BỘ THÔNG TIN VÀ TRUYỀN THÔNG

VIỆN KHOA HỌC KỸ THUẬT BƯU ĐIỆN

THUYẾT MINH TIÊU CHUẨN

CÔNG NGHỆ THÔNG TIN – KỸ THUẬT AN TOÀN – AN TOÀN MẠNG - PHẦN 3: Các kịch bản kết nối mạng tham chiếu - Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát

Information technology – Security techniques – Network security –

Part 3: Reference networking scenarios – Threats, design techniques and control issues

Hà Nội, 12/2012

Mục lục

Mở đầu

Tên tiêu chuẩn:

Công nghệ thông tin – Kỹ thuật an toàn – An toàn mạng - Phần 3: Các kịch bản kết nối mạng tham chiếu – Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát

Information technology - Security techniques – Network security – Part 3: Reference networking scenarios - Threats, design techniques and control issues

Mục tiêu:

Dự thảo tiêu chuẩn quốc gia về an toàn thông tin, liên quan đến các nguy cơ, các kỹ thuật thiết kế và các vấn đề quản lý đối với các loại kịch bản kết nối mạng. Dự thảo tiêu chuẩn này hỗ trợ quản lý, hướng dẫn thực hiện đảm bảo an toàn thông tin cho các tổ chức, cá nhân sử dụng mạng thông tin.

Nội dung:

+ Các đe dọa liên quan đến các kịch bản mạng tham chiếu

+ Các kỹ thuật liên quan đến các kịch bản mạng tham chiếu

+ Các vấn đề quản lý liên quan đến các kịch bản mạng tham chiếu

1. Tình hình an toàn thông tin

1.1 Tình hình an toàn mạng thông tin ở Việt Nam

Tình trạng vi phạm an toàn thông tin tại Việt Nam ngày một nghiêm trọng. Việt Nam đang là nước bị tin tặc lộng hành khá phổ biến tuy lĩnh vực Internet của Việt Nam chưa được xem là phát triển cao trong khu vực. Có rất nhiều các Website quan trọng liên quan đến tài chính, chứng khoán mặc dù đã được các tổ chức về an toàn cảnh báo nhiều lần nhưng tình trạng an toàn vẫn không được cải thiện. Thực tế đó phản ánh sự lơ là trong công tác an toàn thông tin, gián tiếp gây thiệt hại lớn về kinh tế: hệ thống máy tính bị đánh cắp, dữ liệu bị đánh cắp, gây thiệt hại cho doanh nghiệp và khách hàng. Chuyện mua bán trên mạng bằng thẻ tín dụng đánh cắp, thẻ tín dụng giả đã không còn là chuyện hiếm từ vài năm trở lại đây.

Tình hình an toàn mạng thông tin Việt Nam hiện nay còn rất nhiều thách thức, đặc biệt là nguồn nhân lực có trình độ còn thiếu trầm trọng, và sự đầu tư cho lĩnh vực này mới chỉ nhỏ giọt, ít được sự quan tâm và chưa đúng tầm. Về môi trường pháp lý, sự chưa hoàn thiện và

thiếu đồng bộ dẫn tới tình trạng không có chế tài đủ mạnh để răn đe các Hacker có hành vi phát tán Virus trên diện rộng và tấn công vào những hệ thống máy tính doanh nghiệp để trục lợi. Trong khi đó, khả năng công nghệ bị đánh giá là thiếu và yếu. Một hạ tầng mạng không đủ mạnh sẽ không thể đương đầu với những thách thức và đe dọa an toàn có mức độ tinh vi và chuyên nghiệp ngày càng cao. Bên cạnh đó, mức đầu tư cho công nghệ thông tin tại Việt Nam vẫn còn ở mức thấp. Trung bình các nước trên thế giới có mức đầu tư cho công nghệ là 8-10%. Còn tại Việt Nam, con số này thấp hơn nhiều. Do mức đầu tư hạn hẹp nên rất ít doanh nghiệp, tổ chức có một bộ phận IT riêng, chủ yếu những công việc này chỉ do một số ít người kiêm nhiệm. Từ đó dẫn tới tình trạng an ninh, an toàn thông tin lỏng lẻo, có nhiều kẽ hở để kẻ xấu lợi dụng. Các vụ tấn công hiện nay được tổ chức bài bản hơn, quy mô hơn, kín đáo hơn và mức độ thiệt hại cũng lớn hơn.

Hiện nay tại Việt nam có một số các tổ chức chịu trách nhiệm xử lí sự cố an toàn thông tin như: Trung tâm ứng cứu khẩn cấp máy tính Việt Nam VNCERT (Vietnam Computer Emergency Response Team – VNCERT), Hiệp hội an toàn thông tin Việt Nam VNISA (Vietnam Information Security Association), cơ quan E15- Bộ công an…. Nhiệm vụ chính của các tổ chức trên là hướng dẫn cho tổ chức và cá nhân triển khai biện pháp an toàn thông tin, đồng thời đưa ra những cảnh báo về các mối đe dọa an toàn thông tin trong nước cũng như trên thế giới. Ngoài ra còn có một số công ty như Misoft chuyên cung cấp dịch vụ tư vấn, đào tạo về an toàn thông tin, phân phối sản phẩm (phần cứng và phần mềm) an ninh mạng, triển khai và bảo trợ, hỗ trợ kỹ thuật các hệ thống an toàn an ninh mạng. Nhiệm vụ chính của của các Công ty kinh doanh sản phẩm an toàn mạng là mang đến cho khách hàng các dịch vụ và giải pháp an toàn an ninh hệ thống thông tin tốt nhất nhằm luôn đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng của hệ thống thông tin, phục vụ hiệu quả công việc sản xuất, kinh doanh của khách hàng.

1.2 Tình hình an toàn thông tin trên thế giới

Cùng với sự phát triển nhanh chóng của mạng thông tin các phương thức tấn công mạng ngày càng trở nên tinh vi và nguy hiểm. Hiện nay một số điểm mới trong các mối đe dọa càng trở nên khó tưởng tượng: các sự kiện và tấn công có mưu kế, thay đổi đáng kể trong các bối cảnh đe dọa, các vụ bắt giữ phạm tội có tổ chức, các phương pháp thông minh phù hợp với các thiết bị mới thông minh.

Một số các thay đổi đáng kể là có liên quan đến mạng máy tính ma (botnets) và các mối đe dọa đối với bản tin và thiết bị di động. Xét trên phạm vi chung thì gần đây spam và các mạng

máy tính ma giảm đi đáng kể do chúng hoạt động offline, tuy nhiên các khảo sát cho thấy phần nhiều chúng đang chuẩn bị tiếp tục phát triển theo các cách khác.

Android đã trở thành nền tảng mục tiêu thứ ba trong di động xét trên các khía cạnh lịch sử. Các mối đe dọa phần mềm độc hại đối với nền tảng di động vẫn tiếp tục phát triển trên cả về tri thức lẫn tính năng với tốc độ có thể che lấp cả các phần mềm độc hại trong thế giới PC.

Cuộc chiến chống mạng tội phạm vẫn tiếp tục, trong khia các tấn công đang trong chu kì thay đổi. Các hoạt động tội phạm hiện nay tiếp tục tập trung vào các bối cảnh công nghệ và an toàn thông tin.

Đầu năm 2011, phần mềm độc hại xuất hiện nhiều nhất trong lịch sử. Các phần mềm chống vius giả tăng lên và Trojan đánh cắp mật khẩu vẫn thể hiện mức độ hoạt động ổn định. Đồng thời, phần mềm độc hại Autorun và Koobface, đang được phổ biến toàn cầu, và nằm trong Top 5 trong xu hướng các đe dọa.

Các con số thống kê hàng ngày cho thấy 49% các tấn công là các website phần mềm độc hại. Các số liệu dưới đây cho thấy xu hướng của các đối tượng viết phần mềm độc hại, lừa đảo, mạng tội phạm, đang tiếp tục sử dụng các sự kiện hàng ngày, tin, thể thao, và các sự kiện lễ hội như mồi nhử cho các kế hoạch của chúng. Xu hướng tấn công triển khai từ phía khách hàng tiếp tục giảm và trang đầu cho các tấn công dùng SQL thay đổi liên tục. Các xu hướng mới gần đây là sự tăng nhanh các website lừa đảo và các website phần mềm mã độc nói chung.

2. Khảo sát các tiêu chuẩn về an toàn mạng thông tin

2.1 Các tiêu chuẩn an toàn mạng thông tin trên thế giới.

Trong bối cảnh có sự phát triển như vũ bão của công nghệ thông tin, ngày càng nhiều các tổ chức, đơn vị, doanh nghiệp hoạt động lệ thuộc gần như hoàn toàn vào hệ thống mạng máy tính, máy tính, và cơ sở dữ liệu. Nói cách khác, khi hệ thống công nghệ thông tin hoặc cơ sở dữ liệu gặp các sự cố thì hoạt động của các đơn vị này bị ảnh hưởng nghiêm trọng và thậm chí có thể bị tê liệt hoàn toàn. Một trong các biện pháp phòng ngừa được nhắc đến trong thời gian qua chính là triển khai áp dụng Hệ thống Quản lý An toàn Thông tin (ISMS: Information Security Management System) theo các nguyên tắc của bộ tiêu chuẩn quốc tế ISO.

Bộ Tiêu chuẩn về an toàn thông tin ISO 27xxx – Bộ tiêu chuẩn về hệ thống quản lý an toàn thông tin *(ISO27000 - Information Security Management System)*

Có thể nói rằng, ISO 27xxx là một phần của hệ thống quản lý chung trong tổ chức, được thực hiện dựa trên nguyên tắc tiếp cận các rủi ro trong hoạt động, để thiết lập, áp dụng, thực hiện, theo dõi, xem xét, duy trì và cải tiến đảm bảo an toàn thông tin của tổ chức.

Cho tới nay, việc áp dụng hệ thống quản lý an toàn thông tin phù hợp với ISO 27xxx đã được triển khai rộng khắp ở hầu hết các quốc gia trên thế giới đặc biệt là trong lĩnh vực tài chính ngân hàng. Tại Việt Nam, một số ngân hàng cũng đang triển khai áp dụng hệ thống này và bước đầu đã có được những kết quả nhất định.

Xét về lịch sự hình thành của bộ tiêu chuẩn, ISO 27xxx cũng có nguồn gốc từ Anh quốc. Bắt đầu vào năm 1992, Phòng Thương mại và Công nghiệp Anh (UK Department Trade and Industrial) ban hành ra qui phạm thực hành về hệ thống an toàn thông tin dựa trên các hệ thống đảm bảo an toàn thông tin nội bộ của các công ty dầu khí. Tài liệu này sau đó được Viện tiêu chuẩn hoá Anh chính thức ban hành thành tiêu chuẩn quốc gia với mã hiệu BS 7799-1 vào năm 1995. Năm 2000, tiêu chuẩn này được Tổ chức Tiêu chuẩn hoá Quốc tế (ISO) chính thức chấp nhận và ban hành với mã hiệu ISO/IEC 17799:2000 - tiền thân của bộ tiêu chuẩn ISO 27xxx ngày nay.

Mục đích nhằm thiết lập và duy trì một hệ thống quản lý thông tin, sử dụng phương pháp tiếp cận theo quá trình. Thực hiện theo những nguyên tắc của Tổ chức Phát triển và Hợp tác Kinh tế (OECD).Tiêu chuẩn ISO/IEC 27xxx là một phần của hệ thống quản lý chung của các tổ chức, doanh nghiệp do vậy có thể xây dựng độc lập hoặc kết hợp với các hệ thống quản lý khác như ISO 9000, ISO 14000...

Lợi ích của việc áp dụng:

- Chứng tỏ sự cam kết đảm bảo sự an toàn về thông tin ở mọi mức độ.
- Đảm bảo tính sẵn sàng và tin cậy của phần cứng và các cơ sở dữ liệu.
- Bảo mật thông tin, tạo niềm tin cho đối tác, khách hàng.
- Giảm giá thành và các chi phí bảo hiểm.
- Nâng cao nhận thức và trách nhiệm của nhân viên về an ninh thông tin.

Họ các tiêu chuẩn ISMS bao gồm các tiêu chuẩn:

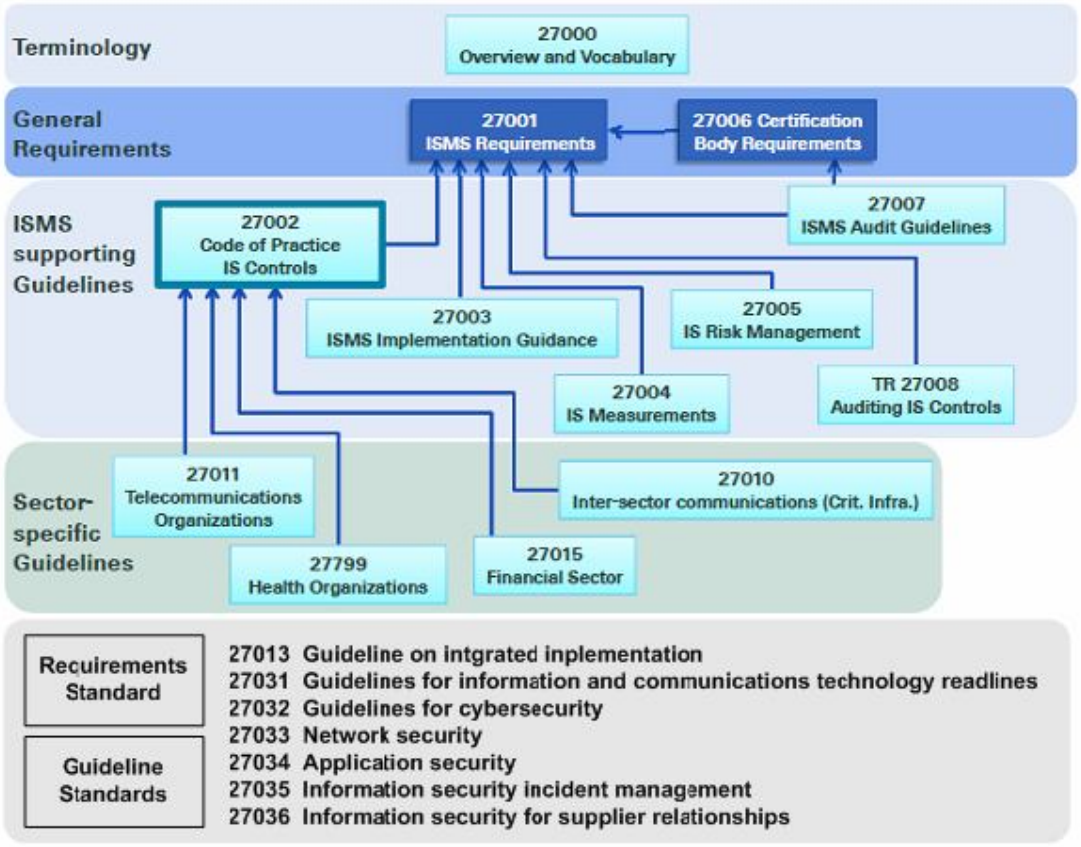
a)Xác định các yêu cầu cho ISMS và cho các yêu cầu chứng nhận các hệ thống như vậy;

b) Cung cấp hỗ trợ trực tiếp, hướng dẫn chi tiết và/hoặc chuyển đổi cho toàn bộ các quá trình và yêu cầu Kế hoạch – Thực hiện – Kiểm tra – Hành động (PDCA);

c) Chỉ ra hướng dẫn cụ thể từng bộ phận cho ISMS; và

d) Đưa ra tính phù hợp đánh giá cho ISMS.

Tổng quan các tiêu chuẩn trọng họ 27xxx được đưa ra trong Hình 1 dưới đây.



Hình 1 – Tổng quan các tiêu chuẩn họ 27xxx.

Theo con số thống kê chưa đầy đủ thì đến năm 2010 số lượng các tổ chức đã áp dụng ISMS và đã được chứng nhận trên toàn thế giới là 2063 trong đó đứng đầu là Nhật Bản với số chứng chỉ được cấp ra là 1190 sau đó là Anh 219, Đài loan 69...

Các lĩnh vực áp dụng đối với ISMS cũng chiếm các tỉ lệ khác nhau. Ví dụ lĩnh vực viễn thông được áp dụng nhiều nhất với 27% tổng số lượng chứng chỉ cấp ra, lĩnh vực tài chính ngân hàng chiếm 20%, lĩnh vực công nghệ thông tin chiếm 15%,..

Hy vọng trong thời gian tới tại Việt Nam sẽ có thêm nhiều hơn nữa các tổ chức áp dụng ISMS để có thể giảm thiểu các rủi ro liên quan tới an toàn thông tin, đảm bảo cho sự phát triển bền vững.

2.2 Các tiêu chuẩn quản lý an toàn mạng thông tin tại Việt nam

Đảm bảo an toàn thông tin là nhu cầu thiết thực để thúc đẩy và phát triển dịch vụ, công nghệ thông tin và truyền thông. Tiêu chuẩn về an toàn thông tin trong lĩnh vực CNTT hãy còn thiếu nhiều. Tổ chức ISO có trên 100 chuẩn về an toàn thông tin, trong khi TCVN hãy còn ban hành khá ít. Thiếu các tiêu chuẩn dẫn đến việc người sử dụng, tổ chức không có cơ sở để thực hiện các biện pháp an toàn cho mình. Do đó, việc xây dựng các tiêu chuẩn về an toàn thông tin nói chung, và về quản lý an toàn mạng nói riêng, là cần thiết.

3. Tiêu chuẩn về an toàn mạng thông tin ISO/IEC 27033

Bộ tiêu chuẩn ISO/IEC 27033 được biên soạn bởi tổ chức ISO/IEC JTC1, Công nghệ thông tin – nhóm SC 27, Kỹ thuật an toàn IT.

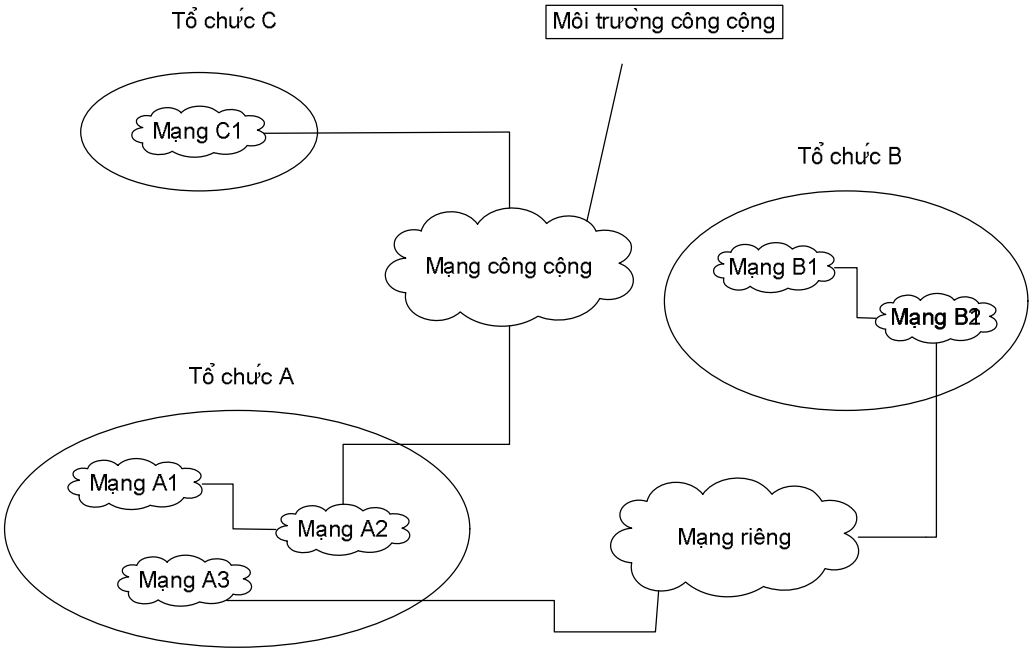
Bộ tiêu chuẩn này kết thúc và thay thế cho ISO/IEC 18028.

Hiện nay Phần 1 và Phần 3 đã được ban hành, các phần còn lại đang trong quá trình biên soạn

3.1 Giới thiệu

Ngày nay, phần lớn các tổ chức thương mại và chính phủ đều có các hệ thống thông tin kết nối bằng các mạng của họ, với các kết nối mạng có thể là một trong những loại sau:

- Trong tổ chức
- Giữa các tổ chức
- Giữa tổ chức và mạng chung



Hình 2 – Các loại kết nối mạng.

Hơn nữa, với sự phát triển rất nhanh của công nghệ mạng (đặc biệt là Internet), đưa ra các cơ hội kinh doanh quan trọng, các tổ chức tăng thiết lập kinh doanh điện tử trên qui mô rộng và cung cấp các dịch vụ chung on-line. Các cơ hội bao gồm cung cấp các truyền thông dữ liệu chi phí thấp cung cấp bởi ISP. Điều này có thể là sử dụng các điểm gắn kết chi phí thấp tại từng điểm cuối của mạch tới thương mại điện tử trên qui mô toàn bộ và các hệ thống phan phối dịch vụ, sử dụng các ứng dụng và dịch vụ dựa trên web. Thêm nữa, công nghệ mới (bao gồm tích hợ dữ liệu, thoại và video) làm tăng các cơ hội cho làm việc từ xa (được biết như teleworking hay telecommuting) cho phép người cá nhận hoạt động xa cơ sở làm việc trong một khoảng thời gian. Họ có khả năng duy trì kết nối thông qua sử dụng các phương tiện từ xa để truy nhập mạng của tổ chức và cộng đồng và các thông tin và dịch vụ hỗ trợ nghiệp vụ liên quan.

Tuy nhiên, trong khi các môi trường đem đến các lợi ích kinh doanh đáng kể, xuất hiện các rủi ro an toàn mới cần quản lý. Với các tổ chức dựa chủ yếu vào sử dụng thông tin và các mạng thích hợp để thực hiện nghiệp vụ của họ, việc mất tính cần mật, tính toàn vẹn, tính sẵn sàng của thông tin và dịch vụ có thể gây ra các tác động bất lợi đáng kể tới hoạt động kinh doanh. Do đó, có các yêu cầu chủ yếu để bảo vệ mạng và các hệ thống thông tin liên quan và

thông tin. Nói một cách khác, *triển khai và duy trì an toàn mạng đầy đủ là tối quan trọng cho sự thành công của bất cứ hoạt động kinh doanh nào của tổ chức.*

Trong bối cảnh này, các nhà công nghiệp công nghệ viễn thông và thông tin đang tìm kiếm các giải pháp an toàn toàn diện và hiệu quả, nhằm bảo vệ mạng chống lại các tấn công và các hành động không đúng, và thỏa mãn các yêu cầu nghiệp vụ cho tính bí mật, tính toàn vẹn, tính sẵn sàng của thông tin và dịch vụ. An toàn mạng cũng rất thiết yếu trong duy trì tính chính xác của cước, hay sử dụng thông tin phù hợp. Khả năng an toàn trong các sản phẩm là quan trọng cho an toàn toàn bộ mạng (bao gồm cả ứng dụng và dịch vụ). Tuy nhiên, càng nhiều sản phẩm được kết hợp để cung cấp các giải pháp tổng thể thì khả năng tương tác sẽ xác định sự thành công của giải pháp. Tính an toàn phải không chỉ cho một sản phẩm hay dịch vụ, mà phải được phát triển sao cho thúc đẩy tréo cho nhau hay khả năng an toàn trên giải pháp an toàn toàn thể.

Mục tiêu của ISO/IEC 27033 là cung cấp hướng dẫn chi tiết trên các khía cạnh của an toàn về quản lý, vận hành và sử dụng mạng hệ thống thông tin, và các kết nối giữa chúng. Các cá nhân trong tổ chức có trách nhiệm an toàn thông tin nói chung, an toàn mạng nói riêng, phải có khả năng thông hiểu các tư liệu trong Tiêu chuẩn này để thỏa mãn các yêu cầu cụ thể của họ. Các mục tiêu của Tiêu chuẩn là

- ISO/IEC 27033-1, *Tổng quan và khái niệm*, xác định và mô tả các khái niệm liên quan với, và cung cấp hướng dẫn quản lý cho, an toàn mạng. Nó bao gồm cung cấp tổng quan của an toàn mạng và các định nghĩa liên quan, hướng dẫn về xác định và phân tích các rủi ro an toàn mạng như thế nào và sau đó xác định các yêu cầu an toàn mạng. Nó cũng đưa ra làm thế nào để đạt được kiến trúc an toàn kỹ thuật chất lượng tốt, và các khía cạnh rủi ro, thiết kế, và kiểm soát liên quan đến các kịch bản mạng và lĩnh vực ‘công nghệ’ mạng điển hình (chúng được xử lý chi tiết trong các phần sau của TC).

- ISO/IEC 27033-2, *Hướng dẫn thiết kế và triển khai an toàn mạng*, xác định tổ chức phải đạt được các kiến trúc, thiết kế và triển khai an toàn kỹ thuật mạng chất lượng tôt như thế nào, chúng sẽ đảm bảo an toàn mạng thích hợp với các môi trường nghiệp vụ của họ, sử dụng tiếp cận nhất quán để lập kế hoạch, thiết kế và triển khai mạng an toàn, nếu liên quan, được trợ giúp từ sử dụng các mô hình/khung (trong bối cảnh này, mô hình/ khung được sử dụng phác thảo diễn tả hay mô tả chỉ ra cấu trúc và mức làm việc

cao của loại kiến trúc/thiết kế an toàn kỹ thuật), và liên quan đến tất cả cá nhân tham gia qui hoạch, thiết kế và triển khai các khía cạnh kiến trúc của an toàn mạng (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

- ISO/IEC 27033-3, *Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát cho các kịch bản mạng khác nhau*, xác định các rủi ro cụ thể, các kỹ thuật thiết kế và các vấn đề kiểm soát liên quan đến các kịch bản mạng điển hình. Nó liên quan tới tất cả cá nhân tham gia vào qui hoạch, thiết kế và triển khai các khía cạnh kiến trúc của an toàn mạng (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

- ISO/IEC 27033-4, *Rủi ro, kỹ thuật thiết kế và các vấn đề kiểm soát cho an toàn truyền thông giữa các mạng sử dụng cổng an toàn*, xác định các rủi ro cụ thể, các kỹ thuật thiết kế và các vấn đề kiểm soát cho an toàn thông tin truyền giữa các mạng sử dụng cổng an toàn. Nó sẽ liên quan đến tất cả cá nhân tham gia vào qui hoạch chi tiết, thiết kế và triển khai các cổng an toàn (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

- ISO/IEC 27033-5, *Rủi ro, kỹ thuật thiết kế và các vấn đề kiểm soát cho an toàn mạng riêng ảo*, xác định các rủi ro cụ thể, các kỹ thuật thiết kế và các vấn đề kiểm soát cho an toàn kết nối được thiết lập sử dụng mạng riêng ảo (VPN). Nó sẽ liên quan đến tất cả cá nhân tham gia vào qui hoạch chi tiết, thiết kế và an toàn VPN (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

- ISO/IEC 27033-6, *Hội tụ IP*, xác định các rủi ro cụ thể, các kỹ thuật thiết kế và các vấn đề kiểm soát cho mạng hội tụ IP, tức là các mạng hội tụ thoại, dữ liệu và video. Nó sẽ liên quan đến tất cả cá nhân tham gia vào qui hoạch chi tiết, thiết kế và triển khai an toàn cho mạng hội tụ IP (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

- ISO/IEC 27033-7, *Mạng không dây*, xác định các rủi ro cụ thể, các kỹ thuật thiết kế và các vấn đề kiểm soát cho an toàn các mạng không dây và vô tuyến. Nó sẽ liên quan đến tất cả cá nhân tham gia vào qui hoạch chi tiết, thiết kế và triển khai an toàn cho mạng không dây và vô tuyến (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

Nhấn mạnh rằng ISO/IEC 27033 cung cấp hướng dẫn triển khai chi tiết hơn cho các kiểm soát an toàn mạng được mô tả tại mức tiêu chuẩn cơ bản ISO/IEC 27002.

Nếu có các phần khác trong tương lai, chúng sẽ liên quan đến tất cả cá nhân tham gia vào qui hoạch chi tiết, thiết kế và triển khai các khía cạnh mạng bao hàm bởi các phần này (ví dụ như người kiến trúc mạng và người thiết kế, người quản lý mạng, và các nhân viên an toàn mạng).

Phải lưu ý rằng Tiêu chuẩn này không phải là tham chiếu hay tài liệu quy phạm cho các yêu cầu an toàn pháp lý hay qui tắc. Mặc dù nhấn mạnh tầm quan trọng của các ảnh hưởng này, nó không thể công bố chúng một cách đặc biệt, vì chúng phụ thuộc vào các nước, loại nghiệp vụ, …

Tiêu chuẩn ISO/IEC 27033 hướng dẫn tham chiếu được áp dụng cho mạng hiện thời và/hoặc mạng được lập kế hoạch.

So với bộ tiêu chuẩn ISO/IEC 18028, Bộ tiêu chuẩn ISO/IEC 27033 được xây dựng lại và bổ sung các nội dung, cập nhật bám sát các thay đổi của: các rủi ro, các công nghệ triển khai áp dụng trên mạng, các kịch bản mạng. Do đó, có sự thay đổi trong tất cả các Phần của Tiêu chuẩn.

Bộ tiêu chuẩn ISO/IEC 27033 được cấu trúc lại theo quá trình lập kế hoạch và quản lý an toàn mạng. Và được biên soạn cấu trúc mở cho các chuyên đề công nghệ khác nhau. Do đó, có khả năng bổ sung các Phần khác ngoài 7 phần đã dự định.

3.2 Cấu trúc tiêu chuẩn ISO/IEC 27033

Cấu trúc của bộ tiêu chuẩn ISO/IEC được biểu diễn trong dạng biểu đồ, hay “chỉ dẫn”, trên Hình 3 ở dưới.

Lưu ý rằng trong Hình 3 các đường liền chỉ thị bản chất phân cấp của các phần của Tiêu chuẩn ISO/IEC 27033. Các đường đứt quãng chỉ thị các quá trình tiếp theo được mô tả trong (a) Phần 1 – Phần 3, 4, 5 và 7 có thể được tham khảo cho thông tin về các rủi ro an toàn, và (b) Phần 2 – Phần 3, 4, 5, 6, và 7 có thể được tham khảo cho thông tin về các kỹ thuật thiết kế và các vấn đề kiểm soát. Hơn nữa, có các tham chiếu trong Phần 3 đối với các khía cạnh bao trùm trong Phần 4, 5, 6 và 7 để tránh lặp lại (tức là khi sử dụng Phần 3 có thể cần tham khảo Phần 4, 5, 6 và 7).

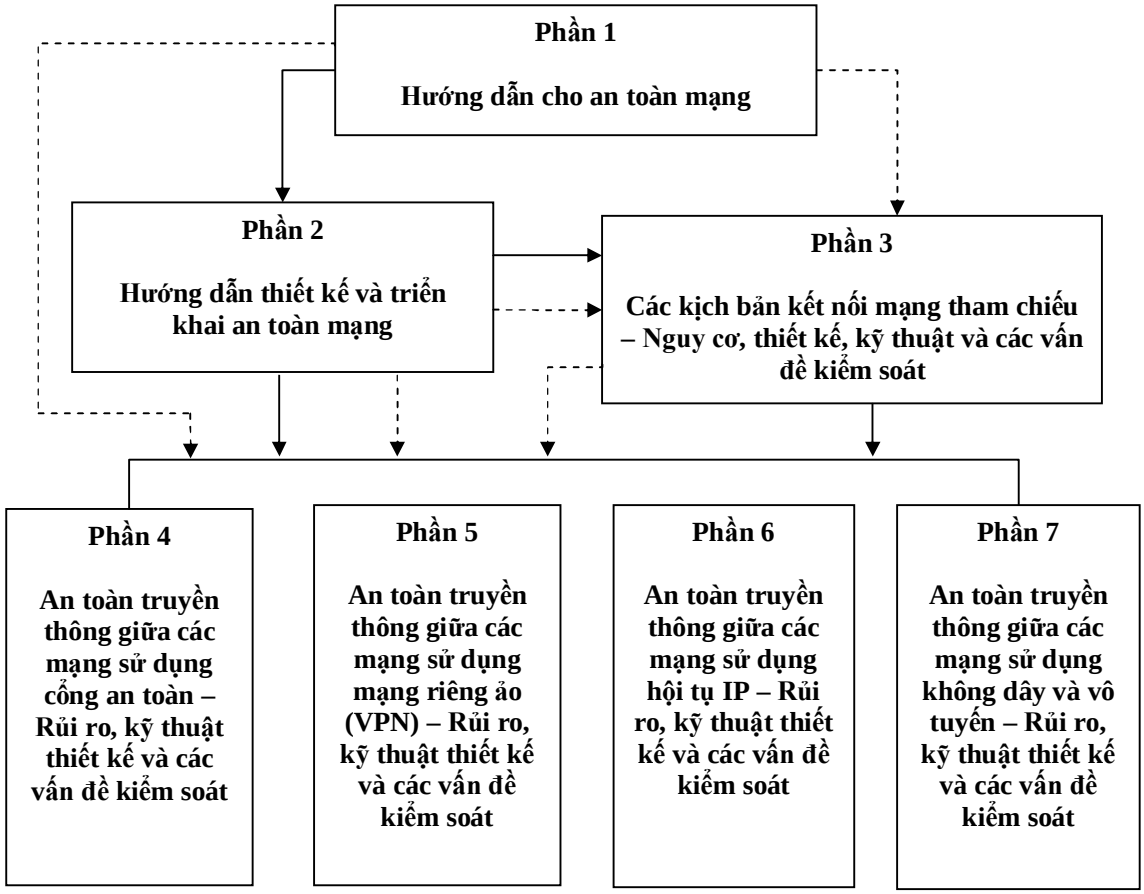
Do đó, đối với bất kì tổ chức nào bắt đầu từ đầu, hay thực hiện soát xét chủ yếu các mạng đang tồn tại, trước hết phải sử dụng nội dung Phần 1 và sau đó Phần 2, nhưng tham khảo khi

cần thiết các thông tin thích hợp về các rủi ro an toàn, các kỹ thuật thiết kế và các vấn đề kiểm soát trong Phần 3 đến 7.

Ví dụ, một tổ chức xem xét triển khai môi trường mạng mới bao gồm sử dụng hội tụ IP, các cổng an toàn và một số sử dụng công nghệ không dây, cũng như sử dụng lưu trữ web và Internet (như e-mail và truy cập hoạt động online).

Khi sử dụng các quá trình mô tả trong Phần 1 tổ chức có thể tham khảo thông tin liên quan đến rủi ro từ các phần liên quan khác của ISO/IEC 27033, tức là các phần xác định rủi ro an toàn cụ thể (cũng như các kỹ thuật thiết kế và các vấn đề kiểm soát) liên quan đến hội tụ IP, các cổng an toàn và sử dụng công nghệ không dây, cũng như sử dụng lưu trữ web và Internet (như e-mail và truy cập online).

Khi sử dụng Phần 3 để xác định kiến trúc an toàn kỹ thuật mạng yêu cầu, tổ chức có thể tham khảo thông tin về các kỹ thuật thiết kế và các vấn đề kiểm soát từ các phần liên quan khác của TCVN xxxx, tức là các phần xác định các thuật thiết kế và các vấn đề kiểm soát cụ thể (cũng như các rủi ro an toàn) – liên quan đến đến hội tụ IP, các cổng an toàn và sử dụng công nghệ không dây, cũng như sử dụng lưu trữ web và Internet (như e-mail và truy cập online).

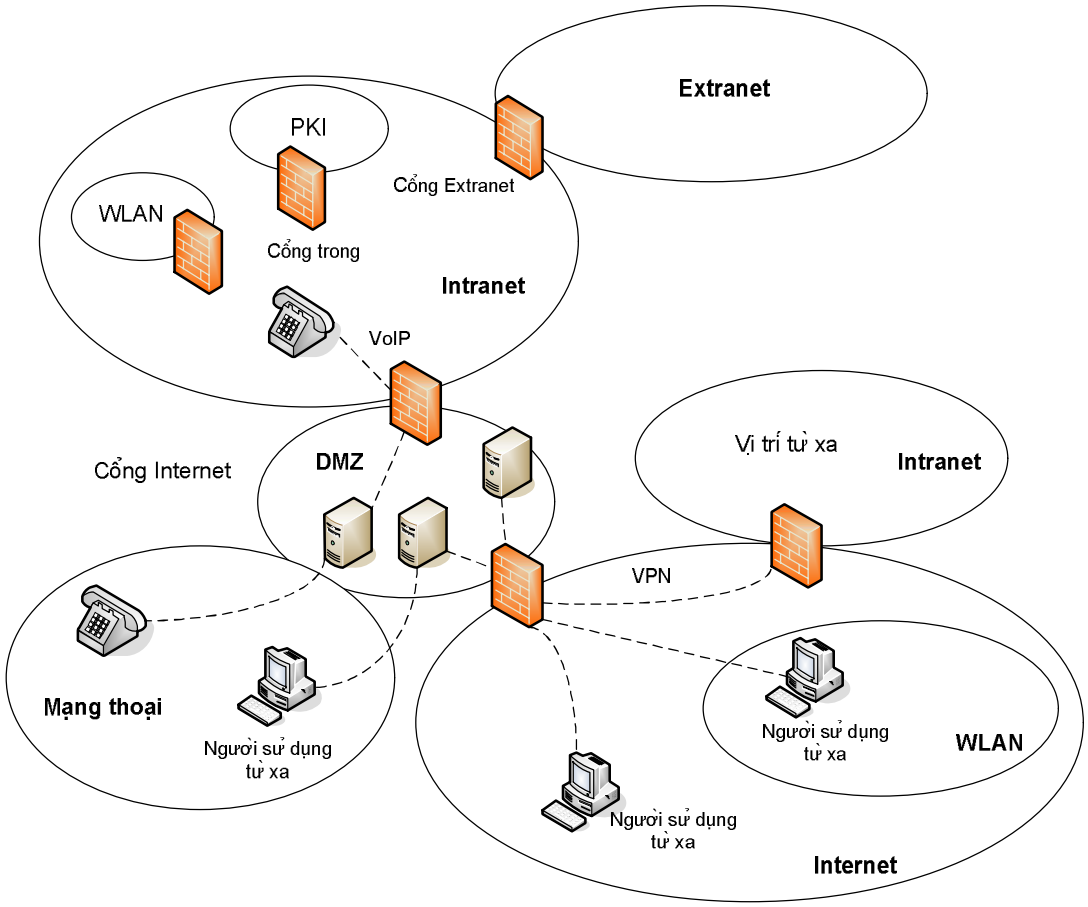


Hình 3 - Chỉ dẫn bộ tiêu chuẩn ISO/IEC 27033

3.3 Tổng quan

3.3.1 Kiến thức cơ sở

Một ví dụ môi trường mạng, nó có thể thấy trong rất nhiều tổ chức hiện nay, được đưa ra trong Hình 4 dưới đây.



Hình 4 - Môi trường mạng ví dụ.

Mạng Intranet xác định một mạng mà tổ chức dựa vào và duy trì từ bên trong. Thông thường, chỉ các cá nhân hoạt động cho tổ chức mới được truy cập vật lý trực tiếp vào mạng, và do mạng được đặt trong phạm vi của tổ chức làm chủ nên mức độ bảo vệ vật lý có thể dễ dàng đạt được. Trong phần lớn các trường hợp, mạng Intranet không đồng nhất trên công nghệ sử dụng và các yêu cầu an toàn; có thể có những hạ tầng đòi hỏi mức bảo vệ cao hơn so với mức mạng Intranet đưa ra. Các hạ tầng như vậy, ví dụ như các phần quan trọng của môi trường PKI, có thể được vận hành trong một đoạn xác định của Intranet. Mặt khác, các công nghệ hiện thời (như các hạ tầng WLAN) có thể yêu cầu một vài cô lập và xác thực vì chúng phát sinh thêm các rủi ro. Trong cả hai trường hợp, các cổng an toàn bên trong có thể được sử dụng để triển khai việc phân chia này.

Các yêu cầu kinh doanh của phần lớn các tổ chức ngày nay cần truyền thông và trao đổi thông tin với các đối tác bên ngoài và tổ chức khác. Thông thường, các đối tác kinh doanh quan trọng nhất được kết nối bằng cách trực tiếp mở rộng kết nối mạng Intranet của tổ chức với mạng của tổ chức đối tác; khái niệm Extranet được thống nhất dùng cho các mở rộng như vậy. Vì độ tin cậy trong tổ chức đối tác được kết nối trong phần lớn các trường hợp thường thấp hơn so với trong cùng tổ chức, các cổng an toàn extranet được sử dụng để bù đắp các rủi ro do các kết nối này phát sinh.

Mạng công cộng, mà mạng Internet là ví dụ chung nhất, ngày nay được sử dụng rộng rãi nhằm cung cấp các phương tiện truyền thông và trao đổi dữ liệu tối ưu về chi phí với đối tác, khách hàng, và công chúng nói chung, và cung cấp các dạng mở rộng khác của Intranet. Do mức độ tin cậy thấp trong mạng công cộng, đặc biệt là Internet, cần phải có các cổng an toàn tinh vi nhằm hỗ trợ quản lý các rủi ro liên quan. Các cổng an toàn này bao gồm các thành phần đặc trưng đáp ứng các yêu cầu cho các dạng khác nhau của mở rộng mạng Intranet cũng như các kết nối của đối tác và khách hàng.

Người sử dụng từ xa có thể được kết nối thông qua công nghệ VPN, và chúng có thể sử dụng các phương tiện kết nối không dây như các điểm WLAN công cộng để truy cập Internet. Một lựa chọn khác, người sử dụng từ xa có thể sử dụng mạng điện thoại để thiết lập kết nối dial-up trực tiếp đến máy chủ truy cập từ xa, thường được đặt bên trong môi trường DMZ của tường lửa Internet.

Khi một tổ chức quyết định sử dụng công nghệ VoIP để triển khai mạng điện thoại nội bộ, thì các cổng an toàn thích hợp với mạng điện thoại thường cũng phải hiện diện.

Các cơ hội kinh doanh đạt được bởi các môi trường mới phải được cân bằng với các rủi ro tạo ra từ các công nghệ mới hơn. Ví dụ, mạng Internet có một số lượng lớn các đặc tính kỹ thuật mà có thể gây ra nguyên nhân trên quan điểm về an toàn, vì từ nguồn gốc nó được thiết kế ưu tiên tính mềm dẻo hơn là tính an toàn - và nhiều giao thức được sử dụng rộng rãi về bản chất không an toàn. Có một số lượng lớn người sử dụng trong môi trường toàn cầu có khả năng, hiểu biết và khuynh hướng truy cập vào cơ cấu hạ tầng và các giao thức, và từ đó tạo ra những sự cố về an toàn, trải khắp từ những truy cập trái phép tới phá hoại và từ chối các dịch vụ trên qui mô rộng.

3.3.2 Lập kế hoạch và quản lý an toàn mạng

Khi xem xét các kết nối mạng, tất cả cá nhân trong tổ chức có trách nhiệm liên quan đến các kết nối phải hiểu rõ yêu cầu và các lợi ích kinh doanh, các rủi ro an toàn liên quan, và các kỹ thuật khía cạnh/ thiết kế kiến trúc an toàn kỹ thuật và các lĩnh vực kiểm soát an toàn liên quan. Các yêu cầu và lợi ích kinh doanh sẽ ảnh hưởng đến nhiều quyết định và hành động trong quá trình xem xét các kết nối mạng, xác định các các kỹ thuật khía cạnh/ thiết kế kiến trúc an toàn kỹ thuật và các lĩnh vực kiểm soát an toàn tiềm năng và từ đó lựa chọn, thiết kế, triển khai và duy trì mạng an toàn.

Toàn bộ quá trình đạt được và duy trì an toàn mạng yêu cầu có thể tóm tắt như sau:

a)Xác định phạm vi/ ngữ cảnh và sau đó đánh giá các rủi ro an toàn:

1)Thu thập thông tin trong môi trường mạng hiện thời và/hoặc được lập kế hoạch;

i)Soát xét chính sách an toàn thông tin doanh nghiệp để công bố về các rủi ro, luôn được xem xét là cao, liên quan đến mạng, và về các kiểm soát an toàn mạng cần phải được triển khai không phụ thuộc vào các rủi ro được đánh giá.

CHÚ THÍCH: Chính sách này cũng phải bao gồm vị trí của tổ chức (1) các yêu cầu an toàn có tính qui định và lập pháp liên quan đến kết nối mạng được xác định bởi các qui định liên quan và cơ quan lập pháp (bao gồm các cơ quan chính phủ), và (2) tính nhạy cảm của dữ liệu được lưu giữ hoặc truyền tải trên mạng.

ii)Thu thập và xem xét thông tin trên mạng hiện thời và/hoặc mạng đã được lập kế hoạch – kiến trúc, ứng dụng, dịch vụ, các loại kết nối và các đặc tính khác – điều này sẽ dẫn đến việc nhận dạng và đánh giá các rủi ro, và xác định cái gì có khả năng trong phạm vi của kiến trúc/ thiết kế an toàn kỹ thuật,

iii)Thu thập thông tin có khả năng đánh giá các ảnh hưởng kinh doanh có hại, các mối đe dọa và các điểm yếu tiềm năng (bao gồm đánh giá hoạt động kinh doanh của thông tin truyền qua các kết nối mạng, bất kì thông tin nào khác có khả năng bị truy cập bằng các cách bất hợp pháp thông qua các kết nối này, và của các dịch vụ được cung cấp),

2)Xác định và đánh giá các rủi ro an toàn mạng, và các lĩnh vực kiểm soát tiềm năng thích hợp

i)Thực hiện đánh giá rủi ro an toàn mạng và soát xét quản lý bao gồm sử dụng thông tin an toàn liên quan tới các kịch bản mạng yêu cầu và các chuyên đề "công nghệ" (xem các phần ISO/IEC 27033-3 đến ISO/IEC 27033-7) – xác định yêu cầu an toàn. (Lưu ý rằng điều này bao gồm (1) đánh giá rủi ro liên quan đến các vi phạm tiềm năng các qui định và luật pháp tương ứng liên quan đến kết nối mạng được xác định bởi các qui định liên quan hay cơ quan lập pháp (bao gồm các cơ quan chính phủ), và (2) sử dụng các tác động kinh doanh có hại tiềm năng được đồng ý, khẳng định tính nhạy cảm/ phân loại dữ liệu được lưu giữ hoặc truyền tải trên mạng),

b)Xác định các kiểm soát an toàn hỗ trợ - không kỹ thuật và kỹ thuật không chỉ áp dụng cho mạng,

c)Soát xét các tùy chọn kiến trúc/ thiết kế an toàn kỹ thuật, xem xét các kịch bản mạng và các chuyên đề "công nghệ", và lựa chọn và lập tài liệu liến trúc/ thiết kế an toàn kỹ thuật và các kiểm soát an toàn liên quan được ưu tiên (xem các phần ISO/IEC 27033-2 đến ISO/IEC 27033-7). Lưu ý rằng điều này bao gồm các kiểm soát yêu cầu tuân thủ theo các qui định và luật pháp tương ứng liên quan đến các kết nối mạng như xác định bởi các qui định liên quan hay cơ quan lập pháp (bao gồm các cơ quan chính phủ),

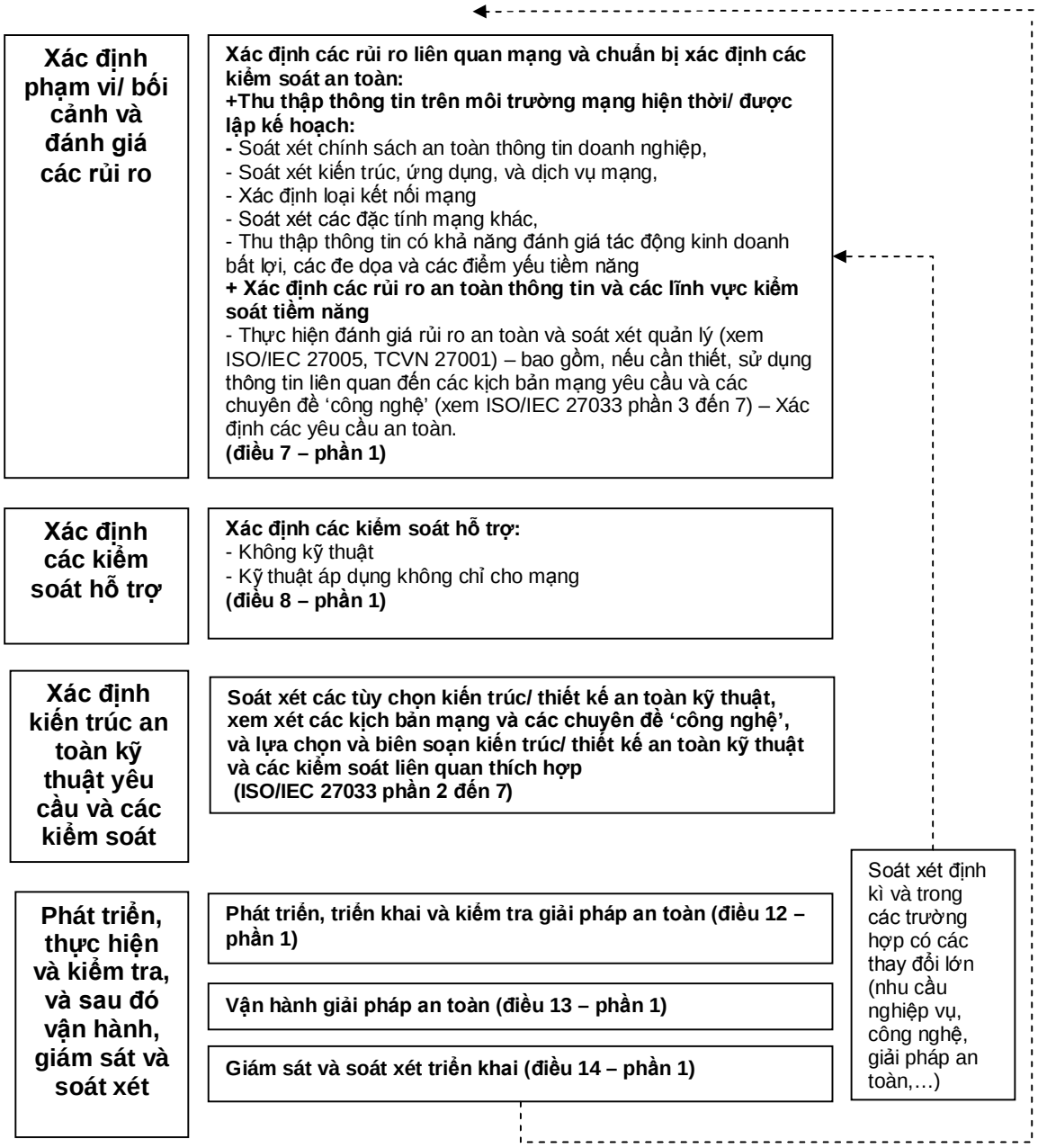
d)Phát triển và kiểm tra giải pháp an toàn,

e)Triển khai và vận hành kiểm soát an toàn,

f)Giám sát và soát xét triển khai. Lưu ý rằng điều này bao gồm giám sát và soát xét các kiểm soát yêu cầu để tuân thủ theo các qui định và luật pháp tương ứng liên quan đến các kết nối mạng như xác định bởi các qui định liên quan hay cơ quan lập pháp (bao gồm các cơ quan chính phủ),

- Soát xét phải được tiến hành định kì, và trong trường hợp thay đổi lớn (về các yêu cầu kinh doanh, công nghệ, các giải pháp an toàn, …), và khi cần thiết các kết quả từ các giai đoạn trước được phác thảo ở trên phải được xem lại và cập nhật.

Tổng quan của quá trình lập kế hoạch và quản lý an toàn mạng được đưa ra dưới dạng biểu đồ trong Hình 5 bên dưới.



CHÚ THÍCH: Xem TCVN 27001, TCVN 27002, ISO/IEC 27003, ISO/IEC 24004 và ISO/IEC 27005.

Hình 5 - Quá trình lập kế hoạch và quản lý an toàn mạng

Cần nhấn mạnh rằng trong toàn bộ quá trình này tham chiếu phải được thực hiện thích hợp với TCVN 27001, TCVN 27002, và ISO/IEC 27005, bao gồm tư vấn chung về nhận dạng các kiểm soát an toàn. Tiêu chuẩn ISO/IEC 27033-1 là sự bổ sung cho các tiêu chuẩn này, cung cấp giới thiệu làm thế nào để xác định các kiểm soát an toàn mạng thích hợp và các phần ISO/IEC 27033-2 đến ISO/IEC 27033-7.

4. Tiêu chuẩn ISO/IEC 27033-3 về các kịch bản tham chiếu mạng – nguy cơ, các kỹ thuật thiết kế và các vấn đề kiểm soát

4.1 Phạm vi áp dụng

Phần này của tiêu chuẩn ISO/IEC 27033 mô tả các nguy cơ, các kỹ thuật thiết kế và các vấn đề liên quan với các kịch bản mạng tham chiếu. Đối với mỗi kịch bản, tiêu chuẩn cung cấp hướng dẫn chi tiết về các nguy cơ và các kỹ thuật và kiểm soát an toàn yêu cầu để giảm thiểu các rủi ro liên quan. Nếu có liên quan, tiêu chuẩn này bao gồm các tham chiếu đến các phần 4-6 của ISO/IEC 27033 để tránh trùng lặp nội dung của các tiêu chuẩn này.

Thông tin trong phần này của tiêu chuẩn ISO/IEC 27033 được sử dụng khi xem xét các tùy chọn kiến trúc/ thiết kế an toàn kỹ thuật và khi lựa chọn và soạn thảo kiến trúc/ thiết kế an toàn kỹ thuật ưu tiên và các kiểm soát an toàn liên quan, tương thích với ISO/IEC 27033-2. Thông tin đặc thù được lựa chọn (cùng với thông tin được lựa chọn từ các phần 4-7 của ISO/IEC 27033) sẽ phụ thuộc vào các đặc tính của môi trường mạng được xem xét, tức là kịch bản mạng đặc thù và chuyên đề "công nghệ" liên quan.

Về tổng thể, phần này của ISO/IEC 27033 sẽ hỗ trợ đáng kể việc xác định và thực hiện toàn diện an toàn cho bất cứ môi trường mạng của tổ chức nào.

4.2 Tổng quan tiêu chuẩn ISO/IEC 27033-3

Hướng dẫn đưa ra trong phần này của ISO/IEC 27033 cho từng kịch bản mạng tham chiếu xác định được dựa trên các cách tiếp cận sau:

- Xem xét thông tin cơ bản và phạm vi của kịch bản.
- Mô tả các nguy cơ liên quan đến kịch bản.
- Thực hiện phân tích rủi ro trên các điểm yếu phát hiện ra.
- Phân tích ảnh hưởng đến kinh doanh của các điểm yếu chỉ ra.
- Xác định các khuyến nghị triển khai để bảo đảm an toàn mạng.

Để giải quyết an toàn cho bất cứ mạng nào, phương pháp tiếp cận một cách hệ thống và cung cấp đánh giá toàn trình được xem xét. Độ phức tạp của phân tích như vậy là hàm số của bản chất và kích cỡ của mạng trong phạm vi đề cập. Tuy nhiên, phương pháp luận thống nhất là rất quan trọng để quản lý an toàn, đặc biệt do bản chất luôn phát triển của công nghệ.

Xem xét đầu tiên trong đánh giá an toàn là xác định các tài sản yêu cầu bảo vệ. Chúng có thể được phân loại rộng thành các tài sản hạ tầng, dịch vụ và ứng dụng. Tuy nhiên, doanh nghiệp có thể chọn để xác định các thể loại của riêng mình, nhưng việc phân định rõ là quan trọng vì rằng để lộ các nguy cơ và các cuộc tấn công là duy nhất cho từng dạng hay loại tài sản. Ví dụ, nếu bộ định tuyến được phân loại vào tài sản hạ tầng, và thoại trên IP như một dịch vụ của người sử dụng cuối, thì tấn công từ chối dịch vụ (DoS) yêu cầu xem xét khác nhau trong mỗi trường hợp. Đặc biệt, bộ định tuyến yêu cầu bảo vệ chống tràn ngập các gói tin giả trên cổng vật lý của bộ định tuyến có thể ngăn chặn hay làm cản trở truyền lưu lượng hợp pháp. Tương tự, dịch vụ VoIP yêu cầu bảo vệ thông tin tài khoản/ dịch vụ của thuê bao khỏi bị xóa hay bị phá hỏng làm cho người sử dụng hợp pháp không được bảo vệ trong quá trình truy cập dịch vụ.

An toàn mạng cũng kéo theo phải bảo vệ các hoạt động khác nhau hỗ trợ mạng, như các hoạt động quản lý; các bản tin điều khiển/ báo hiệu; và dữ liệu người sử dụng cuối (sự hiện diện cố định hay đang đi xa). Ví dụ, quản lý GUI có thể là chủ thể làm lộ thông tin như là hệ quả của truy cập bất hợp pháp (dễ dàng đoán ID quản trị và mật khẩu). Tự bản thân lưu lượng quản lý cũng là chủ thể phá hoại do các lệnh OA&M giả mạo với các địa chỉ IP lừa gạt của hệ thống điều hành, hoặc làm lộ thông tin do bị bắt giữ lưu lượng, hoặc bị ngắt do tấn công tràn ngập gói tin.

Phương pháp tiếp cận xác định các tài sản và hoạt động cho phép xem xét theo mô đun và có hệ thống các nguy cơ. Mỗi kịch bản mạng tham chiếu được khảo sát đối với bộ đã biết các nguy cơ để chắc chắn nguy cơ nào có khả năng ứng dụng. Phụ lục B của Tiêu chuẩn cung cấp một danh sách các nguy cơ cho doanh nghiệp đã biết. Mặc dù danh sách này không phải là hoàn toàn đầy đủ, nó cung cấp điểm xuất phát đầu tiên cho bất kì phân tích nào. Một khi lược sử của nguy cơ đối với mạng được đưa ra, các điểm yếu được phân tích để xác định các nguy cơ có thể được thực hiện như thế nào trong bối cảnh của tài sản cụ thể đang xem xét. Phân tích như vậy sẽ giúp xác định phương pháp giảm thiểu nguy cơ nào đang bị bỏ sót và biện pháp đối phó nào cần phải được thực thi để đạt được mục tiêu bảo vệ. Biện pháp đối phó sẽ giảm khả năng thành công của nguy cơ và/hoặc giảm tác động của nó. Phân tích rủi ro phân

tích rủi ro thể diện bằng các điểm yếu được phát hiện. Phân tích ảnh hưởng đến kinh doanh bao gồm đạt được quyết định kinh doanh tương ứng với giải quyết từng điểm yếu như thế nào: khắc phục, chấp nhận rủi ro, hay chuyển rủi ro.

Thiết kế các biện pháp đối phó và thực hiện kiểm soát các điểm yếu bảo vệ khỏi nguy cơ là một phần của bất cứ phương pháp luận đánh giá an toàn nào. Để tương thích với loạt tiêu chuẩn ISO/IEC 27000 việc lựa chọn và thực hiện các kiểm soát liên quan là tối quan trọng cho bảo vệ tài sản/ thông tin. Tiêu chuẩn yêu cầu duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin, và đặc biệt công bố bổ sung rằng các đặc tính khác như tính xác thực, tính không chối bỏ và tính tin cậy cũng có thể được tính đến.

Sau đây sẽ là bộ các thuộc tính an toàn được sử dụng trong phần này của Tiêu chuẩn ISO/IEC 27033 nhằm phát triển các phương pháp giảm thiểu và biện pháp đối phó dưới dạng hướng đối tượng. Hợp lý hóa nhu cầu cho từng thuộc tính (bổ sung thêm tính bí mật, tính toàn vẹn và tính sẵn sàng) được mô tả dưới đây.

- Tính bí mật liên quan với bảo vệ dữ liệu khỏi lộ thông tin bất hợp pháp.
- Tính toàn vẹn liên quan với bảo trì tính đúng đắn hoặc độ chính xác của dữ liệu và bảo vệ chống lại thay đổi, xóa bỏ, tạo, và nhân bản bất hợp pháp.
- Tính sẵn sàng liên quan với việc đảm bảo rằng không được phép từ chối truy cập hợp pháp vào các thành phần mạng, thông tin lưu trữ, luồng thông tin, dịch vụ và ứng dụng.
- Kiểm soát truy cập, thông qua sử dụng xác nhận và xác thực, cung cấp kiểm soát thực hiện truy cập vào các thiết bị và dịch vụ mạng, và đảm bảo rằng chỉ có cá nhân hay thiết bị hợp pháp mới được cho phép truy cập vào các thành phần mạng, thông tin lưu trữ, luồng thông tin, dịch vụ và ứng dụng. Ví dụ, khi triển khai IPTV, một trong những khuyến nghị an toàn được biết là vô hiệu hóa giao diện gỡ rối trong thiết bị giải mã truyền hình (STB) của thuê bao, được lấy từ xem xét thuộc tính kiểm soát truy cập. Kiểm tra tính bí mật, tính toàn vẹn, tính sẵn sàng sẽ không gây ảnh hưởng đến các khuyến nghị khác.
- Xác thực liên quan với việc khẳng định hoặc chứng minh danh tính khai báo của người sử dụng hay các bên truyền thông khi sử dụng bằng kiểm soát truy cập để ủy quyền, và cung cấp bảo đảm rằng thực thể không cố gắng đóng giả hoặc dùng lại trái phép truyền thông trước đó. Ví dụ, một cá nhân có thể đạt được truy cập đến hệ thống

quản lý mạng, nhưng sẽ cần xác thực để cập nhật các bản ghi dịch vụ thuê bao. Do đó khả năng thực hiện các hoạt động quản lý mạng không thể được bảo đảm bằng cách đơn giản như giải quyết tính bí mật, tính toàn vẹn tính sẵn sàng hoặc kiểm soát truy cập.

CHÚ THÍCH: Trong kiểm soát truy cập dựa trên vai trò, ủy quyền được thực hiện bằng cách đức tính của người sử dụng được gán vào vai trò. Kiểm soát truy cập khi đó xác minh người sử dụng có vai trò gì trước khi cấp truy cập. Tương tự, các danh sách kiểm soát truy cập cấp truy cập tới bất cứ đâu thỏa mãn chính sách, sao cho nếu bạn đáp ứng các yêu cầu chính sách thì bạn được cấp quyền truy cập. Các chức năng xác thực và ủy quyền là bằng không trong trường hợp này.

- An toàn truyền thông hay truyền tải liên quan với việc đảm bảo rằng thông tin chỉ được truyền đi giữa các điểm đầu cuối ủy quyền mà không bị chuyển hướng hay bị chặn.
- Tính không chối bỏ liên quan với duy trì kiểm định, sao cho nguyên bản dữ liệu hay nguyên nhân của sự kiện hay hành động không thể bị từ chối. Định danh cá nhân ủy quyền thực hiện hành động bất hợp pháp trên dữ liệu được bảo vệ không có nghĩa đối với tính bí mật, tính toàn vẹn, tính sẵn sàng của dữ liệu.
- Tính che chắn liên quan với bảo vệ thông tin có thể thu được từ quan sát các hoạt động mạng. Tính che chắn công nhận nhu cầu bảo vệ các hành động bổ sung thêm vào thông tin. Bảo vệ thông tin được chỉ ra bằng tính bí mật. Bảo vệ cuộc trao đổi trong cuộc gọi điện thoại giữa người A và người B bảo vệ tính bí mật của họ. Bảo vệ sự kiện người A và người B có cuộc thoại đảm bảo tính che chắn.

Trong tất cả các kịch bản mô tả trong phần này của ISO/IEC 27033, các thuộc tính an toàn đưa ra ở trên được xem xét như một phần của các kỹ thuật thiết kế an toàn và giai đoạn kiểm soát. Bảng 1 bên dưới chỉ ra các ví dụ của cơ chế an toàn mạng có thể được thực hiện cho các thuộc tính an toàn được chọn để giảm thiểu rủi ro tiềm năng.

Bảng 1 – Ví dụ các kỹ thuật an toàn mạng

Các xem xét an toàn	Các cơ chế/ kỹ thuật an toàn
Kiểm soát truy cập	Hệ thống biểu trưng vật lý, Danh sách kiểm soát truy cập (ACL), Phân chia trách nhiệm
Xác thực	Mật khẩu đăng nhập đơn giản, Chứng thư số, Chữ ký số,

	TLSv1.2, SSO, CHAP
Tính sẵn sàng	Dự phòng và sao lưu, Tường lửa, IDS/IPS (để ngăn chặn DoS), Tính liên tục nghiệp vụ, Mạng và dịch vụ được quản lý với SLA
An toàn truyền thông	IPSec/L2TP, Các đường thuê bao riêng, Các mạng riêng
Tính bí mật	Mã hóa (3DES, AES), Các danh sách kiểm soát truy cập, Quyền truy cập tệp
Tính toàn vẹn	IPSec HMAC (như SHA-256), Kiểm tra dự phòng vòng tròn, Phần mềm diệt virus
Tính không chối bỏ	Ghi lại, kiểm soát truy cập dựa trên vai trò, Chữ ký số
Tính che chắn	Mã hóa mào đầu IP (ví dụ: VPN với chế độ đường hầm IPSec), NAT (cho IPv4)

Trong phần này của ISO/IEC 27033, các xem xét trên được kế thừa trong thiết kế và thực hiện đã đưa ra trong bối cảnh của từng kịch bản mạng tham chiếu. Nói chung, tổ chức sẽ lựa chọn các kiểm soát TCVN 27002 liên quan để đáp ứng mục tiêu kinh doanh của họ, và hướng dẫn trong phần này của ISO/IEC 27033 nhằm cung cấp các xem xét mức mạng yêu cầu cho thực hiện các kiểm soát đã chọn.

4.3 Cấu trúc

Cấu trúc phần này của bộ tiêu chuẩn ISO/IEC 27033 bao gồm:

- Tổng quan phương pháp tiếp cận giải quyết an toàn cho từng kịch bản tham chiếu được đưa ra trong phần này của ISO/IEC 27033 (điều 6).
- Các điều cho mỗi kịch bản tham chiếu (điều 7-15) mô tả:
    - Các nguy cơ cho kịch bản tham chiếu.
    - Thể hiện của các kiểm soát và kỹ thuật an toàn dựa trên các phương pháp trong điều 6.

Các kịch bản trong tiêu chuẩn được sắp đặt theo từng khung mà mục tiêu là đánh giá một kịch bản nhất định như một hàm số của

- Thể loại truy cập người sử dụng, ở đó người sử dụng ở bên trong doanh nghiệp, hoặc người sử dụng truy cập nguồn tài nguyên doanh nghiệp từ bên ngoài, hoặc người sử dụng là khách hàng, nhà cung cấp hay đối tác kinh doanh, và
- Loại tài nguyên thông tin truy cập, nguồn tài nguyên mở, giới hạn hay thuê ngoài.

Do đó, khung này trợ giúp thể hiện cấu trúc thống nhất, và tạo ra các bổ sung của các kịch bản mới có khả năng quản lý, cũng như điều chỉnh nhu cầu cho các kịch bản đưa ra trong phần này của ISO/IEC 27033.

Bảng 2 – Khung các kịch bản mạng được đặt ra

		Người sử dụng		
		Bên trong	**Nhân viên từ bên ngoài**	**Bên ngoài**
Nguồn thông tin được truy cập	**Mở**	- Các dịch vụ truy cập Internet cho nhân viên - Các dịch vụ doanh nghiệp tới doanh nghiệp		- Các dịch vụ doanh nghiệp tới khách hàng
	Giới hạn	- Các dịch vụ hợp tác nâng cao - Các dịch vụ doanh nghiệp tới doanh nghiệp - Phân đoạn mạng - Hỗ trợ nối mạng cho nhà riêng và văn phòng kinh doanh nhỏ	- Truyền thông di động - Hỗ trợ kết nối mạng cho người sử dụng di chuyển	- Các dịch vụ hợp tác nâng cao - Các dịch vụ doanh nghiệp tới doanh nghiệp - Các dịch vụ doanh nghiệp tới khách hàng
	Thuê ngoài	- Các dịch vụ thuê ngoài		- Các dịch vụ thuê ngoài

Vì vậy, thứ tự sắp đặt các kịch bản được liệt kê trong phần này của Tiêu chuẩn ISO/IEC 27033 như sau:

- Các dịch vụ truy cập Internet cho nhân viên (điều 7);

- Các dịch vụ doanh nghiệp tới doanh nghiệp (điều 8);
- Các dịch vụ doanh nghiệp tới khách hàng (điều 9);
- Các dịch vụ hợp tác nâng cao (điều 10);
- Phân đoạn mạng (điều 11);
- Hỗ trợ nối mạng cho nhà riêng và văn phòng kinh doanh nhỏ (điều 12);
- Truyền thông di động (điều 13);
- Hỗ trợ kết nối mạng cho người sử dụng di chuyển (điều 14);
- Các dịch vụ thuê ngoài (điều 15).

5. Xây dựng tiêu chuẩn về các kịch bản tham chiếu mạng – nguy cơ, các kỹ thuật thiết kế và các vấn đề kiểm soát

Tài liệu tham khảo gốc: ***ISO/IEC 27033-3:2010*** *Information technology – Security techniques – Network security – Reference networking scenarios - Threats, design techniques and control issues.*

Hình thức biên soạn: chấp thuận có sửa đổi, bổ sung.

Sở cứ xây dựng Tiêu chuẩn:

- Hiện nay, ISO và IEC đang biên soạn bộ Tiêu chuẩn về an ninh mạng ISO/IEC 27033, nhằm thay thế cho bộ Tiêu chuẩn ISO/IEC 18028. Với mục tiêu xây dựng Bộ Tiêu chuẩn về an toàn mạng nhằm thay thế cho Bộ tiêu chuẩn TCVN 8051 (dựa trên ISO/IEC 18028 đã cũ, lỗi thời) đáp ứng các yêu cầu mới về an toàn mạng, phù hợp với các công nghệ mới hiện nay, thích hợp với các bối cảnh mới về các mối đe dọa, các kịch bản tấn công, cùng với các bổ sung, cập nhật khác, cần thiết xây dựng bộ Tiêu chuẩn mới dựa trên ISO/IEC 27033.

- Năm 2011 dựa trên Phần 1 của Bộ tiêu chuẩn ISO/IEC 27033: ISO/IEC 27033-1 Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng - Phần 1: Tổng quan và khái niệm *(ISO/IEC 27033-1:2009 Information technology – Security techniques – Network security – Part 1: Overview and concepts)* Bộ Thông tin và Truyền thông đã xây dựng dự thảo Phần 1 của Bộ TCVN xxxx.

- Phần 3 của Bộ tiêu chuẩn ISO/IEC 27033 đưa ra các nội dung về các nguy cơ, các kỹ thuật thiết kế và các vấn đề kiểm soát cho các kịch bản mạng tham chiếu khác nhau. Trong

mỗi kịch bản mạng đưa ra hướng dẫn chi tiết về nguy cơ an toàn và các kỹ thuật thiết kế và kiểm soát yêu cầu cho rủi ro liên quan. Tiêu chuẩn hỗ trợ xác định và thực hiện an toàn cho môi trường mạng của bất cứ tổ chức nào. Dự thảo tiêu chuẩn này hỗ trợ quản lý, hướng dẫn thực hiện đảm bảo an toàn thông tin cho các tổ chức, cá nhân sử dụng mạng thông tin.

- Tài liệu tham chiếu gốc ISO/IEC 27033-3:2010 đầy đủ, rõ ràng để làm cơ sở cho việc đưa ra tiêu chuẩn về an toàn mạng, và là phiên bản mới nhất cho đến thời điểm hiện nay.

Nội dung tiêu chuẩn bao gồm:

1. Phạm vi áp dụng

2. Tài liệu viện dẫn

3. Thuật ngữ và định nghĩa

4. Ký hiệu và chữ viết tắt

5. Cấu trúc

6. Tổng quan

7. Các dịch vụ truy cập Internet cho nhân viên

8. Các dịch vụ doanh nghiệp tới doanh nghiệp

9. Các dịch vụ doanh nghiệp tới khách hàng

10. Các dịch vụ hợp tác nâng cao

11. Phân đoạn mạng

12. Các dịch vụ hỗ trợ kết nối mạng cho nhà riêng và văn phòng kinh doanh nhỏ

13. Truyền thông di động

14. Hỗ trợ kết nối mạng cho người sử dụng từ xa

15. Các dịch vụ thuê ngoài

Phụ lục A. (Tham khảo) – Chính sách sử dụng Internet, ví dụ.

Phụ lục B (Tham khảo) – Danh mục các nguy cơ.

Các sửa đổi bổ sung của dự thảo tiêu chuẩn và Tài liệu tham chiếu gốc được đưa ra trong Bảng 3 dưới đây.

Bảng 3 – Tham chiếu nội dung dự thảo Tiêu chuẩn với tài liệu gốc

Dự thảo TCVN	Tài liệu gốc ISO/IEC 27033-3	Hình thức biên soạn	Chú thích
1. Phạm vi áp dụng	Điều 1	Chấp thuận nguyên vẹn	
2. Tài liệu viện dẫn	Điều 2	Chấp thuận nguyên vẹn	
3. Thuật ngữ và định nghĩa	Điều 3 Phụ lục A.6	Chấp thuận có sửa đổi, bổ sung	Ghép điều 3 và phụ lục A.6
4. Ký hiệu và thuật ngữ	Điều 4	Chấp thuận nguyên vẹn	
5. Cấu trúc	Điều 5	Chấp thuận nguyên vẹn	
6. Tổng quan	Điều 6	Chấp thuận nguyên vẹn	
7. Các dịch vụ truy cập Internet cho nhân viên	Điều 7	Chấp thuận nguyên vẹn	
8. Các dịch vụ doanh nghiệp tới doanh nghiệp	Điều 8	Chấp thuận nguyên vẹn	
9. Các dịch vụ doanh nghiệp tới	Điều 9	Chấp thuận có sửa đổi, bổ	Bổ sung phần giải thích trong ():

khách hàng		sung	Tr. 20 - ‘man in the middle‘ MITM (MITM giống như nghe trộm, hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và chuyển hướng các bản tin giữa chúng) hay ‘man in the browser’ (phần mềm độc hại được kích hoạt và hoạt động như là người trung gian giữa người dùng và trang Web); Tr. 21 - các tấn công SQL injection (là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để thâm nhập vào và thi hành các câu lệnh SQL bất hợp pháp), các tấn công Cross-Site Scripting XSS (là một kĩ thuật tấn công bằng cách chèn vào các website động những thẻ HTML hay những đoạn mã script nguy hiểm);
10. Các dịch vụ hợp tác nâng cao	Điều 10	Chấp thuận nguyên vẹn	
11. Phân đoạn mạng	Điều 11	Chấp thuận nguyên vẹn	
12. Các dịch vụ hỗ trợ kết nối mạng cho nhà riêng và văn phòng kinh doanh nhỏ	Điều 12	Chấp thuận nguyên vẹn	

13. Truyền thông di động	Điều 13	Chấp thuận nguyên vẹn	
14. Hỗ trợ kết nối	Điều 14	Chấp thuận nguyên vẹn	
15. Các dịch vụ thuê ngoài	Điều 15	Chấp thuận nguyên vẹn	
Phụ lục A. (Tham khảo) – Chính sách sử dụng Internet ví dụ	Phụ lục A	Chấp thuận có sửa đổi, bổ sung	Bỏ phụ lục A.6 đã ghép phần định nghĩa "spam" vào điều 3. Ghép định nghĩa "blog" của mục A.6 vào mục A.4.4
Phụ lục B (Tham khảo) – Danh mục các nguy cơ.	Phụ lục B	Chấp thuận nguyên vẹn	

6. Kết luận

Dự thảo Phần 3 của bộ Tiêu chuẩn TCVN xxxx, được xây dựng chấp thuận có bổ sung thay đổi so với tài liệu gốc ***ISO/IEC 27033-3:2010*** *Information technology – Security techniques – Network security – Reference networking scenarios - Threats, design techniques and control issues.*

Tài liệu tham khảo

[1] TCVN 8051-1:2009 Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng công nghệ thông tin - Phần 1: Quản lý an ninh mạng.

[2] TCVN 8051-2:2009 Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng công nghệ thông tin - Phần 2: Kiến trúc an ninh mạng.

[3] ISO/IEC 18028-1:2005 Information technology – Security techniques – IT network security – Part 1: Network security management *(ISO/IEC 18028-1:2005 Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng công nghệ thông tin - Phần 1: Quản lý an ninh mạng).*

[4] ISO/IEC 18028-2:2006 Information technology – Security techniques – IT network security – Part 2: Network security architecture *(ISO/IEC 18028-2:2006 Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng công nghệ thông tin - Phần 2: Kiến trúc an ninh mạng).*

[5] ISO/IEC 27033-1:2009 Information technology – Security techniques – Network security – Part 1: Overview and concepts *(ISO/IEC 27033-1:2009 Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng - Phần 1: Tổng quan và khái niệm).*

[6] ISO/IEC 27033-3:2010 - Information technology – Security techniques – Network security Part 3: Reference networking scenarios - Threats, design techniques and control issues. *(ISO/IEC 27033-3:2010 - Công nghệ thông tin – Kỹ thuật an toàn – An toàn mạng – Phần 3: Các kịch bản kết nối mạng tham chiếu – Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát).*
