để xác định các tiêu chuẩn;

d) bộ kiểm soát an ninh được chấp nhận đã sẵn sàng;

e) các thủ tục vận hành hiệu quả;

f) các sắp đặt liên tục trong kinh doanh, được yêu cầu ở 11.1;

g) bằng chứng cho việc lắp đặt hệ thống mới sẽ không ảnh hưởng bất lợi cho các hệ thống đang tồn tại, đặc biệt vào các thời điểm cao điểm cần xử lý, như vào cuối tháng;

h) bằng chứng cho việc xem xét tính hiệu quả của hệ thống mới trong an ninh chung của tổ chức;

i) đào tạo vận hành hoặc sử dụng các hệ thống mới.

Đối với các phát triển mới, các bộ phận vận hành và người sử dụng nên được tư vấn về toàn bộ các nấc trong quá trình phát triển để đảm bảo hiệu quả hoạt động của thiết kế hệ thống được đề xuất. Các cuộc kiểm tra phù hợp nên được tiến hành để chắc chắn rằng toàn bộ các tiêu chuẩn tiếp nhận được thoả mãn đầy đủ.

8.3 Bảo vệ chống lại phần mềm cố ý gây hại

Đối tượng: Để bảo vệ tính toàn vẹn của phầm mềm và thông tin. Yêu cầu có sự đề phòng trước để ngăn ngừa và phát hiện sự khởi đầu của phần mềm gây hại. Phần mềm và các phương tiện xử lý thông tin dễ bị tổn hại bởi sự khởi đầu của phần mềm gây hại, ví dụ các vi rút máy tính, sâu mạng, ngựa Trojan (xem 10.5.4) và bom logic. Người sử dụng nên có nhận thức về các nguy hiểm của phần mềm gây hại hoặc trái phép và các nhà quản lý nên hướng dẫn các cách kiểm soát đặc biệt ở các nơi thích hợp để phát hiện và ngăn ngừa sự hoạt động của nó. cụ thể, các đề phòng trước là cần thiết để phát hiện và ngăn ngừa vi rút máy tính vào máy tính cá nhân.

8.3.1 Kiểm soát chống lại phần mềm cố ý gây hại

Các kiểm soát nhằm phát hiện và ngăn ngừa để bảo vệ chống lại phần mềm gây hại và các thủ tục nhằm nhận thức người sử dụng thích hợp nên được thực hiện. các bảo vệ chống lại phần mềm gây hại nên dựa trên nhận thức an ninh, sự truy cập hệ thống phù hợp và các kiểm soát quản lý biến đổi. Nên xem xét các kiểm soát sau đây:

a) một chính sách chính thức đòi hỏi tuân theo giấy phép phần mềm và ngăn cấm việc sử dụng trái phép phần mềm (xem 12.1.2.2);

b) một chính sách chính thức để bảo vệ chống lại cá rủi ro liên quan đến việc sử dụng các tệp và phần mềm từ cả các mạng bên ngoài hoặc trên bất kỳ phương tiện truyền thông khác, cho biết các biện pháp bảo vệ được sử dụng (xem 10.5, đặc biệt 10.5.4 và 10.5.5);

c) việc lắp đặt và nâng cấp thông thường phần mềm chống virút và sửa chữa để quét máy vi tính và phương tiện truyền thông như một kiểm soát đề phòng trước trên một nền tảng thông thường;

d) chỉ đạo việc soát xét thông thường phần mềm và nội dụng dữ liệu của các hệ thống hỗ trợ các quá trình kinh doanh quyết định. Sự hiện diện của bất kỳ tệp không được chấp nhận hoặc các sửa đổi trái phép nên được điều tra một cách chính thức;

e) kiểm tra virút bất kỳ tệp nào trên phương tiện truyền thông điện tử có nguồn gốc không rõ ràng hoặc trái phép hoặc các tệp nhận được từ các mạng không đáng tin trước khi sử dụng ;

f) kiểm tra các phần mềm gây hại trên bất kỳ tệp gửi kèm thư điện tử hoặc các phần tải trên mạng trước khi sử dụng. Việc kiểm tra này nên được tiến hành ở nhiều vị trí khác nhau, ví dụ như các máy chủ thư điện tử, máy tính bàn hoặc ở các cổng mạng của tổ chức;

g) các thủ tục quản lý và các trách nhiệm giải quyết vấn đề bảo vệ chống virút trên các hệ thống, đào tạo việc sử dụng, báo cáo và khắc phục sự tấn công của virút (xem 6.3 và 8.1.3);

h) các kế hoạch liên tục trong kinh doanh phù hợp với việc khắc phục sự tấn công của virút, bao gồm toàn bộ dữ liệu cần thiết và phần mềm sao lưu và các sắp xếp khôi phục (xem mục 11);

i) các thủ tục thẩm tra toàn bộ thông tin liên quan đến phần mềm có hại và đảm bảo rằng bản tin cảnh báo chính xác và đầy đủ thông tin. Các nhà quản lý nên đảm bảo rằng các nguồn đủ tiêu chuẩn, ví dụ các báo chí danh tiếng, các địa chỉ mạng hoặc các nhà cung cấp phần mềm diệt virút đáng tin, được sử dụng để phân biệt các trò lừa và virút thực. Nhân viên nên nhận thức được vấn đề về các trò lừa bịp và phải làm gì khi nhận được chúng.

Các kiểm soát này đặc biệt quan trọng đối với các máy dịch vụ tập tin trong hệ thống hỗ trợ cho một số lượng lớn máy trạm.

8.4 Công việc cai quản

Đối tượng: Để duy trì tính toàn vẹn và tính sẵn sàng của các dịch vụ truyền đạt và xử lý thông tin.
Các thủ tục thông thường nên được thiết lập để thực hiện chiến dịch sao lưu được đồng ý (xem 11.1) làm các bản sao chép dữ liệu và nhắc nhở việc lưu trữ đúng lúc, ghi lại các sự kiện và các lỗi và ở các nơi cần thiết thì giám sát môi trường thiết bị.

8.4.1 Sao lưu thông tin

Các bản sao chép dự phòng thông tin và phần mềm kinh doanh cần thiết nên được thực hiện đều đặn. Nên cung cấp các phương tiện sao chép thích hợp để đảm bảo rằng toàn bộ thông tin và phần mềm kinh doanh cần thiết có thể được khôi phục sau một tai hoạ hoặc lỗi truyền thông. Sự sắp xếp sao chép các hệ thống cá nhân nên được kiểm tra đều dặn để đảm bảo rằng chúng đáp ứng các yêu cầu của các kế hoạch liên tục trong kinh doanh (xem mục 11). Nên xem xét các kiểm soát sau đây:

a) mức thông tin sao lưu nhỏ nhất, cùng với lưu trữ các bản sao chép dự phòng và các thủ tục lưu trữ được ghi chép lại chính xác và đầy đủ nên được lưu ở một nơi tách biệt, với khoảng cách đủ để thoát khỏi các hư hại do một tai hoạ xảy ra ở vị trí chính. Ít nhất 3 thế hệ hoặc 3 vòng đời của các thông tin sao lưu nên được giữ lại cho các ứng dụng kinh doanh quan trọng;

b) thông tin sao lưu nên có sự bảo vệ về vật lý và môi trường ở mức thích hợp (xem mục 7) phù hợp với các tiêu chuẩn được ứng dụng ở vị trí chính. Các kiểm soát ứng dụng cho phương tiện truyền thông ở vị trí chính nên được mở rộng để bao phủ cả vị trí sao chép;

c) nếu có thể, phương tiện truyền thông sao chép dự phòng nên được kiểm tra đều đặn để đảm bảo rằng chúng có thể chông cậy được trong lúc khẩn cấp khi cần;

d) các thủ tục lưu trữ nên được kiểm tra và thử nghiệm đều đặn để đảm bảo rằng chúng có hiệu quả và có thể được hoàn thành trong thời gian được phân phối trong các thủ tục hoạt động để khôi phục.

Khoảng thời gian lưu giữ thông tin kinh doanh cần thiết, cũng như bất kỳ yêu cầu lưu trữ vĩnh viễn các bản sao (xem 12.1.3) nên được xác định.

8.4.2 Các bản ghi của điều hành viên

Nhân viên vận hành nên duy trì một bản nhật ký các hoạt động của họ. Nếu phù hợp, bản này nên gồm:

a) thời gian bắt đầu và kết thúc hệ thống;

b) các lỗi hệ thống và hoạt động sửa chữa đã diễn ra;

c) xác nhận việc xử lý đúng các tệp dữ liệu và dữ liệu ra của máy tính;

d) tên của người ghi chép lịch ra vào.

Các bản ghi của điều hành viên phải có kiểm tra độc lập và đều đặn với các thủ tục hoạt động..

8.4.3 Ghi lại khiếm khuyết

Các lỗi nên được báo cáo và sửa chữa. Các lỗi được thông báo bởi người sử dụng các vấn đề liên quan đến hệ thống xử lý và truyền thông tin nên được ghi nhật ký. Các quy định để xử lý các lỗi được báo cáo nên bao gồm:

a) giám sát bản nhật ký lỗi để đảm bảo rằng các lỗi được giải quyết thỏa đáng;

b) giám sát các biện pháp đúng đắn để đảm bảo rằng các kiểm soát không bị tổn hại và hoạt động này được tiến hành có đầy đủ quyền.

8.5 Quản lý mạng

Đối tượng: Để đảm bảo việc bảo vệ thông tin trên các mạng và việc bảo vệ hạ tầng hỗ trợ. Việc quản lý an ninh mạng, mà có thể mở rộng ra phạm vi ngoài tổ chức, đòi hỏi được chú ý. các kiểm soát thêm cũng nên được yêu cầu để bảo vệ dữ liệu nhạy cảm đi qua các mạng công cộng.

8.5.1 Kiểm soát mạng

Một loạt các kiểm soát được yêu cầu để đạt được và duy trì an ninh trong các mạng máy tính. Các nhà quản lý mạng nên thực hiện các kiểm soát để đảm bảo an ninh của dữ liệu trong mạng và bảo vệ các dịch vụ được kết nối khỏi truy cập trái phép. Cụ thể, nên xem xét các kiểm soát sau đây:

a) trách nhiệm vận hành mạng nên được phân tách khỏi các hoạt động máy tính ở các chỗ thích hợp (Xem 8.1.4);

b) các trách nhiệm và các thủ tục quản lý thiết bị điều khiển xa, bao gồm thiết bị trong khu vực người sử dụng nên được thiết lập;

c) nếu cần thiết, kiểm soát đặc biệt nên được thiết lập để bảo đảm tính bảo mật và tính toàn vẹn của dữ liệu đi qua các mạng công cộng và để bảo vệ các hệ thống được kết nối (xem 9.4 và 10.3). Kiểm soát đặc biệt cũng có thể được yêu cầu để duy trì khả năng sẵn sàng của các dịch vụ mạng và máy tính được kết nối;

d) các hoạt động quản lý nên được phối hợp mật thiết để tối ưu dịch vụ cho doanh nghiệp đồng thời đảm bảo rằng các kiểm soát được áp dụng nhất quán qua hạ tầng xử lý thông tin.

8.6 Trình điều khiển và an ninh môi trường truyền thông

Đối tượng: Để ngăn ngừa tổn hại tới tài sản và gián đoạn các hoạt động của doanh nghiệp. Phương tiện truyền thông nên được kiểm soát và bảo vệ vật lý. Các thủ tục hoạt động thích hợp nên được thiết lập để bảo vệ các tài liệu, phương tiện truyền thông máy tính (các băng từ, các đĩa, các băng cátsét), dữ liệu ra/đầu vào và tài liệu hệ thống khỏi sự thiệt hại, hành vi đánh cắp và truy cập trái phép.

8.6.1 Việc quản lý của phương tiện truyền thông máy tính có thể tháo lắp được

Nên có các thủ tục quản lý phương tiện truyền thông máy tính có thể tháo lắp được, như các băng từ, các đĩa, các băng cátsét và các báo cáo in sẵn. Nên xem xét các kiểm soát sau đây:

a) nếu không có yêu cầu tiếp, các nội dung trước đó của bất kỳ phương tiện truyền thông có thể tái sử dụng mà phải được gỡ bỏ khỏi tổ chức đó nên được xóa đi;

b) toàn bộ các phương tiện truyền thông được gỡ bỏ khỏi tổ chức nên được cấp phép và một bản lưu chú toàn bộ các sự gỡ bỏ như vậy để duy trì một dấu vết kiểm tra nên được giữ lại (xem 8.7.2);

c) toàn bộ các phương tiện truyền thông nên được lưu trữ trong môi trường an toàn, an ninh, phù hợp với các quy định kỹ thuật của nhà sản xuất.

Toàn bộ các thủ tục và các mức cấp phép nên được tài liệu hóa một cách rõ ràng.

8.6.2 Sự chuyển nhượng môi trường truyền thông

Phương tiện truyền thông nên được hủy bỏ một cách an toàn và an ninh khi không được yêu cầu nữa. Thông tin nhạy cảm có thể lọt ra ngoài nếu việc hủy bỏ phương tiện truyền thông không cẩn thận. Các thủ tục chính thức cho việc hủy bỏ các phương tiện truyền thông an toàn nên được thiết lập để giảm thiểu tối đa rủi ro này. Nên xem xét các kiểm soát sau đây:

a) các phương tiện truyền thông bao gồm thông tin nhạy cảm nên được lưu trữ và hủy bỏ một cách an toàn và an ninh, ví dụ như đốt hoặc xé nhỏ hoặc làm rỗng dữ liệu sử dụng bằng một ứng dụng khác trong tổ chức.

b) danh sách sau đây xác định các mục có thể đòi hỏi sự hủy bỏ an toàn:

1) các tài liệu giấy;

2) việc ghi thoại hoặc các cái khác;

3) giấy than;

4) các báo cáo dữ liệu ra;

5) dải băng in sử dụng một lần;

6) các băng từ;

7) các đĩa hoặc các băng cátsét có thể tháo rời;

8) phương tiện lưu trữ quang học (toàn bộ các dạng và bao gồm toàn bộ các phương tiện truyền thông phân phối phần mềm của nhà sản xuất);

9) liệt kê danh sách chương trình;

10) dữ liệu thử nghiệm;

11) tài liệu hệ thống.

c) có thể dễ dàng sắp xếp toàn bộ các mục phương tiện truyền thông để thu thập và hủy bỏ an toàn, hơn là cố chia tách ra các mục nhạy cảm;

d) nhiều tổ chức đặt hàng các dịch vụ thu thập và hủy bỏ giấy tờ, thiết bị và các phương tiện truyền thông. Nên cẩn thận trong việc chọn lựa nhà thầu phù hợp với các kiểm soát và kinh nghiệm thích hợp;

e) việc hủy bỏ các mục nhạy cảm nên được ghi lại để duy trì một dấu vết kiểm tra;

Khi tập hợp các phương tiện truyền tin để hủy bỏ nên xem xét hậu quả có thể gây ra một số lượng lớn thông tin không được phân loại trở nên nhạy cảm hơn một số lượng nhỏ thông tin được phân loại.

8.6.3 Các thủ tục của trình điều khiển thông tin

Các thủ tục xử lý và lưu trữ thông tin nên được thiết lập để bảo vệ thông tin khỏi bị lộ hoặc lạm dụng trái phép. Các thủ tục nên được thảo ra để xử lý thông tin nhất quán với sự phân loại (xem 5.2) trong các tài liệu, hệ thống máy tính, mạng, tính toán lưu động, truyền thông lưu động, thư, thư thoại, truyền thoại nói chung, đa phương tiện, các dịch vụ/ thiết bị bưu điện, ứng dụng máy fax và các hạng mục nhạy cảm khác, ví dụ séc trắng, hóa đơn trắng. Nên xem xét các kiểm soát sau đây: (xem 5.2 và 8.7.2):

a) việc điều khiển và lập nhãn toàn bộ các phương tiện truyền thông [xem 8.7.2 a];

b) hạn chế truy cập để định danh cá nhân trái phép;

c) duy trì một bản lưu chính thức những người nhận dữ liệu được phép;

d) đảm bảo rằng dữ liệu đầu vào đầy đủ, quá trình được hoàn thành triệt để và kiểm tra tính hợp lệ đầu ra được áp dụng;

e) bảo vệ dữ liệu cuộn chờ dữ liệu ra ở mức phù hợp với tính nhạy cảm của nó;

f) lưu trữ phương tiện truyền thông trong môi trường phù hợp với các quy định kỹ thuật của nhà sản xuất;

g) duy trì sự phân phối dữ liệu ở mức tối thiểu;

h) đánh dấu rõ các bản sao dữ liệu để người nhận có phép chú ý;

i) xem xét các danh sách phân phối và danh sách những người nhận được phép vào các khoảng thời gian đều đặn.

8.6.4 An ninh tài liệu hệ thống

Tài liệu hệ thống có thể chứa một loạt thông tin nhạy cảm, ví dụ sự mô tả các ứng dụng, thủ tục, thủ tục, cấu trúc dữ liệu, thủ tục cấp phép (Xem 9.1). Nên xem xét các kiểm soát sau đây để bảo vệ tài liệu hệ thống khỏi truy cập trái phép.

a) tài liệu hệ thống nên được lưu trữ an toàn;

b) danh sách truy cập tài liệu hệ thống nên được giữ lại mức tối thiểu và phải được phép của chủ sở hữu ứng dụng;

c) tài liệu hệ thống bị giữ trong một mạng công cộng hoặc được cung cấp qua một mạng công cộng nên được bảo vệ thích hợp;

8.7 Các trao đổi thông tin và phần mềm

Đối tượng: Để ngăn ngừa mất mát, thay đổi hoặc sử dụng sai thông tin được trao đổi giữa các tổ chức.

Các trao đổi thông tin và phần mềm giữa các tổ chức nên được kiểm soát và nên được tuân theo bất kỳ pháp chế có liên quan nào (xem mục 12). Các trao đổi nên được tiến hành trên cơ sở của các thỏa thuận. Các thủ tục và các tiêu chuẩn để bảo vệ thông tin và phương tiện truyền thông chuyển tiếp được thiết lập. Doanh nghiệp và các hàm ý an ninh được kết hợp với trao đổi dữ liệu điện tử, thương mại điện tử và thư điện tử và các yêu cầu cho các kiểm soát nên được xem xét.

8.7.1 Các thỏa thuận trao đổi thông tin và phần mềm

Các thỏa thuận, một số là chính thức, bao gồm các thỏa thuận giao kèo phần mềm khi thích hợp nên được thiết lập cho việc trao đổi thông tin và phần mềm (hoặc bằng điện tử hoặc bằng tay) giữa các tổ chức. Nội dung an ninh của một thỏa thuận như vậy nên phản ánh tính nhạy cảm của thông tin kinh doanh liên quan. các thỏa thuận trên các điều kiện an ninh nên xem xét:

a) trách nhiệm quản lý việc kiểm soát và thông báo sự chuyển giao, gửi đi và tiếp nhận;

b) các thủ tục thông báo cho người gửi, việc chuyển giao, gửi và nhận;

c) các tiêu chuẩn kỹ thuật tối thiểu cho việc đóng gói và chuyển giao;

d) các tiêu chuẩn xác định người đưa tin;

e) trách nhiệm và nghĩa vụ pháp lý trong trường hợp mất dữ liệu;

f) sử dụng một hệ thống dán nhãn được thỏa thuận cho thông tin nhạy cảm hoặc có tính phê bình, đảm bảo rằng ý nghĩa của các nhãn hiệu này được hiểu ngay lập tức và thông tin đó được bảo vệ phù hợp;

g) các quyền sở hữu thông tin và phần mềm và các trách nhiệm đối với việc bảo vệ dữ liệu, sự tuân thủ bản quyền phần mềm và các xem xét tương tự (xem 12.1.2 và 12.1.4);

h) các tiêu chuẩn kỹ thuật để ghi và đọc thông tin và phần mềm;

i) mọi kiểm soát đặc biệt có thể được yêu cầu để bảo vệ các hạng mục nhạy cảm, như các khóa mật mã hóa (xem 10.3.5).

8.7.2 An ninh của môi trường truyền

Thông tin có thể bị tổn hại do truy cập trái phép, lạm dụng hoặc tham nhũng trong việc truyền tải vật lý, ví dụ khi gửi phương tiện truyền thông qua dịch vụ bưu điện hoặc qua người vận chuyển. Các kiểm soát sau đây nên được áp dụng để bảo vệ phương tiện truyền thông máy tính giữa các vị trí:

a) nên được sử dụng các phương tiện truyền hoặc người vận chuyển đáng tin cậy. Một danh sách những người vận chuyển được phép nên được thỏa thuận với ban quản lý và nên tiến hành một thủ tục kiểm tra định danh người vận chuyển;

b) đóng gói nên đảm bảo việc bảo vệ các nội dung khỏi mọi nguy hiểm vật lý có thể nảy sinh trong quá trình đi đường và phù hợp với các quy định kỹ thuật của nhà sản xuất;

c) kiểm soát đặc biệt nên được chọn, khi cần thiết, để bảo vệ thông tin nhạy cảm khỏi thay đổi và bị lộ một cách trái phép. Các ví dụ gồm:

1) sử dụng các container được khóa;

2) giao nhận bằng tay;

3) đóng gói chống lục lọi (phát hiện mọi cố gắng xâm nhập);

4) trong các trường hợp ngoại lệ, phân tách hàng ký gửi thành nhiều chuyến và gửi bằng nhiều đường khác nhau;

5) sử dụng các chữ ký điện tử và tính bảo mật sự mật mã hóa (xem 10.3).

8.7.3 An ninh thương mại điện tử

Thương mại điện tử có thể gồm việc sử dụng trao đổi dữ liệu điện tử (EDI), thư điện tử và các giao dịch trên mạng thông qua các mạng công cộng như Internet. Thương mại điện tử có thể bị tổn hại bởi một số mối đe dọa trên mạng có thể do hoạt động gian lận, tranh chấp hợp đồng và việc thay đổi hoặc bị lộ thông tin. Các kiểm soát nên được áp dụng để bảo vệ thương mại điện tử khỏi các mối đe dọa này. Sự xem xét vấn đề an ninh cho thương mại điện tử nên gồm các kiểm soát sau đây:

a) xác nhận quyền. Khách hàng và người giao dịch yêu cầu mức bảo mật nào trong mỗi định danh được đòi hỏi khác nhau?

b) quyền. Ai được phép định giá, phát hành hoặc ký các văn bản giao dịch quan trọng? Đối tác thương mại biết về điều đó như thế nào?

c) hợp đồng và các quá trình. Các yêu cầu về tính bảo mật, tính toàn vẹn và bằng chứng gửi và nhận các văn bản quan trọng và không bác bỏ hợp đồng là gì?

d) định giá thông tin. Tính toàn vẹn của bảng giá được quảng cáo tính bảo mật của các dàn xếp giảm giá nhạy cảm có mức tin tưởng bao nhiêu?

e) các giao dịch đặt hàng. Tính bảo mật và tính toàn vẹn của đơn hàng, chi tiết địa chỉ thanh toán và vận chuyển và sự xác nhận của người nhận được cung cấp như thế nào?

f) hiệu định. Mức xem xét phù hợp với việc kiểm tra thông tin thanh toán do khách hàng cung cấp?

g) thanh toán. Cách thanh toán phù hợp nhất để bảo vệ chống sự gian lận?

h) đặt hàng. Bảo vệ được yêu cầu để duy trì tính bảo mật và toàn vẹn cua thông tin đặt hàng và chống lại sự mất mát hoặc sao lại các giao dich?

i) trách nhiệm pháp lý. Người gây rủi ro đối với các giao dịch gian lận?

Nhiều sự xem xét ở trên có thể được dùng bằng cách áp dụng các kỹ thuật mật mã hóa được phác thảo ở mục 10.3, xem xét sự tuân thủ các yêu cầu pháp luật (xem 12.1, đặc biệt 12.1.6 đối với luật mật mã hóa).

Các dàn xếp thương mại điện tử giữa các đối tác thương mại nên được hỗ trợ bằng một văn bản thỏa thuận ràng buộc các bên với các điều khoản giao dịch thỏa thuận, bao gồm chi tiết của quyền hạn [xem mục b ở trên]. Các thỏa thuận khác với các nhà cung cấp dịch vụ thông tin và mạng giá trị gia tăng có thể cần thiết.

Các hệ thống giao dịch công cộng nên công khai hóa các điều khoản kinh doanh của mình cho khách hàng.

Nên xem xét tính khả năng khôi phục tấn công của máy chủ thương mại điện tử và các ứng dụng an ninh của mạng nội bộ được yêu cầu cho việc thi hành đó (xem 9.4.7).

8.7.4 An ninh thư điện tử

8.7.4.1 Các rủi ro an ninh

Thư điện tử hiện nay được dùng trong trao đổi thông tin trong kinh doanh, thay thế cho các dạng trao đổi thông tin truyền thống là telex và thư. Thư điện tử khác các dạng truyền thống, ví dụ tốc độ, cấu trúc tin nhắn, mức độ không chính thức và dễ bị tổn hại bởi các hoạt động trái phép. Cần xem xét các kiểm soát để giảm các rủi ro an ninh do thư điện tử tạo ra. Các rủi ro an ninh bao gồm:

a) điểm yếu của các thông điệp bởi truy cập trái phép, thay đổi hoặc từ chối dịch vụ;

b) điểm yếu do lỗi, ví dụ xác định sai hoặc không hướng dẫn và tính tin cậy và tính sẵn có nói chung của dịch vụ;

c) tác động của sự thay đổi phương tiện trao đổi thông tin trong các quá trình kinh doanh, ví dụ ảnh hưởng của tốc độ truyền tăng hoặc ảnh hưởng của việc gửi thông điệp chính thức từ cá nhân đến cá nhân hơn là giữa công ty với công ty;

d) xem xét về mặt pháp lý, như là nhu cầu lớn về chứng minh nguồn gốc, việc truyền, phân phối và chấp nhận;

e) hàm ý phát hành các danh sách nhân viên có thể truy cập bên ngoài;

f) kiểm soát từ xa việc truy cập của người sử dụng và tài khoản thư điện tử.

8.7.4.2 Chính sách về thư điện tử

Các tổ chức nên thảo ra một chính sách rõ ràng đối với việc sử dụng thư điện tử, bao gồm:

a) các tấn công thư điện tử, ví dụ virút, nghe trộm;

b) bảo vệ các tệp đi kèm thư điện tử;

c) các hướng dẫn khi không sử dụng thư điện tử;

d) trách nhiệm nhân viên không được làm tổn hại đến công ty, ví dụ gửi thư điện tử nói xấu, sử dụng để quấy rối, mua bán trái phép;

e) sử dụng kỹ thuật mật mã hóa để bảo vệ tính bảo mật và tính toàn vẹn của các thông điệp điện tử (xem 10.3);

f) sở hữu các thông điệp có thể bị phát hiện trong trường hợp tranh chấp, nếu được lưu trữ;

g) các kiểm soát thêm đối với việc xem xét chặt chẽ việc truyền thông điệp không thể xác minh.

8.7.5 An ninh các hệ thống văn phòng điện tử

Các chính sách và các hướng dẫn nên được chuẩn bị và thực hiện để kiểm soát doanh nghiệp và các rủi ro an ninh được kết hợp với các hệ thống văn phòng điện tử. Điều này tạo cơ hội cho việc phổ biến và chia sẻ nhanh hơn thông tin doanh nghiệp sử dụng một sự kết hợp các tài liệu, máy tính, máy tính di động, truyền thông lưu động, thư, thư thoại, truyền thông thoại nói chung, đa phương tiện, các dịch vụ/ thiết bị bưu điện và máy fax.

Việc xem xét sự liên quan của an ninh và kinh doanh với kết nối nội bộ của các phương tiện như trên nên bao gồm:

a) khả năng dễ bị tấn công của thông tin trong các hệ thống văn phòng, ví dụ việc lưu các cuộc gọi điện thoại hoặc hộp thoại, tính bảo mật của các cuộc gọi, lưu trữ các bản fax, mở thư, phân phát thư;

b) chính sách và các kiểm soát phù hợp để quản lý việc chia sẻ thông tin, ví dụ việc sử dụng các bảng tin điện tử chung (xem 9.1);

c) loại bỏ các loại thông tin kinh doanh nhạy cảm nếu hệ thống không có mức bảo vệ phù hợp (xem 5.2);

d) hạn chế truy cập tới thông tin ghi nhớ liên quan đến các cá nhân được lựa chọn, ví dụ nhân viên làm việc trong các dự án nhạy cảm;

e) sự phù hợp của hệ thống để hỗ trợ các ứng dụng kinh doanh, như các yêu cầu và quyền hạn trao đổi thông tin;

f) các loại nhân viên, nhà thầu hoặc đối tác kinh doanh phải được phép sử dụng hệ thống và các vị trí truy cập (xem 4.2);

g) hạn chế các phương tiện được lựa chọn để quy định phân loại người sử dụng;

h) xác định tình trạng người sử dụng, ví dụ những người lao động của tổ chức đó hoặc các nhà thầu trong các mục vì lợi ích của người sử dụng khác;

i) lưu giữ và sao chép dự phòng thông tin trong hệ thống (xem 12.1.3 và 8.4.1);

j) các yêu cầu và các sắp xếp dự trữ (xem 11.1).

8.7.6 Các hệ thống công cộng sẵn có

Nên bảo vệ cẩn thận tính toàn vẹn của thông tin được truyền công khai qua điện tử để ngăn ngừa sự thay đổi trái phép có thể gây hại đến danh tiếng của tổ chức. Thông tin trong một hệ thống công cộng, ví dụ thông tin trên trang web có thể truy cập qua internet, cần tuân thủ pháp luật, các luật và quy định trong phạm vị thực thi mà hệ thống được định vị hoặc nơi trao đổi đang diễn ra. Có thể có một thủ tục cấp phép trước khi thông tin được đưa ra công cộng.

Các phần mềm, dữ liệu và thông tin khác đòi hỏi mức toàn vẹn cao, được công bố trong một hệ thống công cộng nên được bảo vệ bằng các kỹ thuật phù hợp, ví dụ các chữ ký điện tử (xem 10.3.3). Hệ thống điện tử công cộng, đặc biệt những cái cho phép phản hồi và thêm thông tin trực tiếp nên được kiểm soát cẩn thận để:

a) thông tin thu được tuân theo luật bảo vệ dữ liệu (xem 12.1.4);

b) thông tin vao và xử lý trong hệ thống công bố công cộng sẽ được xử lý đầy đủ và chính xác một cách kịp thời;

c) thông tin nhạy cảm sẽ được bảo vệ trong quá trình thu thập và khi được lưu trữ;

d) truy cập tới hệ thống công cộng trái phép truy cập không định hướng trước tới các mạng được kết nối cùng.

8.7.7 Các biểu mẫu trao đổi thông tin khác

Các thủ tục và kiểm soát nên được tiến hành để bảo vệ sự trao đổi thông tin thông qua việc sử dụng các phương tiện truyền thông âm thanh, sao chép và video. Thông tin có thể bị tổn hại do thiếu nhận thức, chính sách hoặc các thủ tục sử dụng các phương tiện, ví dụ việc nghe trộm điện thoại di động ở các nơi công cộng, các máy trả lời tự động bị nghe trộm, truy cập trái phép tới các hệ thống thư thoại hoặc gửi không đảm bảo các sao chép cho không đúng người đang sử dụng thiết bị sao chép.

Các hợp tác kinh doanh có thể bị phá vỡ và thông tin có thể bị tổn hại nếu các phương tiện trao đổi thông tin hỏng, bị quá tải hoặc gián đoạn (xem 7.2 và mục 11). Thông tin cũng có thể bị tổn hại nếu bị truy cập bởi người sử dụng trái phép (xem mục 9).

Nên thiết lập một chính sách rõ ràng, nêu rõ các thủ tục mà nhân viên phải làm theo trong việc sử dụng các phương tiện trao đổi thông tin âm thanh, sao chép và video. chính sách này nên gồm:

a) nhắc nhở nhân viên đề phòng phù hợp, ví dụ không tiết lộ thông tin nhạy cảm để bị nghe trộm hoặc bị chặn khi gọi điện bởi:

1) những người ở gần đặc biệt khi sử dụng điện thoại di động;

2) thủ đoạn nghe trộm bằng cách đấu đường dây và các dạng khác nghe trộm khác qua truy cập vật lý tới máy phát cầm tay hoặc đường dây điện thoại hoặc sử dụng máy thu rađa khi dùng các máy điện thoại di động tương tự;

3) người nhận cuối cùng;

b) nhắc nhở nhân viên không nên có các cuộc trao đổi bí mật ở các nơi công cộng hoặc các văn phòng mở và các nơi họp có tường mỏng;

c) không để các thông điệp ở máy trả lời tự động vì có thể bị những người trái phép bật lại, lưu trữ ở các hệ thống công cộng hoặc lưu trữ không đúng là kết quả của việc quay sai số;

d) nhắc nhở nhân viên về các vấn đề sử dụng máy sao chép, cụ thể là:

1) truy cập trái phép vào các nơi lưu trữ thông điệp cố định để lấy lại các thông điệp;

2) lập chương trình cẩn thận hoặc ngẫu nhiên cho các máy để gửi các thông điệp tới các số cụ thể;

3) gửi các văn bản và thông điệp tới số sai do quay nhầm số và sử dụng sai số lưu trữ.

9 Kiểm soát truy cập

9.1 Yêu cầu kinh doanh đối với kiểm soát truy cập

Đối tượng: Để kiểm soát truy cập thông tin. Truy cập thông tin và các quá trình kinh doanh nên được kiểm soát trên cơ sở các yêu cầu kinh doanh và an ninh. Điều này nên xét đến các chính sách phổ biến thông tin và cấp phép.

9.1.1 Chính sách kiểm soát truy cập

9.1.1.1 Chính sách và yêu cầu kinh doanh

Các yêu cầu của doanh nghiệp đối với kiểm soát truy cập nên được xác định và ghi thành văn bản. các quy định và quyền kiểm soát truy cập đối với mỗi người sử dụng hoặc nhóm người sử dụng nên được công bố rõ ràng trong một bản công bố chính sách truy cập. Người sử dụng và các nhà cung cấp dịch vụ nên được nhận một bản công bố rõ ràng các yêu cầu của doanh nghiệp để đáp ứng các kiểm soát truy cập.

Chính sách này nên xét đến các điều sau:

a) các yêu cầu an ninh của các ứng dụng kinh doanh cá thể;

b) xác định toàn bộ các thông tin liên quan đến các ứng dụng kinh doanh;

c) các chính sách phổ biến thông tin và cấp phép, ví dụ nhu cầu biết mức nguyên tắc và an ninh và phân loại thông tin;

d) tính nhất quán giữa kiểm soát truy cập và các chính sách phân loại thông tin của các hệ thống và mạng khác nhau;

e) luật lệ và mọi nghĩa vụ giao kèo liên quan đối với sự bảo vệ truy cập dữ liệu và các dịch vụ (xem mục 12);

f) sơ lược truy cập của người sử dụng tiêu chuẩn đối với các loại công việc chung;

g) việc quản lý quyền truy cập trong một môi trường rải rác và được nối mạng mà nhận diện được toàn bộ các loại kết nối sẵn có.

9.1.1.2 Các quy tắc kiểm soát truy cập

Trong việc định rõ các quy tắc kiểm soát truy cập nên được cẩn thận với các vấn đề sau:

a) việc phân định rõ giữa các quy tắc luôn phải tuân theo và các quy tắc có thể lựa chọn hoặc có điều kiện;

b) thiết lập các quy tắc dựa trên giả thuyết "Nói chung cái gì phải bị ngăn cấm trừ khi được cho phép rõ ràng" hơn là quy tắc "Nói chung, mọi thứ được cho phép trừ khi bị ngăn cấm rõ ràng";

c) các thay đổi trong các nhãn thông tin (xem 5.2) được khởi tạo tự động bởi các phương tiện xử lý thông tin và các thay đổi được khởi tạo tự ý của người sử dụng;

d) các thay đổi trong các chấp nhận người sử dụng được khởi tạo tự động bởi phương tiện xử lý thông tin và các thay đổi được khởi tạo bởi một nhà quản trị;

e) các quy tắc đòi hỏi nhà quản trị hoặc sự phê chuẩn khác trước khi ban hành và các nguyên tắc không yêu cầu.

9.2 Quản lý truy cập người sử dụng

Đối tượng: Để ngăn ngừa truy cập trái phép to các hệ thống thông tin.

Các thủ tục chính thức nên được tiến hành để kiểm soát sự phân phối các quyền truy cập tới các hệ thống thông tin và các dịch vụ. Các thủ tục nên bao toàn bộ các cấp trong vòng đời truy cập của người sử dụng, từ sự đăng ký ban đầu của người sử dụng mới tới việc cuối cùng xoá tên người sử dụng không yêu cầu truy cập các hệ thống thông tin và dịch vụ nữa. Ở những nơi phù hợp, nên chú ý đặc biệt đến nhu cầu kiểm soát sự phân phối quyền truy cập có đặc quyền cho phép người sử dụng vượt qua các kiểm soát hệ thống.

9.2.1 Đăng ký người sử dụng

Nên có một thủ tục chính thức đối với việc đăng ký và xóa tên người sử dụng để chấp nhận việc truy cập tới toàn bộ các hệ thống thông tin và dịch vụ nhiều người sử dụng cùng một lúc.

Truy cập tới các dịch vụ thông tin nhiều người sử dụng cùng lúc nên được kiểm soát thông qua một thủ tục đăng ký người sử dụng chính thức nên gồm:

a) sử dụng một tên truy cập cá nhân duy nhất để người sử dụng có thể kết nối và chịu trách nhiệm với các hoạt động của mình. Việc sử dụng tên truy cập theo nhóm chỉ nên được cho phép khi phù hợp với công việc được tiến hành;

b) kiểm tra xem người sử dụng có được phép của chủ hệ thống để sử dụng hệ thống hoặc dịch vụ thông tin. phân tách quyền cho phép truy cập trong ban quản lý cho phù hợp;

c) kiểm tra mức cho phép truy cập có phù hợp với mục đích doanh nghiệp (xem 9.1) và có nhất quán với chính sách an ninh của tổ chức, ví dụ không làm tổn hại đến việc phân tách trách nhiệm (xem 8.1.4);

d) đưa cho người sử dụng một bản công bố quyền truy cập của họ;

e) yêu cầu người sử dụng ký các bản kê để chỉ ra rằng họ hiểu các điều kiện truy cập;

f) đảm bảo các nhà cung cấp dịch vụ không cho phép truy cập cho đến khi các thủ tục cấp phép hoàn thành;

g) duy trì một bản lưu chính thức toàn bộ những người đăng ký sử dụng dịch vụ;

h) bỏ quyền truy cập của người sử dụng ngay khi người sử dụng thay đổi công việc hoặc rời tổ chức;

i) kiểm tra định kỳ để xóa bỏ các tên truy cập và tài khoản cá nhân không cần thiết;

j) đảm bảo rằng các tên truy cập cá nhân dư thừa không được phát hành cho người sử dụng khác.

Nên xem xét các mục trong hợp đồng nhân sự và hợp đồng dịch vụ chỉ rõ hình phạt nếu các nhân viên hoặc đại lý dịch vụ cố ý truy cập trái phép (xem 6.1.4 và 6.3.5).

9.2.2 quản lý đặc quyền

Sự phân phối và sử dụng các đặc quyền (bất kỳ đặc trưng hoặc khả năng của hệ thống thông tin nhiều người sử dụng cùng lúc cho phép người sử dụng vượt qua các kiểm soát hệ thống hoặc ứng dụng) nên được hạn chế và kiểm soát. Việc sử dụng không phù hợp các đặc quyền hệ thống thường là nhân tố chính góp phần vào sự hư hỏng của các hệ thống bị xâm phạm.

Các hệ thống nhiều người sử dụng cùng lúc đòi hỏi sự bảo vệ chống lại truy cập trái phép nên có sự kiểm soát việc phân phối đặc quyền thông qua một quá trình cấp phép chính thức. Các bước sau nên được xem xét:

a) nên xác định các đặc quyền kết hợp với mỗi sản phẩm hệ thống, ví dụ hệ thống vận hành, hệ thống quản lý cơ sở dữ liệu và mỗi ứng dụng và các loại nhân viên cần được phân phối;

b) các đặc quyền nên được phân phối cho các cá nhân trên cơ sở cần sử dụng và nền tảng từng sự kiện một, nghĩa là yêu cầu tối thiểu cho vai trò chức năng của họ chỉ khi cần thiết;

c) một quy trình cấp quyền và một bản lưu toàn bộ các đặc quyền được phân phối nên được bảo lưu. Các đặc quyền không nên được cho phép cho đến khi quy trình cấp quyền hoàn tất;

d) việc phát triển và sử dụng các quy trình hệ thống nên được thúc đẩy để tránh nhu cầu cấp bách đặc quyền cho người sử dụng;

e) các đặc quyền nên được ấn định cho một định danh người sử dụng khác từ các đặc quyền được dùng cho việc sử dụng của doanh nghiệp thông thường.

9.2.3 Quản lý mật khẩu người sử dụng

Các mật khẩu có ý nghĩa chung là xác định tính hợp lệ của tên truy cập của người sử dụng khi truy cập vào hệ thống hoặc dịch vụ thông tin. Sự phân phối các mật khẩu nên được kiểm soát thông qua một quá trình quản lý chính thức và việc tiếp cận nên:

a) yêu cầu người sử dụng ký kết một bản kê để giữ bí mật các mật khẩu cá nhân và các mật khẩu làm việc nhóm chỉ trong các thành viên của nhóm (điều này có thể thêm vào trong các điều khoản và điều kiện thuê nhân công (xem 6.1.4);

b) ở những nơi người sử dụng được yêu cầu duy trì các mật khẩu riêng của họ, đảm bảo rằng lúc đầu họ được cung cấp một mật khẩu tạm thời an toàn mà họ buộc phải thay đổi ngay lập tức. Các mật khẩu tạm thời cung cấp khi người sử dụng quên mật khẩu của họ chỉ nên được cấp theo định danh chắc chắn người sử dụng;

c) yêu cầu đưa các mật khẩu tạm thời cho người sử dụng một cách an toàn. Nên tránh việc sử dụng của các bên thứ ba hoặc các thông điệp thư điện tử không được bảo vệ (văn bản trắng). Người sử dụng nên thông báo đã nhận được các mật khẩu.

Các mật khẩu không bao giờ nên lưu trong hệ thống máy tính ở dạng không được bảo vệ (xem các công nghệ khác để định danh và xác nhận người sử dụng, như sinh trắc học, ví dụ xác minh dấu vân tay, xác minh chữ ký và sử dụng các thẻ phần cứng, ví dụ thẻ chip, sẵn sàng và nên được cân nhắc nếu phù hợp.

9.2.4 Soát xét các quyền truy cập của người sử dụng

Để duy trì kiểm soát hiệu quả đối với việc truy cập tới các dịch vụ dữ liệu và thông tin, ban quản lý nên tiến hành một quy trình chính thức sau mỗi khoảng thời gian đều đặn để soát xét quyền truy cập của người sử dụng để:

a) quyền truy cập của người sử dụng được soát xét sau mỗi khoảng thời gian đều đặn (giả sử theo định kỳ 6 tháng) và sau bất kỳ sự thay đổi nào (xem 9.2.1);

b) việc cấp đặc quyền truy cập đặc biệt (xem 9.2.2) nên được soát xét sau khoảng thời gian ngắn hơn, giả sử theo định kỳ 3 tháng;

c) phân phối đặc quyền được kiểm tra thường sau mỗi khoảng thời gian đều đặn để đảm bảo rằng không có các đặc quyền trái phép.

9.3 Trách nhiệm của người sử dụng

Đối tượng: Để ngăn ngừa người sử dụng truy cập trái phép. Sự phối hợp của người sử dụng được cấp phép là cần thiết để an ninh có hiệu quả. Người sử dụng nên có nhận thức về các trách nhiệm của họ đối với việc duy trì kiểm soát truy cập hiệu quả, đặc biệt đối với việc sử dụng các mật khẩu và an ninh của thiết bị của người sử dụng.

9.3.1 Sử dụng mật khẩu

Người sử dụng nên theo các thông lệ an ninh tốt trong việc lựa chọn và sử dụng các mật khẩu.

Các mật khẩu có ý nghĩa xác định tính hợp lệ của tên truy nhập của người sử dụng và như vậy sẽ thiết lập quyền truy cập tới các phương tiện xử lý thông tin hoặc các dịch vụ. Toàn bộ người sử dụng được khuyên phải:

a) giữ bí mật các mật khẩu;

b) tránh giữ lại một tờ giấy ghi mật khẩu, trừ phi nó được lưu giữ an toàn;

c) thay đổi mật khẩu bất kỳ lúc nào có dấu hiệu hệ thống hoặc mật khẩu có thể bị tổn hại;

d) chọn các mật khẩu có chất lượng với độ dài ít nhất 6 ký tự và:

1) dễ nhớ;

2) không dựa trên bất kỳ cái gì mà một ai khác có thể dễ dàng đoán ra hoặc có được các thông tin liên quan đến cá nhân, ví dụ tên, số điện thoại, ngày sinh v..v.;

3) tránh các nhóm ký tự giống nhau liên tiếp hoặc các số hoặc các chữ cái.

e) thay đổi các mật khẩu sau mỗi khoảng thời gian đều đặn hoặc theo những lần truy cập (các mật khẩu của cá tài khoản đặc quyền nên được thay đổi thường xuyên hơn các mật khẩu thông thường) và tránh sử dụng lại, quay lại các mật khẩu cũ;

f) thay đổi mật khẩu tạm thời vào lần khởi động đầu tiên;

g) không tính đến các mật khẩu trong bất kỳ quá trình khởi động tự động hoá nào, ví dụ được lưu trữ trong một phím chức năng hoặc macro;

h) không chia sẻ các mật khẩu cá nhân.

Nếu người sử dụng cần truy cập các dịch vụ phức tạp hoặc các nền tảng cơ sở và được yêu cầu duy trì các mật khẩu phức tạp, họ nên được khuyên nên dùng mật khẩu đơn, có chất lượng [xem mục d) ở trên] đối với toàn bộ các dịch vụ có một mức bảo vệ mật khẩu lưu trữ hợp lý.

9.3.2 Thiết bị người sử dụng không được giám sát

Người sử dụng nên đảm bảo rằng các thiết bị không được giám sát có sự bảo vệ thích hợp. Thiết bị lắp đặt ở các khu vực của người sử dụng, ví dụ các máy trạm hoặc các máy dịch vụ tập tin, đòi hỏi sự bảo vệ đặc biệt khỏi truy cập trái phép khi không được giám sát trong thời gian làm thêm. Toàn bộ người sử dụng và các nhà thầu nên có nhận thức về các yêu cầu an ninh và các thủ tục bảo vệ các thiết bị không được giám sát, cũng như các trách nhiệm của họ đối với việc thực hiện sự bảo vệ này. Người sử dụng được khuyên phải:

a) chấm dứt các bộ phận hoạt động khi kết thúc, trừ khi các bộ phận đó có thể được an toàn bằng một kỹ thuật khoá phù hợp, ví dụ một mật khẩu bảo vệ màn hình;

b) ngừng hoàn toàn các máy tính lớn khi bộ phận này kết thúc (nghĩa là: không chỉ tắt PC mà cả các cổng);

c) bảo vệ các PC và cổng khỏi bị sử dụng trái phép bằng một khóa hoặc một kiểm soát tương đương, ví dụ mật khẩu truy cập, khi không sử dụng nữa.

9.4 Kiểm soát truy cập mạng

Đối tượng: Sự bảo vệ của các dịch vụ được nối mạng.

Truy cập tới các dịch vụ được nối mạng cả nội bộ và bên ngoài nên được kiểm soát. điều này là cần thiết để đảm bảo rằng người sử dụng truy cập và các mạng và các dịch vụ của mạng không làm tổn hại đến an ninh của các dịch vụ mạng này bằng việc đảm bảo:

a) các giao diện phù hợp giữa mạng của tổ chức và các mạng của các tổ chức khác hoặc các mạng công cộng;

b) các kỹ thuật xác minh người sử dụng và thiết bị phù hợp;

c) kiểm soát việc truy cập của người sử dụng vào các dịch vụ thông tin.

9.4.1 Chính sách về sử dụng các dịch vụ mạng

Các kết nối không an toàn tới các dịch vụ mạng có thể ảnh hưởng đến toàn bộ tổ chức. Người sử dụng chỉ nên được truy cập trực tiếp tới các dịch vụ mà họ được phép sử dụng rõ ràng. Kiểm soát này đặc biệt quan trọng đối với các kết nối mạng tới các ứng dụng kinh doanh nhạy cảm hoặc có tính phê bình hoặc tới người sử dụng trong khu vực rủi ro cao, ví dụ các khu vực công cộng hoặc bên ngoài mà nằm ngoài tầm kiểm soát và quản lý an ninh của tổ chức.

Một chính sách nên được trình bày rõ ràng chính xác về việc sử dụng các mạng và dịch vụ mạng. Điều này nên bao gồm:

a) các mạng và dịch vụ mạng được phép mới được truy cập;

b) các thủ tục cấp phép để xác định rõ người được phép truy cập các mạng và dịch vụ mạng đó;

c) các kiểm soát và thủ tục quản lý để bảo vệ truy cập tới các kết nối mạng và dịch vụ mạng.

d) chính sách này nên được thống nhất với chính sách kiểm soát truy cập của doanh nghiệp (xem 9.1).

9.4.2 Đường dẫn bắt buộc

Đường dẫn từ cổng của người sử dụng tới dịch vụ máy tính có thể cần phải kiểm soát. Các mạng được thiết kế cho phép phạm vi tối đa việc chia sẻ các nguồn và sự linh hoạt của lộ trình. Những đặc tính này có thể cũng tạo ra những cơ hội truy cập trái phép vào các ứng dụng của doanh nghiệp hoặc sử dụng trái phép các phương tiện xử lý thông tin. Các kiểm soát kết hợp mà hạn chế lộ trình giữa cổng của người sử dụng và các dịch vụ tin học mà người sử dụng được phép truy cập, ví dụ tạo ra một đường dẫn bắt buộc, có thể giảm các rủi ro như vậy.

Mục đích của đường dẫn bắt buộc là ngăn bất kỳ người sử dụng lựa chọn các lộ trình ngoài lộ trình giữa cổng của người sử dụng và các dịch vụ mà người sử dụng được phép truy cập.

Điều này thường yêu cầu việc thực hiện một số kiểm soát tại các điểm khác nhau trong lộ trình. Quy tắc này là để giới hạn các lựa chọn lộ trình tại mỗi điểm trong mạng qua các lựa chọn xác định trước.

Các ví dụ cho điều này như sau:

a) phân phối các đường hoặc số điện thoại chuyên dụng;

b) kết nối các cảng tự động để xác minh các hệ thống ứng dụng và các cổng ra vào an ninh;

c) hạn chế các lựa chọn trình đơn và trình đơn phụ cho các cá nhân sử dụng;

d) ngăn ngừa việc đi trong mạng không giới hạn;

e) bắt buộc việc sử dụng các hệ thống ứng dụng được định rõ và/choặc các cổng ra vào an ninh đối với người sử dụng mạng bên ngoài;

f) kiểm soát tích cực nguồn được phép cho các truyền thông đích qua các cổng ra vào an ninh, ví dụ các tường lửa;

g) hạn chế truy cập mạng bằng việc thiết lập các miền logic riêng biệt, ví dụ các mạng tư nhân ảo, đối với các nhóm sử dụng trong tổ chức (xem 9.4.6).

Các yêu cầu cho một đường dẫn bắt buộc nên dựa trên chính sách kiểm soát truy cập của doanh nghiệp (xem 9.1).

9.4.3 Xác thực người sử dụng đối với các kết nối bên ngoài

Các kết nối bên ngoài tạo khả năng truy cập trái phép thông tin doanh nghiệp, ví dụ truy cập bằng các phương pháp quay số. Như vậy, việc truy cập bởi những người sử dụng từ xa nên được thẩm định. Có nhiều loại phương pháp thẩm định khác nhau, một một số loại có mức bảo vệ lớn hơn các loại kia, ví dụ các phương pháp dựa trên việc sử dụng kỹ thuật mã hoá có thể có tính thẩm định mạnh hơn. Điều quan trọng là xác định từ một đánh giá rủi ro mức bảo vệ yêu cầu. Điều này là cần thiết để lựa chọn phương pháp thẩm định phù hợp.

Có thể sử dụng xác thực người sử dụng từ xa, ví dụ một mã hoá dựa trên phương pháp kỹ thuật, các mã thông báo phần cứng hoặc một giao thức thách thức/phản hồi. Các đường dây cá nhân chuyên dụng hoặc một địa chỉ của người sử dụng mạng kiểm tra khả năng cũng có thể được dùng để đảm bảo nguồn của các kết nối.

Các thủ tục và kiểm soát quay số lại, ví dụ sử dụng các modem quay số lại, có thể bảo vệ chống lại các kết nối trái phép và không mong muốn tới phương tiện xử lý thông tin của tổ chức. Loại kiểm soát này xác minh những người sử dụng đang cố gắng thiết lập kết nối tới một mạng của tổ chức từ các vị trí từ xa. Khi sử dụng kiểm soát này, một tổ chức không nên sử dụng các dịch vụ mạng bao gồm chuyển tiếp cuộc gọi, nếu có thì họ nên vô hiệu hoá việc sử dụng các đặc tính này để tránh những điểm yếu được kết hợp với việc chuyển tiếp cuộc gọi. Điều cũng quan trọng khác là quá trình gọi lại bao gồm việc đảm bảo rằng việc ngừng kết nối thực tế của tổ chức sẽ xuất hiện. Nói cách khác, người sử dụng từ xa có thể giữ đường dây mở giả bộ việc xác minh cuộc gọi lại đã xảy ra. Các thủ tục và kiểm soát gọi lại nên được kiểm tra kỹ lưỡng cho khả năng này.

9.4.4 Xác thực nút mạng

Một khả năng kết nối tự động tới một máy tính từ xa có thể tạo ra một cách tăng truy cập trái phép tới một ứng dụng của doanh nghiệp. Như vậy, các kết nối tới các hệ thống máy tính từ xa nên được xác minh. Điều này đặc biệt quan trọng nếu việc kết nối sử dụng một mạng nằm ngoài kiểm soát của ban quản lý an ninh của tổ chức. Một số ví dụ cho việc thẩm định và cách hiệu quả được đưa ra ở mục 9.4.3 ở trên.

Xác thực các nút có thể là phương tiện thay thế của việc xác thực các nhóm người sử dụng từ xa tại nơi được kết nối an toàn tới một phương tiện máy tính được chia sẻ, (xem 9.4.3).

9.4.5 Bảo vệ cổng chẩn đoán từ xa

Truy cập tới các cổng chẩn đoán nên được kiểm soát an toàn. Nhiều máy tính và các hệ thống truyền thông được lắp đặt với một phương tiện chuẩn đoán từ xa kết nối để các kỹ sư bảo dưỡng sử dụng. Nếu không được bảo vệ, các cổng chẩn đoán này sẽ tạo ra sự truy cập trái phép tiềm ẩn. Vì vậy, chúng nên được bảo vệ bằng một kỹ thuật an ninh phù hợp, ví dụ một khóa và một thủ tục để đảm bảo rằng chúng chỉ có thể bị truy cập được bằng sắp xếp giữa quản lý dịch vụ máy tính và phần cứng/ phần mềm hỗ trợ cá nhân yêu cầu truy cập.

9.4.6 Tình trạng phân tách trong các mạng

Các mạng đang ngày càng mở rộng vượt qua biên giới tổ chức truyền thống, vì các mối quan hệ kinh doanh được hình thành đòi hỏi sự kết nối lẫn nhau hoặc chia sẻ các phương tiện xử lý thông tin và nối mạng. Việc mở rộng này có thể làm tăng rủi ro truy cập trái phép đối với các hệ thống thông tin đã và đang tồn tại sử dụng mạng, một số hệ thống yêu cầu bảo vệ khỏi người sử dụng mạng khác vì tính nhạy cảm hoặc tính phê bình của chúng. Trong các trường hợp này, việc hướng dẫn các kiểm soát trong mạng, để cách ly các nhóm dịch vụ thông tin, nên xem xét người sử dụng và các hệ thống thông tin.

Một biện pháp kiểm soát tính an toàn của các mạng lớn là chia chúng thành các miền mạng logic riêng biệt, ví dụ các miền mạng nội bộ và các miền mạng bên ngoài của một tổ chức, mỗi cái được bảo vệ bởi một vành đai an ninh xác định. Vành đai này có thể được thực hiện bằng việc lắp đặt một cổng ra vào an ninh giữa hai mạng này để được kết nối lẫn nhau để kiểm soát truy cập và luồng thông tin giữa 2 miền. Cổng này nên được định hình thành một bộ lọc giữa các miền này (xem 9.4.7 và 9.4.8) và để chặn truy cập trái phép liên quan đến chính sách kiểm soát truy cập của tổ chức (xem 9.1). Ví dụ cho loại cổng này thường được nói đến như một bức tường lửa.

Tiêu chuẩn để chia tách các mạng thành các miền nên dựa trên chính sách kiểm soát truy cập, các yêu cầu truy cập (xem 9.1) và cũng phải tính đến chi phí tương đối và ảnh hưởng biểu hiện của việc kết hợp công nghệ cổng ra vào và lộ trình mạng phù hợp (xem 9.4.7 và 9.4.8).

9.4.7 Kiểm soát kết nối của mạng

Các yêu cầu chính sách kiểm soát truy cập đối với các mạng chia sẻ, đặc biệt những mạng mở rộng qua ranh giới tổ chức, đòi hỏi sự kết hợp các kiểm soát để hạn chế khả năng kết nối của người sử dụng. các kiểm soát này có thể được thực hiện qua cá cổng ra vào mạng có bộ lọc là các bảng hoặc quy tắc được xác định trước. Các hạn chế được áp dụng nên dựa trên chính sách truy cập và các yêu cầu của các ứng dụng của doanh nghiệp (xem 9.1) và nên được duy trì và cập nhật.

Các ví dụ cho các ứng dụng mà các hạn chế nên được áp dụng:

a) thư điện tử;

b) truyền tệp một chiều;

c) truyền tệp hai chiều;

d) truy cập tương tác;

e) truy cập mạng được liên kết với thời gian theo ngày và tháng.

9.4.8 Kiểm soát định tuyến mạng

Các mạng chia sẻ, đặc biệt các mạng mở rộng qua biên giới tổ chức, yêu cầu sự kết kợp các kiểm soát lộ trình để đảm bảo rằng các kết nối máy tính và các luồng thông tin không vi phạm chính sách kiểm soát truy cập của các ứng dụng của doanh nghiệp (xem 9.1). Kiểm soát này thường cần thiết cho các mạng được chia sẻ với người sử dụng là bên thứ ba (không trong tổ chức).

Các lộ trình nên được dựa trên nguồn tích cực và các kỹ thuật kiểm tra địa chỉ đích. Chuyển dịch địa chỉ mạng cũng là một kỹ thuật rất hữu ích để phân tách các mạng và ngăn ngừa các lộ trình phổ biến từ mạng của một tổ chức tới các mạng khác. Chúng có thể được tiến hành trong phần mềm hoặc phần cứng. Những người thực hiện nên nhận thức về khả năng của tất cả kỹ thuật triển khai.

9.4.9 An ninh của các dịch vụ mạng

Có một dãy rộng các dịch vụ mạng công cộng và tư nhân, một số cung cấp dịch vụ giá trị gia tăng. Các dịch vụ mạng có thể có các đặc tính an ninh đơn nhất hoặc phức tạp. Các tổ chức sử dụng các dịch vụ mạng nên đảm bảo rằng cung cấp một bản trình bày rõ các thuộc tính an ninh của toàn bộ các dịch vụ được sử dụng.

9.5 Kiểm soát định truy cập hệ điều hành

Đối tượng: Để ngăn ngừa truy cập máy tính trái phép.

Các phương tiện an ninh ở mức hệ thống hoạt động nên được sử dụng để hạn chế truy cập tới các tài nguyên máy tính. Các phương tiện này nên có đủ khả năng sau:

a) định danh và xác minh định danh và nếu cần cả cổng hoặc nơi mỗi người sử dụng được cấp phép;

b) ghi lại các truy cập hệ thống thành công và thất bại;

c) đưa ra các biện pháp thích hợp cho việc xác minh; nếu một hệ thống quản lý mật khẩu được sử dụng thì nó nên đảm bảo cá mật khẩu có chất lượng [xem 9.3.1 d];

d) khi thích hợp, hạn chế số lần kết nối của người sử dụng.

Các phương pháp kiểm soát truy cập khác, như thách thức-phản hồi, sẵn sàng nếu các phương tiện này có lý do cho rằng có rủi ro kinh doanh.

9.5.1 Định danh tự động thiết bị đầu cuối

Định danh cổng tự động nên được xem xét để xác minh các kết nối tới các khu vực riêng biệt và các thiết bị có thể di chuyển. Định danh cổng tự động là một công nghệ có thể được sử dụng nếu phiên làm việc chỉ có thể khởi đầu từ một vị trí hoặc cổng máy tính cụ thể là điều quan trọng. Một định danh bên trong hoặc gắn với cổng đó có thể được sử dụng để chỉ ra liệu cổng cụ thể này có được phép khởi đầu hoặc nhận các giao địch riêng biệt. có thể cần phải áp dụng bảo vệ vật lý với cổng này để duy trì an ninh của từ định danh của cổng. Một số công nghệ khác cũng có thể được sử dụng để xác minh người sử dụng (xem 9.4.3).

9.5.2 Các thủ tục nhập vào thiết bị đầu cuối

Truy cập tới các dịch vụ thông tin nên khả thi thông qua một quá trình đăng nhập an toàn thủ tục cho việc vào hệ thống máy tính nên được thiết kế để giảm thiểu tối đa cơ hội truy cập trái phép. Như vậy thủ tục đăng nhập nên đưa ra tối thiểu các thông tin về hệ thống để tránh có một người sử dụng trái phép với hỗ trợ không cần thiết. Thủ tục đăng nhập nên:

a) không trình bày các từ định danh hệ thống hoặc ứng dụng cho đến khi quá trình đăng nhập hoàn tất;

b) đưa ra một cảnh báo chung rằng máy tính chỉ nên truy cập bởi những người sử dụng được phép;

c) không cung cấp các thông điệp gíp đỡ trong khi thủ tục đăng nhập chưa xong vì nó có thể giúp một người sử dụng trái phép;

d) xác định giá trị thông tin đăng nhập chỉ khi hoàn tất toàn bộ dữ liệu đầu vào. Nếu có trường hợp lỗi phát sinh, hệ thống không nên chỉ ra phần dữ liệu nào đúng hoặc không đúng;

e) hạn chế số lần thử đăng nhập không thành công cho phép (nên là 3) và xem xét:

1) ghi lại các lần thử không thành công;

2) áp buộc một thời hạn hoãn trước khi các lần thử đăng nhập tiếp được phép hoặc từ chối mọi lần thử tiếp nếu không được cấp phép cụ thể;

3) không kết nối các kết nối dữ liệu liên quan;

f) giới hạn thời gian tối đa và tối thiểu được phép cho thủ tục đăng nhập. Nếu quá hệ thống sẽ huỷ bỏ đăng nhập;

g) đưa ra các thông tin sau để hoàn thành một đăng nhập thành công:

1) ngày và thời gian lần đăng nhập thành công trước;

2) chi tiết của các lần thử đăng nhập không thành công tính từ lần đăng nhập thành công gần nhất.

9.5.3 Định danh và xác thực người sử dụng

Toàn bộ người sử dụng (bao gồm nhân viên hỗ trợ kỹ thuật, như những người vận hành, quản trị, lập chương trình hệ thống, quản trị cơ sở dữ liệu) nên có một định danh duy nhất (ID cho người sử dụng) cho việc sử dụng cá nhân và độc quyền để các hoạt động có thể sau đó tìm ra cá nhân chịu trách nhiệm. các ID của người sử dụng không nên có bất kỳ sự ám chỉ nào về mức đặc quyền của người sử dụng (xem 9.2.2), ví dụ nhà quản lý, nguười giám sát.

Trong các trường hợp ngoại lệ, nơi có một lợi ích kinh doanh rõ ràng, có thể sử dụng một ID chung cho một nhóm người sử dụng hoặc một công việc đặc biệt. Việc chấp thuận của ban quản lý nên được ghi chép lại đối với các trường hợp như vậy. Các kinh doanh thêm nên được yêu cầu để duy trì trách nhiệm giải trình.

Có nhiều thủ tục xác minh có thể được sử dụng để chứng minh định danh của người sử dụng. Các mật khẩu (xem 9.3.1 và bên dưới) là cách thông thường để cung cấp định danh và xác minh (I &A) dựa trên cơ sở bí mật chỉ người sử dụng biết. Tương tự cũng có thể đạt hiệu quả với các biện pháp mã hoá và các giao thức xác minh.

Các thẻ nhớ và thẻ thông minh mà người sử dụng có cũng có thể được sử dụng cho I &A. Công nghệ xác minh sinh học sử dụng các đặc điểm hoặc thuộc tính độc nhất của một cá nhân cũng có thể được sử dụng để xác minh định danh của người đó. Sự kết hợp giữa công nghệ và kỹ thuật một cách an toàn sẽ tạo ra cách xác minh tốt hơn.

9.5.4 Hệ thống quản lý mật khẩu

Các mật khẩu là một biện pháp nguyên tắc của việc xác định giá trị của quyền truy cập vào dịch vụ máy tinh của người sử dụng. Các hệ thống quản lý mật khẩu nên cung cấp một phương tiện hiệu quả, tương tác, đảm bảo các mật khẩu có chất lượng (xem 9.3.1 hướng dẫn về việc sử dụng các mật khẩu).

Một số ứng dụng yêu cầu các mật khẩu của người sử dụng phải được ấn định bằng một quyền độc lập. Trong hầu hết các trường hợp, các mật khẩu được lựa chọn và duy trì bởi người sử dụng.

Một hệ thống quản lý mật khẩu tốt nên:

a) bắt buộc việc sử dụng các mật khẩu cá nhân để duy trì trách nhiệm giải trình;

b) khi thích hợp, cho phép người sử dụng lựa chọn và thay đổi các mật khẩu riêng của họ và có một thủ tục khẳng định lại cho các lỗi đầu vào;

c) bắt buộc lựa chọn các mật khẩu có chất lượng như đã nói ở mục 9.3.1;

d) ở nơi người sử dụng duy trì mật khẩu riêng của họ, bắt buộc những thay đổi mật khẩu phải như đã nói ở mục 9.3.1;

e) ở nơi người sử dụng lựa chọn các mật khẩu, buộc họ phải thay đổi cá mật khẩu tạm thời vào lần đăng nhập đầu tiên (xem 9.2.3);

f) duy trì một bản ghi các mật khẩu của người sử dụng trước đây, ví dụ trong vòng 12 tháng trước và ngăn không cho sử dụng lại;

g) không hiện mật khẩu trên màn hình khi được nhập vào;

h) lưu giữ các tệp mật khẩu tách biệt khỏi dữ liệu hệ thống ứng dụng;

i) lưu giữ các mật khẩu ở dạng mã hoá sử dụng một thuật toán mã hoá một chiều;

j) thay đổi các mật khẩu mặc định của đại lý theo việc cài đặt phần mềm.

9.5.5 Sử dụng các tiện ích của hệ thống

Hầu hết các cài đặt máy tính có một hoặc nhiều chương trình hệ thống tiện ích có khả năng vượt qua các kiểm soát của hệ thống và ứng dụng. Điều cốt yếu là việc sử dụng chúng bị hạn chế và kiểm soát chặt chẽ. Nên xem xét các kiểm soát sau đây:

a) sử dụng các thủ tục xác minh đối với các tiện ích hệ thống;

b) phân đoạn các tiện ích hệ thống từ các ứng dụng phần mềm;

c) giới hạn việc sử dụng các tiện ích hệ thống để tối thiểu số thực tế người sử dụng được phép, đáng tin;

d) cấp phép cho việc sử dụng đặc biệt các tiện ích hệ thống;

e) giới hạn sự xuất hiện các tiện ích hệ thống, ví dụ trong khoảng thời gian một sự thay đổi được phép;

f) ghi nhật ký toàn bộ việc sử dụng các tiện ích hệ thống;

g) xác định và ghi lại các mức cho phép đối với các tiện ích hệ thống;

h) loại bỏ toàn bộ các phần mềm không cần thiết trên cơ sở các tiện ích và phần mềm hệ thống.

9.5.6 Cảnh báo bắt buộc để bảo vệ người sử dụng

Việc cung cấp một báo động bắt buộc nên được xem xét đối với người sử dụng có thể là mục tiêu của sự áp buộc. Quyết định liệu có cung ứng một báo động như vậy không nên dựa trên cơ sở đánh giá rủi ro. Nên có các trách nhiệm và thủ tục xác định để phản ứng với một báo động bắt buộc.

9.5.7 Thời gian chờ của thiết bị đầu cuối

Các cổng không hoạt động ở các vị trí rủi ro cao, ví dụ khu vực công cộng hoặc bên ngoài quản lý an ninh của hệ thống hoặc phục vụ các hệ thống rủi ro cao nên được đóng lại sau một thời gian không hoạt động được xác định để ngăn ngừa việc truy cập của người sử dụng trái phép. Thời hạn ngừng này nên xoá màn hình và đóng cả các vùng ứng dụng và vùng mạng sau một thời gian không hoạt động được xác định việc trì hoãn thời gian ngừng này nên phản ánh các rủi ro an ninh của khu vực và người sử dụng cổng đó.

Một dạng giới hạn của biện pháp thời hạn ngừng của cổng có thể được cung cấp cho một số máy tính cá nhân để xoá màn hình và ngăn ngừa truy cập trái phép nhưng không đóng các vùng ứng dụng hoặc vùng mạng.

9.5.8 Giới hạn của thời gian kết nối

Các hạn chế về số lần kết nối nên cung cấp an ninh thêm cho các ứng dụng rủi ro cao. Giới hạn thời gian các kết nối cổng được phép tới các dịch vụ máy tính lamg giảm cơ hội truy cập trái phép. Một kiểm soát như vậy nên được xem xét đối với các ứng dụng máy tính nhạy cảm, đặc biệt với những cổng cài đặt trong khu vực rủi ro cao, ví dụ khu vực công cộng hoặc bên ngoài quản lý an ninh của tổ chức. Các ví dụ cho việc hạn chế này bao gồm:

a) sử dụng các khe thời gian xác định trước, ví dụ đối với các chuyển giao một loạt tệp hoặc các vùng tương tác thông thường trong thời gian ngắn;

b) hạn chế số lần kết nối trong giờ làm việc bình thường nếu không có yêu cầu cho việc hoạt động quá giờ hoặc thêm giờ.

9.6 Kiểm soát truy cập của ứng dụng

Đối tượng: Ngăn chặn truy cập trái phép tới các thông tin trong các hệ thống thông tin.

Các phương tiện an ninh nên được sử dụng để ngăn chặn truy cập trong các hệ thống ứng dụng. Các truy cập logic tới các phần mềm và thông tin nên được hạn chế trong người sử dụng được phép các hệ thống ứng dụng nên:

a) kiểm soát truy cập của người sử dụng vào các chức năng hệ thống thông tin và ứng dụng, liên quan tới một chính sách kiểm soát truy cập kinh doanh được xác định;

b) cung cấp biện pháp bảo vệ khỏi truy cập trái phép bất kỳ tiện ích và phần mềm hệ thống hoạt động nào mà có thể vượt qua các kiểm soát hệ thống hoặc ứng dụng;

c) không làm tổn hại đến an ninh của các hệ thống khác với các nguồn thông tin được chia sẻ;

d) có thể chỉ truy cập thông tin đối với chủ sở hữu, các cá nhân được phép chính thức khác hoặc nhóm người sử dụng xác định.

9.6.1 Hạn chế truy cập thông tin

Người sử dụng các hệ thống ứng dụng, bao gồm nhân viên hỗ trợ nên được cho truy cập tới các chức năng thông tin và hệ thống ứng dụng liên quan tới một chính sách kiểm soát truy cập xác định, dựa trên cơ sở các yêu cầu ứng dụng kinh doanh cá nhân và thống nhất với chính sách truy cập thông tin của tổ chức (xem 9.1). Áp dụng nên xem xét các kiểm soát sau đây để hỗ trợ các yêu cầu hạn chế truy cập:

a) đưa ra các bảng chọn để kiểm soát truy cập tới các chức năng hệ thống ứng dụng;

b) hạn chế kiến thức của người sử dụng về các chức năng thông tin hoặc hệ thống ứng dụng trái phép truy cập với việc biên tập thích hợp tư liệu về người sử dụng;

c) kiểm soát quyền truy cập của người sử dụng, ví dụ đọc, viết, xoá và thi hành;

d) đảm bảo rằng các dữ liệu ra từ các hệ thống ứng dụng xử lý thông tin nhạy cảm chỉ bao gồm thông tin liên quan tới việc sử dụng đầu ra đó và chỉ được gửi tới các cổng và vị trí cho phép, bao gồm soát xét định kỳ các đầu ra này để đảm bảo rằng thông tin thừa bị loại đi.

9.6.2 Cách ly hệ thống nhạy cảm

Các hệ thống nhạy cảm có thể yêu cầu một môi trường máy tính chuyên dụng (phân biệt). Một số hệ thống ứng dụng nhạy cảm một cách thích đáng với sự mất mát tiềm ẩn mà chúng yêu cầu việc quản lý đặc biệt. Tính nhạy cảm có thể chỉ ra rằng hệ thống ứng dụng nên chạy trong một máy tính chuyên dụng, chỉ nên chia sẻ các nguồn với các hệ thống ứng dụng đáng tin hoặc không có giới hạn. Các xem xét sau được áp dụng:

a) tính nhạy cảm của hệ thống ứng dụng nên được định danh và ghi chép rõ ràng bởi người sở hữu ứng dụng (xem 4.1.3);

b) khi một ứng dụng nhạy cảm chạy trong một môi trường chung, các hệ thống ứng dụng với những nguồn mà nó sẽ chia sẻ nên được định danh và chấp nhận với người sở hữu ứng dụng nhạy cảm.

9.7 Kiểm tra sự truy cập và sử dụng hệ thống

Đối tượng: Để phát hiện các hoạt động trái phép.

Các hệ thống nên được giám sát để phát hiện sự chệch hướng khỏi chính sách kiểm soát truy cập và lưu giữ các sự kiện có thể kiểm soát được để cung cấp bằng chứng trong trường hợp có sự cố an ninh. Giám sát hệ thống cho phép tính hiệu quả của kiểm soát được chấp nhận để được kiểm tra và phù hợp với một mẫu chính sách truy cập (xem 9.1) được xác minh.

9.7.1 Ghi lại sự kiện

Các ghi chép kiểm toán ghi lại các ngoại lệ và các sự kiện liên quan đến an ninh khác nên được thực hiện và giữ trong một thời gian được đồng ý để giúp cho các điều tra trong tương lai và giám sát kiểm soát truy cập. Các ghi chép kiểm toán cũng nên gồm:

a) ID (định danh) của người sử dụng;

b) ngày và giờ đăng nhập và thoát khỏi;

c) cổng định danh hoặc vị trí nếu có thể;

d) các bản lưu các lần thử truy cập hệ thống thành công và bị từ chối;

e) các bản lưu các lần thử truy cập dữ liệu và các nguồn khác thành công và bị từ chối.

Các ghi chép kiểm toán chắc chắn có thể yêu cầu được lưu trữ như một phần của chính sách sở hữu bản ghi hoặc vì các yêu cầu thu thập bằng chứng (xem mục 12).

9.7.2 Kiểm tra việc sử dụng hệ thống

9.7.2.1 Các thủ tục và phạm vi rủi ro

Các thủ tục đối với việc kiểm soát sử dụng các phương tiện xử lý thông tin nên được thiết lập. Những thủ tục như vậy là cần thiết để người sử dụng chỉ tiến hành các hoạt động được phép một cách rõ ràng. Mức độ kiểm soát yêu cầu đối với các phương tiện cá nhân nên được xác lập qua đánh giá rủi ro. Các khu vực nên được xem xét bao gồm:

a) truy cập được phép bao gồm chi tiết như:

1) ID của người sử dụng;

2) ngày và giờ của các sự kiện chính;

3) kiểu sự kiện;

4) các tệp được truy cập;

5) các chương trình/tiện ích được sử dụng;

b) toàn bộ các hoạt động được đặc quyền như:

1) sử dụng tài khoản người giám sát;

2) bật và ngừng hệ thống;

3) gắn/gỡ thiết bị I/O;

c) các lần thử truy cập trái phép, như:

1) các lần thử thất bại;

2) các vi phạm chính sách truy cập và khai báo với các cổng ra vào và tường lửa của mạng;

3) báo động từ các hệ thống phát hiện sự xâm nhập có đang ký độc quyền;

d) báo động và lỗi hệ thống như:

1) báo động bằng máy hoặc các thông điệp;

2) các ngoại lệ ghi chép hệ thống;

3) các báo động quản lý mạng.

9.7.2.2 Các nhân tố rủi ro

Kết quả của các hoạt động giám sát nên được soát xét thường xuyên. Tần số soát xét nên phụ thuộc vào các rủi ro. Các yếu tố rủi ro nên được xem xét bao gồm:

a) tính phê bình của cá quá trình ứng dụng;

b) giá trị, tính nhạy cảm hoặc tính phê bình của các thông tin bao gồm;

c) kinh nghiệm quá khứ của việc truy cập và lạm dụng hệ thống;

d) mở rộng kết nối hệ thống (đặc biệt các mạng công cộng).

9.7.2.3 Ghi lại và xem xét các sự kiện

Một soát xét ghi chép bao gồm việc hiểu biết các mối đe doạ có thể nảy sinh mà hệ thống và cách thực phải đối mặt. Các ví dụ cho các sự kiện có thể yêu cầu điều tra thêm trong trường hợp sự cố an ninh được đưa ra trong ở 9.7.1.

Các ghi chép nhật ký hệ thống thường bao gồm một lượng lớn thông tin, nhiều thông tin không liên quan tới kiểm soát an ninh. Để giúp định danh các sự kiện quan trọng cho mục đích kiểm soát an ninh nên xem xét việc sao chép tự động các loại thông điệp thích hợp thành một bản ghi thứ hai và/hoặc sử dụng các tiện ích hệ thống phù hợp hoặc các dụng cụ kiểm toán để thực hiện dò tệp.

Khi phân phối trách nhiệm soát xét ghi chép nên xem xét việc chia tách vai trò giữa những người thực hiện soát xét và những người có hoạt động đang bị giám sát.

Chú ý đặc biệt đến an ninh của phương tiện ghi chép nhật ký vì nếu bị xáo trộn nó có thể đưa ra một phán đoán an ninh sai lầm. Các kiểm soát nên nhắm tới việc bảo vệ chống lại các thay đổi trái phép và cá vấn đề hoạt động bao gồm:

a) phương tiện ghi chép nhật ký bị mất tác dụng;

b) các thay đổi đối với các kiểu thông điệp được lưu giữ;

c) các tệp ghi chép nhật ký bị sửa hoặc xoá;

d) phương tiện truyền thông tệp ghi chép trở nên quá tải và không thể lưu các sự kiện hoặc viết đè.

9.7.3 Đồng bộ hóa đồng hồ

Việc đặt các đồng hồ máy tính đúng là quan trọng để đảm bảo độ chính xác của các dấu vết kiểm tra mà có thể được yêu cầu cho các cuộc điều tra hoặc là chứng cứ trong các trường hợp kiện tụng hoặc vi phạm kỷ luật. Các dấu vết kiểm tra không chính xác có thể cản trở các cuộc điều tra này và làm hại đến sự tin cậy của các chứng cứ này.

Khi một thiết bị máy tính hoặc truyền tin có khả năng vận hành một đồng hồ đúng giờ, nó nên được đặt theo một chuẩn chung, ví dụ giờ hợp tác toàn cầu (UCT) hoặc giờ chuẩn địa phương. Vì một số đồng hồ là thụ động với thời gian nên có một thủ tục kiểm tra và chỉnh sửa mọi mức biến động quan trọng.

9.8 Công tác từ xa và tính toán lưu động

Đối tượng: Để đảm bảo an ninh thông tin khi sử dụng các phương tiện máy tính di động và các phương tiện công tác từ xa.

Sự bảo vệ được yêu cầu nên tương xứng với các rủi ro của cách làm việc riêng biệt này. Khi sử dụng máy tính di động nên xem xét các rủi ro của công việc trong một môi trường không được bảo vệ và áp dụng biện pháp bảo vệ thích hợp. Trong trường hợp làm việc từ xa, tổ chức nên áp dụng bảo vệ vị trí làm việc từ xa này và đảm bảo rằng việc sắp xếp phù hợp được tiến hành cho kiểu làm điều này.

9.8.1 Tính toán lưu động

Khi sử dụng các phương tiện máy tính di động, ví dụ sổ tay, máy tính xách tay và điện thoại di động nên đặc biệt cẩn thận để đảm bảo rằng thông tin của doanh nghiệp không bị tổn hại. Một chính sách chính thức nên được thông qua và tính tới các rủi ro của công việc với các phương tiện máy tính di động, đặc biệt trong các môi trường không được bảo vệ. Ví dụ một chính sách như vậy nên bao gồm các yêu cầu về bảo vệ vật lý, các kiểm soát truy cập, kỹ thuật mã hoá, sao lưu, chống virút. Chính sách này cũng nên bao gồm các quy định và lời khuyên về các phương tiện di động đang kết nối với các mạng và hướng dẫn việc sử dụng các phương tiện này ở nơi công cộng.

Nên cẩn thận khi sử dụng các phương tiện máy tinh di dộng ở nơi công cộng, các phòng họp và các khu vực không được bảo vệ khác nằm ngoài vành đai của tổ chức. Việc bảo vệ nên tiến hành để tránh truy cập trái phép hoặc làm lộ thông tin được lưu trữ và lập trình bởi các phương tiện này, ví dụ sử dụng kỹ thuật mã hoá (xem 10.3).

Điều quan trọng là khi sử dụng các phương tiện này ở nơi công cộng nên cẩn thận tránh các rủi ro về nhìn trộm bởi những người trái phép. Các thủ tục chống lại phần mềm gây hại nên được tiến hành và cập nhật (xem 8.3). Thiết bị nên sẵn sàng để cho phép sao chép dự phòng thông tin nhanh và dễ dàng. Các bản sao lưu này nên có sự bảo vệ thích hợp chống lại ví dụ bị ăn cắp hoặc mất mát thông tin.

Bảo vệ phù hợp nên được thực hiện đối với việc sử dụng các phương tiện di động kết nối với các mạng. Truy cập từ xa vào thông tin của doanh nghiệp qua mạng công cộng sử dụng các phương tiện máy tính di động chỉ nên thực hiện sau khi định danh và xác minh thành công và với các kỹ thuật kiểm soát truy cập phù hợp (xem 9.4).

Các phương tiện máy tính di động cũng nên được bảo vệ về mặt vật lý chống lại việc bị ăn cắp đặc biệt khi được bỏ lại trên ôtô và các phương tiện di chuyển khác, phòng khách sạn, trung tâm hội nghị và các nơi gặp gỡ. Các thiết bị mang các thông tin kinh doanh quan trọng, nhạy cảm và/ hoặc có tính phê bình không nên được chú ý và nếu có thể nên được khoá về mặt vật lý hoặc khoá đặc biệt để an toàn cho cá thiết bị. Thông tin thêm về biện pháp bảo vệ vật lý các thiết bị di động có thể xem ở 7.2.5.

Đào tạo nên được sắp xếp cho các nhân viên sử dụng máy tính di động để nâng cao nhận thức của họ về các rủi ro thêm do cách làm điều này và nên thực hiện các kiểm soát.

9.8.2 Công tác từ xa

Làm việc từ xa sử dụng công nghệ truyền tin cho phép cá nhân viên có thể làm việc từ một vị trí bên ngoài tổ chức. Biện pháp bảo vệ phù hợp cho vị trí làm việc từ xa nên được thực thi để chống lại ví dụ ăn cắp thiết bị và thông tin, tiết lộ thông tin trái phép, truy cập từ xa trái phép tới các hệ thống nội bộ của tổ chức hoặc lạm dụng các phương tiện. Quan trọng là làm việc từ xa phải được phép và kiểm soát bởi ban quản lý và thực hiện các sắp xếp phù hợp cho cách làm điều này.

Các tổ chức nên xem xét việc phát triển một chính sách, các thủ tục và tiêu chuẩn kiểm soát các hoạt động của làm việc từ xa. Các tổ chức chỉ nên cho phép các hoạt động làm việc từ xa nếu chúng thoả mãn các sắp

xếp an ninh thích hợp và các kiểm soát được thực hiện và phù hợp với chính sách an ninh của tổ chức. Nên xem xét những điều sau:

a) duy trì an ninh về mặt vật lý vị trí làm việc từ xa, có tính đến an ninh vật lý của toà nhà và môi trường vùng;

b) môi trường làm việc từ xa được đề xuất;

c) các yêu cầu an ninh truyền tin tính tới nhu cầu truy cập từ xa tới các hệ thống nội bộ của tổ chức, tính nhạy cảm của thông tin sẽ bị truy cập và vượt qua liên kết truyền thông và tính nhạy cảm của hệ thống nội bộ;

d) mối đe dọa của truy cập trái phép tới thông tin hoặc các nguồn từ những người khác đang ở cùng, ví dụ gia đình và bạn bè.

Các kiểm soát và sắp xếp nên được xem xét gồm:

a) cung cấp các thiết bị phù hợp và đồ dùng lưu trữ cho các hoạt động làm việc từ xa;

b) xác định công việc được phép, thời gian làm việc, phân loại thông tin được lưu giữ và các hệ thống và dịch vụ nội bộ mà người làm việc từ xa được phép truy cập;

c) cung cấp các thiết bị truyền tin phù hợp, bao gồm cả các phương pháp đảm bảo an toàn truy cập từ xa;

d) an ninh vật lý;

e) các quy tắc và hướng dẫn về việc xâm phạm của gia đình và khách tới thiết bị và thông tin;

f) cung cấp việc hỗ trợ và bảo dưỡng phần mềm và phần cứng;

g) các thủ tục sao chép dự phòng và liên tục trong kinh doanh;

h) giám sát kiểm toán và an ninh;

i) huỷ bỏ quyền, quyền truy cập và lấy lại cá thiết bị khi ngừng các hoạt động làm việc từ xa.

10 Phát triển và duy trì hệ thống

10.1 Các yêu cầu an ninh của hệ thống

Đối tượng: Đảm bảo rằng an ninh được thiết lập trong các hệ thống thông tin.

Điều này bao gồm cơ sở hạ tầng, các ứng dụng của doanh nghiệp và các ứng dụng được người sử dụng phát triển. Thiết kế và thực hiện quá trình kinh doanh hỗ trợ ứng dụng hoặc dịch vụ có thể là cốt yếu cho an ninh. Các yêu cầu an ninh nên được định danh và chấp thuận trước cho việc phát triển các hệ thống thông tin.

Toàn bộ các yêu cầu an ninh, bao gồm nhu cầu về chuẩn bị dự trữ nên được định danh tại các giai đoạn được yêu cầu của một dự án và được chứng minh, chấp thuận và ghi chép như một phần của trường hợp kinh doanh toàn diện đối với một hệ thống thông tin.

10.1.1 Phân tích và đặc tả các yêu cầu an ninh

Các bản trình bày các yêu cầu kinh doanh cho các hệ thống mới hoặc nâng cao các hệ thống đang có nên chỉ rõ các yêu cầu kiểm soát. Sự chỉ rõ này nên xem xét các kiểm soát tự động được kết hợp trong hệ thống và nhu cầu hỗ trợ các kiểm soát thủ công. Những xem xét tương tự nên được áp dụng khi đánh giá các gói phần

mềm cho các ứng dụng kinh doanh. Nếu thấy thích hợp, ban quản lý có thể hy vọng sử dụng các sản phẩm được đánh giá và chứng nhận độc lập.

Các yêu cầu và kiểm soát an ninh nên phản ánh giá trị các tài sản thông tin của doanh nghiệp và tổn thất kinh doanh tiềm ẩn có thể do lỗi hoặc thiếu an ninh. Khung sườn của việc phân tích các yêu cầu an ninh và định danh các kiểm soát để thực hiện chúng là đánh giá rủi ro và quản lý rủi ro.

Các kiểm soát được đưa vào ở bộ phận thiết kế rẻ hơn đáng kể cho việc thực hiện và duy trì so với các kiểm soát trong và khi thực hiện.

10.2 An ninh trong các hệ thống ứng dụng

Đối tượng: Để ngăn ngừa mất mát, thay đổi hoặc lạm dụng dữ liệu người sử dụng trong các hệ thống ứng dụng. Các kiểm soát thích hợp và các dấu vết kiểm tra hoặc các nhật ký hoạt động nên được thiết kết trong các hệ thống ứng dụng, bao gồm các ứng dụng do người sử dụng viết. Điều này nên gồm cả kiểm tra tính hợp lệ của dữ liệu đầu vào, quá trình xử lý và dữ liệu đầu ra.

Các kiểm soát thêm có thể được yêu cầu cho các hệ thống mà có ảnh hưởng đến các tài sản nhạy cảm, giá trị hoặc có tính phê bình. Các kiểm soát này nên được xác định trên cơ sở các yêu cầu an ninh và đánh giá rủi ro.

10.2.1 Xác định tính hợp lệ của dữ liệu đầu vào

Dữ liệu đầu vào cho các hệ thống ú nên được kiểm tra tính hợp lệ để đảm bảo rằng chính xác và thích hợp. các kiểm tra nên được áp dụng đối với đầu vào của cá giao dịch kinh doanh, trên dữ liệu (tên và địa chỉ, hạn mức tín dụng, số liên hệ khách hàng) và bảng tham số (giá bán, tỷ lệ đối thoại hiện tại, tỷ lệ thuế). Nên xem xét các kiểm soát sau đây:

a) kiểm tra hai đầu vào và đầu vào khác để phát hiện các lỗi sau:

1) các giá trị ngoài vùng;

2) các đặc tính không giá trị trong các miền dữ liệu;

3) dữ liệu thiếu hoặc không đầy đủ;

4) vượt quá giới hạn độ lớn dữ liệu cao nhất và thấp nhất;

5) dữ liệu kiểm soát trái phép hoặc không thống nhất;

b) soát xét định kỳ nội dung các miền hoặc tệp dữ liệu quan trọng để khẳng định giá trị và tính toàn vẹn của chúng;

c) thanh tra các tài liệu đầu vào khó sao chép đối với mọi thay đổi trái phép về dữ liệu đầu vào (toàn bộ thay đổi tài liệu đầu phải được phép);

d) các thủ tục đáp ứng với các lỗi giá trị;

e) các thủ tục kiểm tra tính hợp lý của dữ liệu đầu vào;

f) xác định trách nhiệm của toàn bộ những cá nhân liên quan trong quá trình dữ liệu đầu vào.

10.2.2 Kiểm soát quá trình nội bộ

10.2.2.1 Các phạm vi rủi ro

Dữ liệu được nhập vào đúng có thể bị sai lệch do các lỗi xử lý hoặc qua các hoạt động có chủ ý. Kiểm tra tính hợp lệ nên được kết hợp vào các hệ thống để phát hiện những sai lạc này. Thiết kế các ứng dụng nên đảm bảo rằng các biện pháp hạn chế được thực hiện để giảm tối đa rủi ro các lỗi xử lý dẫn đến mất mát, không toàn vẹn. Các khu vực riêng biệt được xem xét bao gồm:

a) việc sử dụng và vị trí trong các chương trình của các chức năng thâm và xoá để thực hiện các thay đổi dữ liệu;

b) các thủ tục ngăn ngừa các chương trình đang chạy theo thứ tự sai hoặc chạy sau khi có lỗi xử lý trước (xem 8.1.1);

c) việc sử dụng các chương trình đúng để khôi phục các lỗi để đảm bảo quá trình xử lý dữ liệu đúng.

10.2.2.2 Kiểm tra và kiểm soát

Các kiểm soát được yêu cầu sẽ phụ thuộc vào tính chất của ứng dụng và ảnh hưởng kinh doanh của mọi sự sai lệch dữ liệu. Các ví dụ cho các kiểm tra có thể được kết hợp gồm:

a) các kiểm soát phiên hoặc đợt, để điều hoà cân bằng tệp dữ liệu sau các cập nhật giao dịch;

b) cân bằng các kiểm soát để kiểm tra các cân bằng mở chống lại các cân bằng đóng trước đó, gồm:

1) các kiểm soát hoạt động với hoạt động;

2) tổng số cập nhật tệp;

3) các kiểm soát chương trình với chương trình;

c) kiểm tra tính hợp lệ của dữ liệu hệ thống được phát (xem 10.2.1);

d) các kiểm tra tính toàn vẹn của dữ liệu hoặc phần mềm được tải xuống hoặc tải lên, giữa trung tâm và các máy tính từ xa (xem 10.3.3);

e) tổng số các bản ghi và flie;

f) các kiểm tra để đảm bảo rằng các chương trình ứng dụng được chạy đúng thời gian;

g) các kiểm tra để đảm bảo rằng các chương trình được chạy đúng thứ tự và huỷ bỏ trong trường hợp có lỗi và quá trình xử lý thêm bị ngừng cho đến khi vấn đề được giải quyết.

10.2.3 Xác thực thông điệp

Xác thực thông điệp là một kỹ thuật sử dụng để phát hiện cá thay đổi trái phép hoặc sai lạc nội dung của một thông điệp điện tử được truyền. Việc xác thực thông điệp có thể được thực hiện trên phần cứng hoặc phần mềm hỗ trợ một phần xác thực thông điệp vật lý hoặc một thuật toán phần mềm.

Xác thực thông điệp nên được xem xét đối với các ứng dụng có yêu cầu an ninh để bảo vệ tính toàn vẹn của nội dung thông diệp, ví dụ di chuyển cá nguồn điện tử, các đặc tính, hợp đồng, thoả thuận v.v… Với tính quan trọng cao hoặc các trao đổi dữ liệu điện tử tương tự. Việc đánh giá các rủi ro an ninh nên được tiến hành để xác định nếu xác thực thông điệp được yêu cầu và để định danh hầu hết phương pháp thực hiện thích hợp.

Xác thực thông điệp không được thiết kế để bảo vệ nội dung của một thông diệp từ việc bị lộ trái phép. Các kỹ thuật mã hóa (xem 10.3.2 và 10.3.3) có thể được sử dụng như một biện pháp thích hợp để thực hiện xác thực thông điệp.

10.2.4 Kiểm tra tính hợp lệ của dữ liệu ra

Dữ liệu đầu vào từ một hệ thống ứng dụng nên được kiểm tra tính hợp lệ để đảm bảo rằng quá trình xử lý thông tin lưu trữ đúng và thích hợp với các trường hợp. Điển hình, các hệ thống được xây dựng trên giả thuyết rằng thực hiện việc kiểm tra tính hợp lệ, xác minh và thử nghiệm thích hợp để các dữ liệu ra sẽ luôn đúng. Điều này không luôn luôn xảy ra. Việc kiểm tra tính hợp lệ của đầu ra có thể gồm:

a) kiểm tra tính tin cậy để thử nghiệm dữ liệu ra có hợp lý không;

b) kiểm soát sự điều hoà có giá trị để đảm bảo quá trình xử lý toàn bộ dữ liệu;

c) cung cấp đầy đủ thông tin cho người đọc hoặc hệ thống xử lý sau để xác định tính chính xác, đầy đủ, có giá trị và phân loại thông tin;

d) các thủ tục phản ứng với kiểm tra tính hợp lệ đầu ra;

e) xác định trách nhiệm của toàn bộ cá nhân liên quan trong quá trình xử lý dữ liệu ra.

10.3 Các kiểm soát mật mã hóa

Đối tượng: Để bảo vệ tính tin cẩn, xác thực hoặc toàn vẹn của thông tin. các hệ thống và kỹ thuật mã hoá nên được sử dụng để bảo vệ thông tin được xem là có rủi ro và các kiểm soát khác không có bảo vệ thích hợp.

10.3.1 Chính sách về việc sử dụng các kiểm soát mật mã hóa

Đưa ra quyết định liệu một giải pháp mã hoá có thích hợp được xem như một phần của một quá trình đánh giá rủi ro và lựa chọn kiểm soát rộng hơn. Đánh giá rủi ro nên được tiến hành để xác định mức độ bảo vệ thông tin. Đánh giá này sau đó có thể được sử dụng để xác định xem một kiểm soát mã hoá liệu có phù hợp, loại kiểm soát nào nên được áp dụng và cho mục đích và các quá trình kinh doanh nào.

Một tổ chức nên phát triển một chính sách về việc sử dụng các kiểm soát mã hoá để bảo vệ thông tin. Một chính sách như vậy là cần thiết để tối đa lợi ích và giảm thiểu rủi ro của việc sử dụng các kỹ thuật mã hoá và để tránh việc sử dụng không thích hợp hoặc không đúng. Khi phát triển một chính sách, các điều sau nên được xem xét:

a) phương pháp quản lý hướng tới việc sử dụng các kiểm soát mật mã hóa trên toàn bộ tổ chức, bao gồm các quy tắc chung theo đó thông tin của doanh nghiệp được bảo vệ;

b) tiếp cận với quản lý khóa, bao gồm bao gồm xử lý khôi phục thông tin được mật mã trong trường hợp các khóa bị mất, hư hỏng hoặc tổn thất;

c) vai trò và trách nhiệm, ví dụ người chịu trách nhiệm;

d) thực thi chính sách đó;

e) quản lý khóa;

d) mức bảo vệ mã hoá thích hợp được xác định như thế nào;

g) các tiêu chuẩn được đưa vào để thực hiện có hiệu quả trong toàn tổ chức (giải pháp nào được sử dụng cho cá quá trình kinh doanh nào).

10.3.2 Sự mật mã hóa

Sự mật mã hóa là một kỹ thuật mã hoá có thể sử dụng để bảo vệ tính bảo mật của thông tin. Việc bảo vệ thông tin nhạy cảm hoặc có tính phê bình nên được xem xét.

Dựa trên đánh giá rủi ro, mức bảo vệ được yêu cầu nên được xác định có tính đến loại và chất lượng thuật toán mật mã được sử dụng và chiều dài của khóa mật mã được sử dụng.

Khi thực hiện chính sách mật mã của tổ chức nên cân nhắc các nguyên tắc và hạn chế về mặt quốc gia có thể áp dụng đối với việc sử dụng kỹ thuật mã hoá ở các vùng khác nhau trên thế giới và đối với các vấn đề luồng thông tin mật mã qua biên giới. Thêm vào đó nên cân nhắc các kiểm soát áp dụng đối với xuất nhập khẩu công nghệ mã hoá (xem thêm 12.1.6).

Lời khuyên chuyên gia nên được làm theo để xác định mức bảo vệ thích hợp, để lựa chọn các sản phẩm thích hợp sẽ cung cấp sự bảo vệ yêu cầu và triển khai một hệ thống an ninh quản lý khóa (xem 10.3.5). Ngoài ra, lời khuyên pháp lý có thể cần phải tuân theo liên quan đến các pháp và các nguyên tắc có thể áp dụng cho việc sử dụng mật mã dự định của tổ chức.

10.3.3 Các chữ ký điện tử

Các chữ ký điện tử có ý nghĩa bảo vệ tính xác thực và toàn vẹn của các tài liệu điện tử. Ví dụ; chúng có thể được sử dụng trong thương mại điện tử khi có nhu cầu xác minh người ký một văn bản điện tử và kiểm tra xem nội dung của văn bản đã ký có bị thay đổi không.

Các chữ ký điện tử có thể được áp dụng cho tất cả các dạng văn bản được xử lý điện tử, ví dụ chúng có thể được sử dụng để ký các thanh toán điện tử, chuyển giao vốn, hợp đồng và thoả thuận. Chữ ký điện tử có thể được thực hiện thông qua việc sử dụng một kỹ thuật mã hoá dựa trên một cặp khoá duy nhất mà một khóa được sử dụng để tạo ra chữ ký (khóa riêng) và khóa còn lại để kiểm tra chữ ký (khóa công bố).

Nên bảo vệ tính bảo mật của khóa riêng. Khoá này nên được giữ bí mật khi bất kỳ ai truy cập vào khóa này có thể ký văn bản, ví dụ thanh toán, hợp đồng, như vậy sẽ giả mạo chữ ký của người sở hữu khóa này. Ngoài ra, bảo vệ tính toàn vẹn của khóa công cộng cũng quan trọng. Việc bảo vệ này được cung cấp bằng việc sử dụng một chứng chỉ khóa công cộng (xem 10.3.5).

Cần phải cân nhắc loại và chất lượng của thuật toán chữ ký được sử dụng và chiều dài của khóa được sử dụng. Cá khóa mã hoá được sử dụng cho chữ ký điện tử nên khác các khóa sử dụng cho mật mã (xem 10.3.2).

Khi sử dụng chữ ký điện tử nên xem xét pháp luật liên quan mô tả các điều kiện theo đó một chữ ký điện tử bị ràng buộc về pháp lý. Ví dụ, trong trường hợp thương mại điện tử biết vị trí pháp lý của chữ ký điện tử là quan trọng. nó có thể cần thiết để có các hợp đồng hoặc các thoả thuận khác ràng buộc để hỗ trợ việc sử dụng chữ

ký điện tử khi khung luật pháp không thích hợp. Lời khuyên pháp lý nên được tuân theo liên quan đến các pháp và các nguyên tắc có thể áp dụng cho việc sử dụng mật mã dự định tổ chức của các chữ ký điện tử.

10.3.4 Các dịch vụ không từ chối nhận

Các dịch vụ không từ chối nhận nên được sử dụng ở nơi có thể cần thiết để giải quyết các tranh luận về việc xảy ra hoặc không xảy ra của một sự kiện hoặc hoạt động, ví dụ một tranh luận liên quan đến việc sử dụng một chữ ký điện tử trong một hợp đồng hoặc thanh toán điện tử. Chúng có thể giúp thiết lập bằng cớ để chứng minh một sự kiện hoặc hoạt động cụ thể có diễ ra hoặc không, ví dụ từ chối gửi một hướng dẫn sử dụng thư điện tử được ký bằng điện tử. Các dịch vụ này dựa trên việc sử dụng kỹ thuật mật mã và chữ ký điện tử (xem 10.3.2 và 10.3.3).

10.3.5 Quản lý khóa

10.3.5.1 Sự bảo vệ của các khóa mật mã hóa

Việc quản lý các khóa mật mã hóa là cần thiết để sử dụng hiệu quả các kỹ thuật mã hoá. Mọi tổn thất hoặc mất mát khóa mã hoá có thể dẫn đến tổn hại của tính bảo mật, xác thực và toàn vẹn của thông tin. Một hệ thống quản lý nên được thực hiện để hỗ trợ việc sử dụng 2 loại kỹ thuật mã hoá này của tổ chức, đó là:

a) kỹ thuật khóa bí mật, khi 2 bên hoặc hơn chia sẻ cùng một khóa và khóa này được sử dụng cho cả thông tin mã hoá và giải mã. Khóa này phải được giữ bí mật khi bất kỳ ai truy cập nó có thể giải mã toàn bộ thông tin được mã hoá với khóa đó hoặc đưa ra các thông tin trái phép;

b) kỹ thuật khóa công cộng, khi mỗi người sử dụng có một đôi khóa, một khóa công cộng (có thể tiết lộ với bất kỳ ai) và một khóa riêng (phải giữ bí mật). Kỹ thuật khóa công cộng có thể được sử dụng để mật mã hoá (xem 10.3.2) và tạo ra các chữ ký điện tử (xem 10.3.3).

Toàn bộ khóa nên được bảo vệ chống lại việc thay đổi và phá hoại và các khóa bí mật và riêng tư cần bảo vệ chống lại việc bị tiết lộ trái phép. Kỹ thuật mã hoá cũng có thể dược sử dụng cho mục đích này. Bảo vệ vật lý nên được sử dụng để bảo vệ thiết bị dùng để phát, lưu và lưu trữ khóa.

10.3.5.2 Các tiêu chuẩn, các thủ tục và phương pháp

Một hệ thống quản lý khóa nên được dựa trên một bộ các tiêu chuẩn, thủ tục và biện pháp an ninh được thoả thuận cho việc:

a) phát khóa cho các hệ thống mã hoá khác nhau và các ứng dụng khác nhau;

b) phát và dành được các chứng chỉ khóa công cộng;

c) phân phối khóa cho người sử dụng dự định, bao gồm việc các khóa được kích hoạt khi được nhận như thế nào;

d) lưu giữ các khóa, bao gồm việc người sử dụng đạt được truy cập khóa như thế nào;

e) thay đổi hoặc cập nhật các khóa bao gồm các quy tắc khi các khóa được thay đổi và sẽ được làm thế nào;

f) xử lý các khóa bị tổn hại;

g) thu hồi các khóa bao gồm việc các khóa bị rút hoặc mất tác dụng như thế nào, ví dụ khi cá khóa bị tổn hại hoặc khi một người sử dụng rời tổ chức (trong trường hợp đó các khóa cũng nên được lưu trữ lại);

h) thu hồi các khóa bị mất hoặc sai lạc như một phần của quản lý tính liên tục trong kinh doanh, ví dụ khôi phục thông tin mật mã;

i) lưu trữ các khóa, ví dụ các thông tin được lưu giữ hoặc sao chép dự phòng;

y) huỷ các khóa;

k) ghi nhật ký và kiểm tra sổ quản lý khóa liên quan đến các hoạt động.

Để giảm tổn thất có thể xẩy ra, cá khóa nên xác định các ngày có hiệu lực và hết hiệu lực, như vậy chúng chỉ có thể bị sử dụng trong một thời gian giới hạn. Khoảng thời gian này nên phụ thuộc vào từng trường hợp theo đó kiểm soát mã hoá được sử dụng và nhận biết rủi ro.

Các thủ tục có thể cần được cân nhắc đê giải quyết cá yêu cầu pháp lý đối với việc truy cập khóa mã hoá, ví dụ các thông tin được mật mã hoá có thể cần có ghi trong một dạng không mật mã như một chức cứ trong một vụ kiện.

Bên cạnh vấn đề các khóa bí mật và cá nhân tư được quản lý an toàn, việc bảo vệ cá khóa công cộng cũng nên được xem xét. Có một mối đe doạ về việc ai đó giả mạo chữ ký điện tử băng việc thay thế một khóa công cộng của người sử dụng với khóa của họ. Vấn đề này được định vị bằng việc sử dụng một chứng chỉ khóa công cộng. Các chứng chỉ này nên được tạo ra bằng cách trói buộc thông tin độc nhất liên quan tới người sở hữu cặp khóa công cộng/cá nhân với khóa công cộng. Như vậy điều quan trọng là quá trình quản lý cấp phát các chứngchỉ này có thể tin được. Quá trình này được thực hiện thông thường bằng việc cấp quyền chứng nhận từ một tổ chức được công nhận với các kiểm soát và thủ tục phù hợp để đưa ra mức độ tin cậy yêu cầu.

Nội dung của cá thoả thuận hoặc hợp đồng mức dịch vụ với cá nhà cung cấp bên ngoài các dịch vụ mã hoá, ví dụ với một quyền chứng nhận nên gồm các vấn đề về trách nhiệm pháp lý, sự tin cậy của các dịch vụ và thời gian trả lời cho việc cung cấp các dịch vụ (xem 4.2.2).

10.4 An ninh các tệp hệ thống

Đối tượng: Để đảm bảo rằng cá dự án IT và các hoạt động hỗ trợ được quản lý một cách an toàn.
việc truy cập vào các tệp hệ thống nên được kiểm soát.
Việc duy trì tính toàn vẹn của hệ thống nên là trách nhiệm của nhóm chức năng va phát triển người sử dụng đối với hệ thống ứng dụng hoặc phần mềm thuộc về ai.

10.4.1 Kiểm soát phần mềm thao tác

Nên có kiểm soát đối với việc tiến hành phần mềm trên các hệ thống hoạt động. Để giảm thiểu rủi ro của việc làm sai lạc các hệ thống hoạt động, các kiểm soát sau nên được xem xét:

a) cập nhật các thư viện chương trình hoạt động chỉ nên được tiến hành bởi người quản lý thư viện được bổ nhiệm theo quyền quản lý thích hợp (xem 10.4.3);

b) nếu có thể, các hệ thống hoạt động chỉ nên giữ mã có thể thể hiện được;

c) mã có thể thể hiện được không nên tiến hành trên một hệ thống hoạt động cho đến khi có được bằng chứng về việc kiểm tra và chấp nhận người sử dụng thành công và các thư viện nguồn chương trình tương ứng được cập nhật;

d) một dấu vết kiểm tra nên được duy trì về toàn bộ các cập nhật đối với các thư viện chương trình hoạt động

e) các phiên bản phần mềm trước nên được giữ lại để đề phòng bất trắc.

Các phần mềm do đại lý cung ứng được sử dụng trong các hệ thống hoạt động nên được duy trì ở mức được hỗ trợ bởi nhà cung ứng. Mọi quyết định nâng cấp tới mới bản mới nên tính đến an toàn của bản đó, tức là hướng dẫn về tính thiết thực an ninh mới hoặc số lượng và tính ác liệt của vấn đề an ninh ảnh hưởng tới phiên bản này. Các sửa đổi phần mềm nên được áp dụng khi chúng cần giúp để gỡ bỏ hoặc giảm những điểm yếu an ninh.

Các nhà cung ứng chỉ nên được truy cập vật lý hoặc logic để hỗ trợ các mục đích khi cần và với sự chấp thuận của ban quản lý. Các hoạt động của nhà cung ứng nên được giám sát.

10.4.2 Sự bảo vệ của dữ liệu thử nghiệm hệ thống

Dữ liệu thử nghiệm nên được bảo vệ và kiểm soát. Kiểm tra hệ thống và chấp nhận thường yêu cầu mức độ thật của dữ liệu thử nghiệm gần nhất có thể với dữ liệu hoạt động. Việc sử dụng cơ sở dữ liệu hoạt động chứa thông tin cá nhân nên được tránh. Nếu các thông tin này được dùng, chúng nên được giao lại cho cá nhân trước khi sử dụng. Các kiểm soát sau đây nên được áp dụng để bảo vệ dữ liệu hoạt động, khi được sử dụng cho các mục đích thử nghiệm.

a) các thủ tục kiểm soát truy cập áp dụng cho các hệ thống ứng dụng hoạt động, cũng nên áp dụng các hệ thống ứng dụng thử nghiệm;

b) nên có quyền riêng biệt mỗi lần thông tin hoạt động được sao chép tới một hệ thống ứng dụng thử nghiệm;

c) thông tin hoạt động nên được xóa khỏi một hệ thống ứng dụng thử nghiệm ngay sau khi thử nghiệm hoàn thành;

d) việc sao chép và sử dụng thông tin hoạt động nên được ghi chép nhật ký thành một dấu vết kiểm tra.

10.4.3 Kiểm soát truy cập tới thư viện gốc của chương trình

Để giảm tiềm ẩn của việc sai lạc các chương rình máy tính, kiểm soát chặt chẽ nên được duy trì đối với việc truy cập các thư viện nguồn chương trình như sau (xem 8.3):

a) nơi có thể, các thư viện nguồn chương trình không nên được giữ trong các hệ thống hoạt động;

b) một thư viện chương trình nên được chỉ định cho mỗi ứng dụng;

c) nhân viên hỗ trợ IT không nên không được hạn chế truy cập tới các thư viện nguồn chương trình;

d) các chương trình phát triển hoặc bảo dưỡng không nên giữ trong các thư viện nguồn chương trình;

e) cập nhật các thư viện nguồn chương trình và phát hành cá nguồn chương trình tới nhưng người làm chương trình chỉ nên được thực hiện bởi người quản lý thư viện được chỉ định theo quyền từ người quản lý hỗ trợ IT cho ứng dụng đó cấp;

f) lập danh sách chương trình nên được giữ trong một môi trường an toàn (xem 8.6.4);

g) một dấu vết kiểm tra nên được duy trì toàn bộ cá nhân truy cập vào thư viện nguồn chương trình;

h) các phiên bản cũ của cá chương trình hoạt động nên được lưu trữ, với một sự chỉ định rõ ràng ngày giờ chính xác khi chũng được hoạt động, cùng với toàn bộ phần mềm hỗ trợ, kiểm soát công việc, xác định dữ liệu và cá thủ tục;

i) duy trì và sao chép các thư viện nguồn chương trình nên là để giám sát chặt cá thủ tục kiểm soát thay đổi (xem 10.4.1).

10.5 An ninh quá trình hỗ trợ và phát triển

Đối tượng: Để duy trì an ninh của phần mềm và thông tin hệ thống ứng dụng.
Các môi trường dự án và hỗ trợ nên được kiểm soát chặt chẽ.
Các nhà quản lý có trách nhiệm đối với các hệ thống ứng dụng cũng nên có trách nhiệm với an ninh của môi trường dự án và hỗ trợ. Họ nên đảm bảo rằng toàn bộ cá thay đổi hệ thống đưa ra được soát xét để kiểm tra rằng chúng không làm tổn hại an ninh của hệ thống cũng như môi trường hoạt động.

10.5.1 Kiểm soát sự thay đổi các thủ tục

Để tối thiểu sự sai lạc của các hệ thống thông tin nên có kiểm soát chặt chẽ đối với việc thực hiện các thay đổi. Các thủ tục kiểm soát thay đổi chính thức nên được bắt buộc. Nên đảm bảo rằng các thủ tục an ninh và kiểm soát không bị tổn hại, những người làm chươngtrình hỗ trợ chỉ được truy cập tới những phần của hệ thống cần cho công việc của họ và có được sự đồng ý và chấp thuận chính thức cho bất kỳ thay dổi nào. Thay đổi phần mềm ứng dụng có thể ảnh hưởng môi trường hoạt động. Ở mọi nơi có thể thử nghiệm, các thủ tục ứng dụng và kiểm soát thay đổi hoạt động nên được thống nhất (xem 8.1.2). Thủ tục này nên bao gồm:

a) duy trì một bản ghi các mức độ quyền hạn được thoả thuận;

b) đảm bảo những thay đổi là do người sử dụng được cấp phép;

c) soát xét các kiểm soát và các thủ tục toàn vẹn để đảm bảo rằng chúng sẽ không bị tổn hại vì các thay đổi;

d) định danh toàn bộ phần mềm máy tính, thông tin, các thực thể cơ sở dữ liệu và phần cứng yêu cầu sự sửa đổi;

e) đạt được sự chấp thuận chính thức cho các đề xuất chi tiết trước khi công việc bắt đầu;

f) đảm bảo rằng người sử dụng có phép chấp nhận những thay đổi trước khi có bất kỳ hoạt động nào;

g) đảm bảo rằng việc thực hiện được tiến hành để giảm tối đa sự phá vỡ kinh doanh;

h) đảm bảo rằng bộ ghi chép hệ thống được cập nhật đầy đủ mỗi thay đổi và ghi chép cũ được lưu giữ hoặc sắp xếp;

i) duy trì một phiên bản kiểm soát cho toàn bộ các cập nhật phần mềm;

j) duy trì một dấu vết kiểm tra toàn bộ các yêu cầu thay đổi;

k) đảm bảo rằng việc ghi tài liệu hoạt động (xem 8.1.1) và các thủ tục cho người sử dụng được thay đổi nếu cần để thích hợp;

l) đảm bảo rằng việc thực hiện các thay đổi tiến hành đúng lúc và không làm rối loạn các thủ tục kinh doanh liên quan.

Nhiều tổ chức duy trì một môi trường trong đó người sử dụng thử nghiệm các phần mềm mới và được tách biệt với các môi trường phát triển và sản phẩm. Điều này có nghĩa là có kiểm soát đối với phần mềm mới và cho phép bảo vệ thêm thông tin hoạt động được sử dụng cho mục đích thử nghiệm.

10.5.2 Xem xét kỹ thuật của các thay đổi hệ điều hành

Thay đổi hệ thống hoạt động một cách định kỳ là cần thiết, ví dụ để thiết lập một bản hoặc cá sửa đổi phần mềm được cung ứng gần đây. Khi xảy ra các thay đổi, các hệ thống ứng dụng nên được soát xét và thử nghiệm để đảm bảo rằng không có ảnh hưởng có hại tới hoạt động hoặc an ninh. Thủ tục này nên gồm:

a) soát xét các thủ tục kiểm soát ứng dụng và toàn vẹn để đảm bảo rằng chúng không bị tổn hại do các thay đổi hệ thống đang hoạt động;

b) đảm bảo rằng kế hoạch và ngân sách hỗ trợ thường niên sẽ bao gồm các soát xét và thử nghiệm hệ thống do các thay đổi hệ thống hoạt động;

c) đảm bảo rằng việc thông báo các thay đổi hệ thống hoạt động được đưa ra đúng lúc để cho phép các soát xét thích hợp tiến hành trước khi thực hiện;

d) đảm bảo rằng các thay đổi thích hợp được làm cho các kế hoạch hoặc liên tục trong kinh doanh (xem mục 11).

10.5.3 Các hạn chế thay đổi đối với các gói phần mềm

Các thay đổi về gói phần mềm nên được can ngăn. Các gói phần mềm do đại lý cung ứng nên được sử dụng mà không có thay đổi trong chừng mực có thể và có thể thử nghiệm. Nếu cho rằng cần thiết phải thay đổi gói phần mềm, các điểm sau nên được xem xét:

a) rủi ro của các kiểm soát cài đặt sẵn và các thủ tục toàn vẹn bị tổn hại;

b) liệu có nên đạt được sự cho phép của đại lý không;

c) khả năng đạt được cá thay đổi được yêu cầu từ đại lý như là các cập nhật chương trình tiêu chuẩn;

d) sự tác động nếu tổ chức đó trở nên có trách nhiệm đối với cá bảo dưỡng các phần mềm trong tương lai như kết quả của sự thay đổi.

Nếu các thay đổi được cho là cần thiết phần mềm gốc nên được giữ lại và các thay đổi áp dụng cho một bản sao định danh rõ ràng. Toàn bộ thay đổi nên được thử nghiệm và ghi chép đầy đủ, như vậy chúng có thể được áp dụng lại nếu cần cho các nâng cấp phần mềm trong tương lai.

10.5.4 Các kênh chuyển đổi và mã thành Troa

Một kênh ngầm có thể phô bày thông tin bằng một số cách không trực tiếp và khó hiểu. Nó có thể bị kích hoạt bằng sự thay đổi một tham số có thể truy cập được bằng cả các yếu tố an ninh và không an ninh của một hệ thống máy tính hoặc bằng việc đưa thông tin vào một suối dữ liệu. Mã trojan được thiết kế để ảnh hưởng đến một sý bằng một cách trái phép và khôngđược thông báo sẵn sàng và không được yêu cầu bởi người nhận hoặc người sử dụng chương trình. Các kênh ngầm và mã trojan hiếm khi xảy ra bởi tai nạn. Nơi có các kênh ngầm hoặc mã trojan là một nỗi lo, các điều sau nên được xem xét:

a) chỉ mua các chương trình có nguồn đáng tin;

b) mua các chương trình có mã nguồn mà có thể được xác minh;

c) sử dụng các sản phẩm đã được đánh giá;

d) thanh tra toàn bộ mã nguồn trước khi sử dụng hoạt động;

e) kiểm soát truy cập và thay đổi mã khi cài đặt;

f) sử dụng nhân viên có độ tin cậy qua thử thách để làm việc tại các hệ thống quan trọng.

10.5.5 Xây dựng phần mềm được cung ứng

Nơi phát triển phần mềm nhận cung ứng, các điểm sau nên được xem xét:

a) các thoả thuận cấp giấy phép, các quyền sở hữu mã và quyền sở hữu trí tuệ (xem 12.1.2);

b) chứng nhận về chất lượng và sự chính xác của công việc được thực hiện;

c) các thoả thuận có bên thứ 3 trong trường hợp lỗi của bên thứ 3;

d) quyền truy cập kiểm toán chất lượng và độ chính xác của công việc được làm;

e) các yêu cầu bằng hợp đồng về chất lượng mã;

f) thử nghiệm trước khi cài đặt để phát hiện mã trojan.

11 Quản lý liên tục trong kinh doanh

11.1 Các khía cạnh về quản lý liên tục trong kinh doanh

Đối tượng: Để chống lại sự gián đoạn các hoạt động kinh doanh và để bảo vệ các thủ tục kinh doanh có tính phê bình khỏi các tác động của các lỗi hoặc thảm hoạ lớn.

Một thủ tục quản lý liên tục trong kinh doanh nên được thực hiện để giảm sự phá vỡ do các thảm hoạ và lỗi an ninh (có thể do ví dụ thiên tai, tai nạn, lỗi thiết bị và các hành động có chủ ý) đối với một mức chấp nhận được qua một sự kết hợp các kiểm soát phòng ngừa và khôi phục.

Hậu quả của các thảm hoạ, lỗi an ninh và mất dịch vụ nên được phân tích. Các kế hoạch bất ngờ nên được phát triển và thực hiện để đảm bảo rằng các thủ tục kinh doanh có thể khôi phục trong phạm vi thời gian yêu cầu. Các kế hoạch như vậy nên được duy trì và thử nghiệm để trở thành một phần không thể thiếu của toàn bộ các thủ tục quản lý khác. Quản lý liên tục trong kinh doanh nên bao gồm các kiểm soát để định danh và giảm rủi ro, hạn chế hậu quả của các sự cố nguy hại và đảm bảo sự tiếp tục lại các hoạt động cần thiết đúng lúc.

11.1.1 Quản lý tính liên tục của thủ tục kinh doanh

Nên có một thủ tục được quản lý cho việc phát triển và duy trì liên tục trong kinh doanh trong suốt tổ chức. Nó nên gồm cả các yếu tố quản lý liên tục trong kinh doanh chính:

a) hiểu biết các rủi ro mà tổ chức phải đối mặt dưới dạng có thể xảy ra và tác động của chúng, bao gồm định danh và understanding các rủi ro tổ chức đó is facing dưới dạng their likelihood và their impact, bao gồm an identification và dành ưu tiên của các thủ tục kinh doanh có tính phê bình;

b) hiểu biết tác động mà sự gián đoạn chắc chắn có trong kinh doanh (điều quan trọng là các giải pháp được tìm ra sẽ xử lý các sự cố nhỏ hơn, cũng như các sự cố nghiêm trọng có thể đe doạ khả năng tồn tại và phát triển của tổ chức) và thiết lập các mục tiêu kinh doanh của các phương tiện xử lý thông tin;

c) xem xét việc mua bán bảo hiểm phù hợp có thể là một phần của thủ tục liên tục trong kinh doanh;

d) trình bày và ghi chép rõ một chiến lược liên tục trong kinh doanh thống nhất với các mục tiêu và quyền ưu tiên của doanh nghiệp đã được thông qua;

e) trình bày và ghi chép rõ các kế hoạch liên tục trong kinh doanh theo chiến lược đã thông qua;

f) thường xuyên kiểm tra và cập nhật các kế hoạch và thủ tục đang diễn ra;

g) đảm bảo rằng việc quản lý liên tục trong kinh doanh được phối hợp trong các thủ tục và cấu trúc của tổ chức. Trách nhiệm phối hợp các quản lý liên tục trong kinh doanh nên được ấn định ở một mức thích hợp trong tổ chức, ví dụ tại diễn đàn an ninh thông tin (xem 4.1.1).

11.1.2 Phân tích tác động và liên tục trong kinh doanh

Tính liên tục trong kinh doanh nên bắt đầu bằng định danh các sự kiện có thể gây ra sự gián đoạn các thủ tục kinh doanh, ví dụ lỗi thiết bị, lụt lội và hoả hoạn. Điều này nên được tiếp theo bằng một sự đáng giá rủi ro để xác định tác động của những sự gián đoạn đó (cả ở quy mô tổn thất và thời gian khôi phục). Các hoạt động này nên được thực hiện với sự liên quan đầy đủ từ chủ sở hữu các nguồn và thủ tục kinh doanh. Việc đánh giá này xem xét toàn bộ các thủ tục kinh doanh và không được giới hạn đối với cá phương tiện xử lý thông tin.

Dựa vào kết quả đánh giá rủi ro, một kế hoạch chiến lược nên được phát triển để xác định sự tiếp cận toàn diện tới tính liên tục trong kinh doanh. khi kế hoạch này được tạo ra, nó nên được xác nhận bởi ban quản lý.

11.1.3 Ghi lại và thực hiện các kế hoạch về tính liên tục

Các kế hoạch nên được phát triển để duy trì hoặc khôi phục các hoạt động kinh doanh trong phạm vi thời gian yêu cầu theo sự gián đoạn hoặc lỗi của các thủ tục kinh doanh có tính phê bình. Thủ tục lập kế hoạch liên tục trong kinh doanh nên xem xét các vấn đề sau:

a) định danh và thỏa thuận toàn bộ các trách nhiệm và các thủ tục trong trường hợp khẩn cấp;

b) thực hiện các thủ tục về tình trạng khẩn cấp để cho phép khắc phục và khôi phục trong phạm vi thời gian yêu cầu. cần chú ý đặc biệt tới sự đánh giá của những bên phụ thuộc kinh doanh bên ngoài và các hợp đồng thực hiện;

c) tài liệu hoá các thủ tục và thủ tục thoả thuận;

d) đào tạo thích hợp nhân viên về các thủ tục và thủ tục trong trường hợp khẩn cấp được thoả thuận bao gồm quản lý khủng hoảng;

e) kiểm tra và cập nhật các kế hoạch.

Thủ tục lập kế hoạch nên nhắm vào các mục tiêu kinh doanh được yêu cầu, ví dụ khôi phục các dịch vụ cụ thể cho khách hàng trong khoảng thời gian chấp nhận được. Các dịch vụ và nguồn sẽ có thể xảy ra nên được xem xét, bao gồm việc bố trí nhân viên, các nguồn xử lý phi thông tin, cũng như các sắp xếp dự trữ cho các phương tiện xử lý thông tin.

11.1.4 Khuôn khổ lập kế hoạch liên tục trong kinh doanh

Một khuôn khổ các kế hoạch liên tục trong kinh doanh nên được duy trì để đảm bảo rằng toàn bộ các kế hoạch nhất quán và để định danh quyền ưu tiên cho việc kiểm tra và bảo dưỡng. Mỗi kế hoạch liên tục trong kinh doanh nên phân biệt rõ ràng các điều kiện cho sự kích hoạt của nó, cũng như trách nhiệm cá nhân về thực thi từng phần của kế hoạch. Khi các yêu cầu mới được xác định, thiết lập các thủ tục về trường hợp khẩn cấp, ví dụ cá kế hoạch tản cư hoặc bất kỳ sự sắp xếp dự phòng tồn tại nên được sửa đổi thích hợp.

Một bộ khuôn khổ cho việc lập kế hoạch liên tục trong kinh doanh nên xem xét những điều sau:

a) các điều kiện để kích hoạt các kế hoạch trình bày thủ tục được tiếp diễn (cách đánh giá tình hình, người có liên quan, v.v) trước khi mỗi kế hoạch được bắt đầu;

b) các thủ tục về tình trạng khẩn cấp trình bày các hoạt động diễn ra sau một sự cố mà có nguy cơ cho các hoạt động kinh doanh và/hoặc đời sống con người. Điều nên bao gồm các chuẩn bị cho quản lý các quan hệ công chúng và liên lạc có hiệu quả với các bộ phận thẩm quyền công cộng thích hợp, ví dụ cảnh sát, phòng cháy chữa cháy và chính quyền địa phương;

c) các thủ tục dự phòng trình bày các hoạt động diễn ra để di chuyển các hoạt động kinh doanh cần thiết và các dịch vụ hỗ trợ cho các địa phương tạm thời khác và để đưa các thủ tục kinh doanh hoạt động lại trong phạm vi thời gian được yêu cầu;

d) các thủ tục bắt đầu lại trình bày các hoạt động diễn ra để quay lại các hoạt động kinh doanh thông thường;

e) một lịch trình bảo dưỡng xác định cách và khi nào kế hoách sẽ được kiểm tra và thủ tục duy trì kế hoạch;

f) các hoạt động nhận thức và giáo dục được thiết kế để tạo ra sự hiểu biết về các thủ tục liên tục trong kinh doanh và đảm bảo rằng cá thủ tục tiếp tục có hiệu quả;

g) trách nhiệm của các cá nhân, trình bày ai chịu trách nhiệm thực thi phần nào của kế hoạch. các sự lựa chọn nên được bổ nhiệm theo yêu cầu.

Mỗi kế hoạch nên có chủ sở hữu cụ thể. các thủ tục về trường hợp khẩn cấp, các kế hoach dự phòng thủ công và các kế hoạch bắt đầu lại nên trong trách nhiệm của chủ sở hữu các nguồn và thủ tục kinh doanh thích hợp có liên quan. Các chuẩn bị dự phòng cho các dịch vụ kỹ thuật lựa chọn, như các phương tiện xử lý và truyền thông tin nên thường xuyên là trách nhiệm của người cung cấp dịch vụ.

11.1.5 Thử nghiệm, duy trì và đánh giá lại các kế hoạch liên tục của doanh nghiệp

11.1.5.1 Kế hoạch thử nghiệm

Các kế hoạch liên tục trong kinh doanh có thể thất bại khi được kiểm tra, thường là do các giả định, giám sát, thay đổi sai của thiết bị hoặc con người. Vì vậy chúng nên được kiểm tra thường xuyên để đảm bảo rằng chúng đợc cập nhật vàhq. Các kiểm tra như vậy cũng nên đảm bảo rằng toàn bộ các thành viêm của đội khôi phục và các nhan viên có liên quan khác biết rõ về các kế hoạch.

Lịch trình kiểm tra cho các kế hoạch liên tục trong kinh doanh nên chỉ rõ cách thức và khi nào thì mỗi yếu tố của kế hoạch đợc thử nghiệm. Khuyến cáo nên kiểm tra các bộ phận cá nhân của kế hoạch thường xuyên. Nhiều kỹ thuật nên được sử dụng để đảm bảo rằng các kế hoạch sẽ hoạt động thực sự. Điều này nên bao gồm:

a) thử nghiệm trên bàn nhiều viễn cảnh (thảo luận các sắp xếp khôi phục kinh doanh sử dụng những sự gián đoạn ví dụ);

b) bắt chước (đặc biệt đào tạo con người trong các vai trò quản lý hậu sự cố/ khủng hoảng của họ);

c) thử nghiệm cách khôi phục kỹ thuật (đảm bảo các hệ thống thông tin có thể được khôi phục hiệu quả);

d) thử nghiệm khôi phục tại một vị trí lựa chọn (chạy các thủ tục kinh doanh song song với các hoạt động khôi phục xa vị trí chính);

e) các cuộc thử nghiệm các phương tiện và dịch vụ cung ứng (đảm bảo các dịch vụ và sản phẩm cung cấp bên ngoài sẽ đáp ứng sự cam kết đã được ký kết);

f) hoàn thành những lần diễn tập (kiểm tra xem tổ chức, cá nhân, thiết bị, các phương tiện và thủ tục có đương đầu được với những sự gián đoạn).

Các kỹ thuật có thể được sử dụng bởi bất kỳ tổ chức nào và nên phản ánh đặc tính của kế hoạch khôi phục cụ thể.

11.1.5.2 Các kế hoạch duy trì và đánh giá lại

Các kế hoạch liên tục trong kinh doanh nên được duy trì bằng các cuộc soát xét và cập nhật đều đặn để đảm bảo tính hiệu quả liên tiếp của chúng (xem 11.1.5.1 và 11.1.5.3). Các thủ tục nên được có trong chương trình quản lý thay đổi của tổ chức để đảm bảo rằng các vấn đề liên tục trong kinh doanh được định vị thích hợp.

Trách nhiệm nên được ấn định cho các soát xét đều đặn cho mỗi kế hoạch liên tục trong kinh doanh, định danh các thay đổi trong các sắp xếp kinh doanh vẫn chưa phản ánh trong các kế hoạch liên tục trong kinh doanh nên được tiếp theo bởi sự cập nhật kế hoạch thích hợp. Thủ tục kiểm soát thay đổi chính thức này nên đảm bảo rằng các kế hoạch cập nhật được phân phối và tăng cường bởi các soát xét đều đặn kế hoạch đầy đủ.

Các ví dụ cho cácc tình huống có thể đòi hỏi cập nhật các kế hoạch bao gồm cái thu được của thiết bị mới hoặc sự nâng cấp các hệ thống hoạt động và các thay đổi về:

a) con người;

b) các địa chỉ và số điện thoại;

c) chiến lược kinh doanh;

d) vị trí, các phương tiện, các nguồn;

e) pháp luật;

f) các nhà thầu, các nhà cung ứng và các khách hàng quan trọng;

g) các thủ tục hoặc các thủ tục mới/ loại bỏ;

h) rủi ro (về hoạt động và tài chính).

12 Sự tuân thủ

12.1 Tuân thủ các yêu cầu pháp lý

Đối tượng: Để tránh các vi phạm bất kỳ luật hình sự và dân sự, các nghĩa vụ có tính luật pháp, nguyên tắc hoặc giao kèo và bất kỳ yêu cầu an ninh nào.

Việc thiết kế, hoạt động, sử dụng và quản lý các hệ thống thông tin có thể cần có các yêu cầu có tính luật pháp, nguyên tắc hoặc giao kèo.

Lời khuyên về các yêu cầu pháp lý cụ thể nên được theo các nhà tư vấn pháp lý của tổ chức hoặc những người thực hành luật pháp có chất lượng phù hợp. Các yêu cầu pháp lý về việc thông tin được tạo ra ở một nước truyền phát tới một nước khác (tức là luồng dữ liệu qua biên giới) là khác nhau giữa các nước.

12.1.1 Xác định văn bản pháp lý có thể áp dụng

Toàn bộ các yêu cầu có tính luật pháp, nguyên tắc hoặc giao kèo nên được xác định và tài liệu hoá rõ ràng đối với mỗi hệ thống thông tin. Các kiểm soát cụ thể và các trách nhiệm cá nhân phải đáp ứng các yêu cầu nên được xác định và tài liệu hoá tương ứng.

12.1.2 Các quyền sở hữu trí tuệ (IPR)

12.1.2.1 Bản quyền

Các thủ tục thích hợp nên được thi hành để đảm bảo tuân thủ các hạn chế pháp lý về việc sử dụng tư liệu đặc biệt là về cái có thể là các quyền sở hữu trí tuệ, như bản quyền, quyền thiết kế, nhãn hiệu thị trường. Sự xâm phạm bản quyền có thể dẫn tới kiện tụng có thể liên quan đến tội phạm.

Toàn bộ các yêu cầu có tính luật pháp, nguyên tắc hoặc giao kèo có thể xảy ra các hạn chế về bản quyền tư liệu độc quyền. Cụ thể, họ có thể yêu cầu chỉ có thể sử dụng tư liệu được phát triển bởi tổ chức hoặc được cấp giấy phép hoặc cung cấp bởi những nhà phát triển của tổ chức.

12.1.2.2 Bản quyền phần mềm

Các sản phẩm phần mềm độc quyền thường được cung ứng dưới một thoả thuận giấy phép giới hạn việc sử dụng các sản phẩm cho các máy cụ thể và có thể giới hạn bản quyền cho việc tạo lập chỉ các bản sao dự phòng. Nên xem xét các kiểm soát sau đây:

a) xuất bản một chính sách tuân thủ bản quyền phần mềm xác định việc sử dụng pháp lý các sản phẩm phần mềm và thông tin;

b) phát hành các tiêu chuẩn cho các thủ tục giành được cá sản phẩm phần mềm;

c) việc duy trì nhận thức về bản quyền phần mềm và các chính sách giành được và đưa ra thông báo về mục đích thự hiện hoạt động kỷ luật đối với các nhân viên vi phạm;

d) việc duy trì những người đăng ký sở hữu thích hợp;

e) việc duy trì bằng chứng và chứng cớ về các quyền sở hữu giấy phép, các đĩa chủ, sách hướng dẫn, v.v;

f) việc thực hiện các kiểm soát để đảm bảo rằng số người sử dụng lớn nhất được phép không vượt quá;

g) tiến hành các kiểm tra để chỉ cài đặt được các phần mềm được phép và các sản phẩm có giấy phép;

h) cung cấp một chính sách để duy trì các điều kiện giấy phép thích hợp;

i) cung cấp một chính sách để sắp xếp và chuyển giao phần mềm cho những người khác;

j) sử dụng các công cụ kiểm toán thích hợp;

k) tuân thủ các điều khoản và điều kiện lấy được phần mềm và thông tin từ các mạng công cộng (xem 8.7.6).

12.1.3 Bảo vệ các báo cáo của tổ chức

Các bản lưu quan trọng của một tổ chức nên được bảo vệ khỏi mất mát, phá hoại và làm giả. Một số bản lưu cần được lưu giữ an toàn để đáp ứng các yêu cầu có tính pháp luật hoặc nguyên tắc, cũng như hỗ trợ các hoạt động kinh doanh cần thiết. Ví dụ các bản lưu có thể được yêu cầu như bằng cớ để một tổ chức hoạt động trong các quy tắc pháp lý hoặc nguyên tắc hoặc để đảm bảo phòng vệ thích hợp chống lại các vụ kiện dân sự hoặc hình sự tiềm tàng hoặc để xác định lại tình trạng tài chính của tổ chức đối với các cổ đông, đối tác và kiểm toán viên. Khoảng thời gian và nội dung dữ liệu đối với việc sở hữu thông tin có thể xác định bằng luật hoặc nguyên tắc quốc gia.

Các bản lưu nên được phân tách thành các loại bản lưu, ví dụ các bản lưu giải trình, các bản lưu cơ sở dữ liệu, các nhật ký giao dịch và các thủ tục hoạt động, mỗi chi tiết của thời hạn sở hữu và loại phương tiện truyềnthông lưu trữ, ví dụ giấy, tấm vi phim, chất có từ tính, dụng cụ quang học. Bất kỳ khóa mã hoá liên quan được kết hợp với các hồ sơ được mật mã hoá hoặc các chữ ký điện tử (xem 10.3.2 và 10.3.3) nên được giữ an toàn và sẵn sàng cho những người được phép khi cần.

Nên xem xét khả năng xuống cấp của phương tiện truyền thông sử dụng cho việc lưu trữ các bản lưu. Lưu trữ và xử lý các thủ tục nên được thực hiện theo các khuyến cáo của nhà sản xuất.

Khi phương tiện truyền thông lưu trữ điện tử được lựa chọn, cá thủ tục đảm bảo khả năng truy cập dữ liệu (cả phương tiện truyền thông và khả năng đọc dạng mẫu) trong suốt thời hạn sở hữu nên có để bảo vệ chống lại sự mất ámt do thay đổi công nghệ trong tương lai.

Các hệ thống lưu trữ dữ iệu nên được chọn để cá dữ liệu đước yêu cầu cóthể lấy lại trong dạng có thể chấp nhận được cho một phiên toà, ví dụ toàn bộ các bản lưu được yêu cầu có thể lấy lại trong một khung thời gian có thể chấp nhận và trong một khuôn mẫu có thể chấp nhận được.

Hệ thống lưu trữ và xử lý nên đảm bảo việc định danh rõ ràng các bản lưu và thời hạn sở hữu có tính luật pháp hoặc nguyên tắc của chúng. Nên cho phép phá hoại thích hợp các bản lưu sau thời hạn đó nếu chúng không có cần cho tổ chức nữa.

Đáp ứng những nghĩa vụ này, các bước sau nên được thực hiện trong một tổ chức:

a) các hướng dẫn nên được phát hành về việc sở hữu, lưu trữ, xử lý và huỷ bỏ các bản lưu và thông tin.

b) một lịch trình sở hữu nên được xây dựng để định danh các loại bản lưu cần thiết và khoảng thời gian có được chúng.

c) một bản kiểm kê các nguồn của thông tin quan trọng nên được duy trì.

d) các kiểm soát thích hợp nên được thực hiện để bảo vệ các bản lưu và thông tin cần thiết khỏi mất mát, phá hoại và làm giả.

12.1.4 Bảo vệ dữ liệu đảm bảo bí mật của thông tin cá nhân

Một số nước hướng dẫn xây dựng luật thực hiện các kiểm soát về xử lý và chuyển giao dữ liệu cá nhân (nói chung thông tin về cuộc sống các cá nhân những người có thể được định danh từ các thông tin đó). Các kiểm soát như vậy có thể buộc trách nhiệm cho việc thu thập, xử lý và phổ biến thông tin cá nhân và có thể hạn chế khả năng chuyển dữ liệu đó tới các nước khác.

Việc tuân thủ xây dựng luật bảo vệ dữ liệu yêu cầu cấu trúc và kiểm soát quản lý thích hợp. Điều này thường đạt hiệu quả nhất bằng việc bổ nhiệm một quan chức bảo vệ dữ liệu đưa ra hướng dẫn cho các nhà quản lý, người sử dụng và người cung cấp dịch vụ về trách nhiệm của họ và các thủ tục cụ thể nên được tuân theo. việc thông báo cho quan chức bảo vệ dữ liệu về bất kỳ đề xuất nào để giữ thông tin cá nhân trong một tệp được cấu trúc và để đảm bảo nhận thức về quy tắc bảo vệ dữ liệu được xác định trong việc xây dựng luật pháp liên quan nên là trách nhiệm của chủ sở hữu.

12.1.5 Ngăn ngừa việc sử dụng sai các phương tiện xử lý thông tin

Các phương tiện xử lý thông tin của một tổ chức được cung cấp vì những mục đích kinh doanh. Ban quản lý nên cấp quyền sử dụng chúng. Bất kỳ việc sử dụng nào các phương tiện này vì mục đích phi kinh doanh hoặc trái phép, không có sự chấp thuận của ban quản lý nên được coi như sử dụng sai các phương tiện này. Nếu hoạt động như vậy được định danh bằng việc các phương tiện giám sát hoặc các phương tiện khác, nhà quản lý cá nhân nên chú ý liên quan tới hoạt động kỷ luật thích hợp.

Tính hợp pháp của việc giám sát cách sử dụng khác nhau giữa các nước và có thể yêu cầu nhân viên phải được khuyến cáo về các giám sát như vậy hoặc phải có được sự đồng ý của họ. Những lời khuyên pháp lý nên được đưa ra trước khi thực hiện các thủ tục giám sát.

Nhiều nước có hoặc đang trong thủ tục giới thiệu, xây dựng luật để bảo vệ chống lại lạm dụng máy tính. Nên có phòng vệ tội phạm sử dụng máy tính vì những mục đích trái phép. Vì vậy toàn bộ người sử dụng phải nhận thức về chính xác phạm vi được phép truy cập là điều cần thiết. Ví dụ điều này có thể đạt hiệu quả bằng cách đưa cho người sử dụng giấy phép viết tay, một bản sao của nó nên được người sử dụng ký và được tổ chức giữ an toàn. Các nhân viên của một tổ chức và người sử dụng bên thứ ba nên được khuyên rằng không truy cập nếu trái phép.

Ở bước khởi động, một thông điệp cảnh báo nên được hiện ra trên màn hình máy tính chỉ rõ rằng hệ thống đang được mở là riêng tư và truy cập trái phép là trái phép. Người sử dụng phải hiểu và phản ứng thích hợp với thông điệp trên màn hình này để tiếp tục thủ tục khởi động.

12.1.6 Quy định các kiểm soát mật mã hóa

Một một số nước đã thực hiện các thỏa thuận, luật, nhuyên tắc hoặc các văn kiện khác để kiểm soát việc truy cập hoặc sử dụng các kiểm soát mã hoá. kiểm soát như vậy có thể bao gồm:

a) nhập khẩu và/ hoặc xuất khẩu phần cứng và phần mềm máy tính để tiến hành các chức năng mã hoá;

b) nhập khẩu và/ hoặc xuất khẩu phần cứng và phần mềm máy tính được thiết kế để có thêm các chức năng mã hoá;

c) cách cách thức truy cập có tính bắt buộc hoặc thực thi tuỳ chọn bởi các nước đối với thông tin được mật mã hoá báng phần mềm và phần cứng để cung cấp tính bảo mật của nội dung.

Lời khuyên pháp lý nên được theo để đảm bảo tuân thủ luật quốc gia. Trước khi các thông tin được mật mã và các kiểm soát mã hoá được chuyển cho một nước khác, lời khuyên pháp lý cũng nên được đưa ra.

12.1.7 Tập hợp chứng cớ

12.1.7.1 Các quy tắc đối với chứng cớ

Cần thiết phải có chứng cớ đầy đủ để hỗ trợ một hoạt động chống lại một người hoặc một tổ chức. Mỗi khi hoạt động này là một vấn đề kỷ luật nội bộ chứng cớ cần thiết sẽ được trình bày bằng các thủ tục nội bộ.

Khi hoạt động này liên quan đến luật pháp, dân sự và hình sự, chứng cớ được trình bày nên phù hợp với các quy tắc để chứng cớ được đặt trong luật có liên quan hoặc các quy tắc của toà án cụ thể mà trường hợp này sẽ được đưa ra. nói chung, các quy tắc này gồm:

a) tính thừa nhận chứng cớ. Liệu chứng cớ này có thể sử dụng trong toà hoặc không;

b) sức nặng của chứng cớ: Chất lượng và tính đầy đủ của chứng cớ;

c) chứng cớ tương xứng mà các kiểm soát được tiến hành chính xác và nhất quán (tức là thủ tục kiểm soát chứng cớ) trong suốt thời gian chứng cớ được tìm lại được hệ thống lưu giữ và xử lý.

12.1.7.2 Tính thừa nhận chứng cớ

Để đạt được sự thừa nhận chứng cớ, các tổ chức nên đảm bảo rằng hệ thống thông tin của họ tuân thủ mọi tiêu chuẩn được phát hành hoặc mã thử nghiệm đối với sản phẩm của chứng cớ có thể được thừa nhận.

12.1.7.3 Chất lượng và tính đầy đủ của chứng cớ

Để đạt được chất lượng và tính đầy đủ của chứng cớ, cần một chuỗi chứng cớ mạnh. nói chung, một chuỗi mạnh chứng cớ như vậy có thể được thiết lập theo các điều kiện sau.

a) đối với các tài liệu giấy: Bản gốc được giữ an toàn và được ghi người đã tìm ra, nơi tìm ra, thời điểm tìm ra và người làm chứng cho phát hiện này. Mọi cuộc điều tra nên đảm bảo rằng các bản gốc không bị giả mạo.

b) đối với thông tin trên phương tiện truyền thông máy tính: Nên có bản sao của mọi phương tiện truyền thông có thể di rời, thông tin trên các đĩa cứng hoặc trong bộ nhớ để đảm bảo tính sẵn sàng. Nhật ký toàn bộ các

hoạt động trong thủ tục sao chép nên được giữ lại và thủ tục nên được làm chứng. Một bản sao của phương tiện truyền thông và nhật ký nên được giữ an toàn.

Khi một sự cố được phát hiện lần đầu, nó có thể hiển nhiên là nó sẽ đưa đến một vụ kiện có thể xảy ra. như vậy, nguy hiểm tồn tại mà chứng cớ cần thiết bị huỷ bỏ bất ngờ trước khi nhận ra tính nghiêm trọng của sự cố. Cần có một luật sư hoặc cảnh sát sớm trong mọi vụ kiện dự tính và thực hiện lời khuyên về chứng cớ được yêu cầu là những điều nên làm theo.

12.2 Soát xét của chính sách an ninh và yêu cầu kỹ thuật

Đối tượng: Để đảm bảo việc tuân thủ của hệ thống với các chính sách và tiêu chuẩn an ninh của tổ chức.
An ninh của các hệ thống thông tin nên được soát xét đều đặn. soát xét như vậy nên được tiến hành ngược lại các chính sách an ninh thích hợp và các bậc kỹ thuật và các hệ thống thông tin nên được kiểm tra để tuân thủ các tiêu chuẩn thực thi an ninh.

12.2.1 Sự tuân theo chính sách an ninh

Các nhà quản lý nên đảm bảo rằng toàn bộ các thủ tục an ninh trong khu vực trách nhiệm của họ phải thực hiện chính xác. Hơn nữa, toàn bộ các khu vực trong tổ chức nên được xem xét việc soát xét đều đặn để đảm bảo tuân thủ với các chính sách và tiêu chuẩn an ninh. Điều này nên gồm:

a) các hệ thống thông tin;

b) các nhà cung cấp hệ thống;

c) các chủ sở hữu của thông tin và các tài sản thông tin;

d) người sử dụng;

e) nhà quản lý.

Các chủ sở hữu của các hệ thống thông tin (xem 5.1) nên hỗ trợ các soát xét tuân thủ đều đặn của hệ thống họ với các chính sách, tiêu chuẩn an ninh thích hợp và mọi yêu cầu an ninh khác. Giám sát hoạt động của việc sử dụng hệ thống được nêu trong 9.7.

12.2.2 Kiểm tra sự tuân theo kỹ thuật

Các hệ thống thông tin nên được kiểm tra đều đặn về việc tuân thủ các tiêu chuẩn an ninh. Việc kiểm tra tuân thủ kỹ thuật gồm kiểm tra về các hệ thống hoạt động để đảm bảo rằng các kiểm soát phần cứng và phần mềm được thực hiện chính xác. Loại kiểm tra việc tuân thủ này yêu cầu chuyên gia về trợ giúp kỹ thuật. Nên thực hiện thủ công (hỗ trợ bằng các công cụ phần mềm thích hợp nếu cần) bởi một kỹ sư hệ thống có kinh nghiệm hoặc bởi một gói phần mềm tự động mà đưa ra một báo cáo kỹ thuật về sự thể hiện tiếp theo bởi một chuyên gia kỹ thuật.

Kiểm tra việc tuân thủ cũng gồm, ví dụ, kiểm tra thủ tục truy cập, có thể tiến hành bởi các chuyên gia độc lập đặc biệt được ký kết vì mục đích này. Điều này hữu ích trong việc phát hiện những khả năng bị tấn công trong hệ thống và để kiểm tra các kiểm soát ngăn ngừa truy cập trái phép do những khả năng bị tấn công này có hiệu quả thế nào. Cảnh báo nên được sử dụng trong trường hợp thành công của một cuộc kiểm tra thủ tục truy

cập có thể dẫn đến một sự tổn hại về an ninh của hệ thống và lợi dụng không cố ý các khả năng dễ bị tấn công khác.

Mọi kiểm tra việc tuân thủ kỹ thuật chỉ nên được tiến hành bởi hoặc dưới sự giám sát của những người có thẩm quyền, thạo việc.

12.3 Sự xem xét kiểm tra hệ thống

Đối tượng: Để tối đa tính hiệu lực của và để giảm thiểu sự can thiệp tới/ từ quy trình kiểm tra hệ thống đó. Nên có các kiểm soát để bảo vệ các hệ thống hoạt động và các công cụ kiểm toán trong suốt các cuộc kiểm toán. Bảo vệ cũng nên được yêu cầu để bảo vệ tính toàn vẹn và ngăn ngừa sự lạm dụng các công cụ kiểm toán.

12.3.1 Các kiểm soát kiểm tra hệ thống

Các yêu cầu và các hoạt động kiểm toán gồm các cuộc kiểm tra các hệ thống hoạt động nên được lập kế hoạch cẩn thận và được thoả thuận để tối thiểu rủi ro gián đoạn các thủ tục kinh doanh. Nên chú ý các điều sau:

a) các yêu cầu kiểm toán nên được thoả thuận với ban quản lý thích hợp;

b) phạm vị các cuộc kiểm tra nên được thoả thuận và kiểm soát;

c) các cuộc kiểm tra nên được giới hạn việc truy cập chỉ đọc với các phần mềm và dữ liệu;

d) việc truy cập khác hơn là chỉ đọc chỉ nên được cho phép đối với các bản sao riêng biệt các tệp hệ thống mà nên được xoá khi kiểm toán hoàn thành;

e) các nguồn IT để tiến hành các kiểm tra nên được định danh rõ ràng và sẵn có;

f) các yêu cầu cho thủ tục xử lý đặc biệt hoặc thêm nên được định danh và được đồng ý;

g) toàn bộ các truy cập nên được giám sát và ghi nhật ký để tạo ra một chuỗi tham chiếu;

h) toàn bộ các thủ tục, yêu cầu và trách nhiệm nên được tài liệu hóa.

12.3.2 Sự bảo vệ của các công cụ kiểm tra hệ tthống

Truy cập tới các công cụ kiểm toán hệ thống, nghĩa là: Phần mềm hoặc các tệp dữ liệu nên được bảo vệ khỏi mọi sự lạm dụng và bị tổn hại có thể xảy ra. Các công cụ này nên được chia tách khỏi hệ thống phát triển và hoạt động và không lưu giữ trong các thư viện băng hoặc các khu vực người sử dụng, trừ khi có một mức bảo vệ thêm thích hợp.