TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN xxxx-3:2013
ISO/IEC 27033-3:2010

Xuất bản lần 1

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 – 2013

Mục lục

Lời nói đầu

TCVN xxxx-3:2013 hoàn toàn tương đương Tiêu chuẩn ISO/IEC 27033-3: 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*).

TCVN xxxx-3:2013 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin – 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

1 Phạm vi áp dụng

TCVN xxxx-3 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, các kỹ thuật và kiểm soát an toàn yêu cầu để giảm thiểu các rủi ro liên quan. Tiêu chuẩn này bao hàm các tham chiếu đến các tiêu chuẩn quốc gia từ TCVN xxxx-4 đến TCVN xxxx-7 để tránh trùng lặp nội dung của các tiêu chuẩn này.

TCVN xxxx-3 được sử dụng khi xem xét các tùy chọn kiến trúc (hoặc thiết kế) về an toàn kỹ thuật và khi lựa chọn, soạn thảo kiến trúc (hoặc thiết kế) về an toàn kỹ thuật ưu tiên, các kiểm soát an toàn liên quan, tương thích với TCVN xxxx-2. Thông tin cụ thể được lựa chọn (cùng với thông tin được lựa chọn từ các tiêu chuẩn quốc gia từ TCVN xxxx-4 đến TCVN xxxx-7) sẽ phụ thuộc vào các đặc tính của môi trường mạng được xem xét, tức là kịch bản mạng cụ thể và chuyên đề "công nghệ" liên quan.

Về tổng thể, Tiêu chuẩn này sẽ hỗ trợ đáng kể việc xác định và thực hiện toàn diện về an toàn cho bất cứ môi trường mạng nào của tổ chức.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN xxxx-1:2011 – Công nghệ thông tin - Kỹ thuật an toàn – An toàn mạng – Phần 1: Tổng quan và khái niệm *(TCVN xxxx-1:2011 – Information technology – Security techniques – Network security – Part 1: Overview and concepts)*.

ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. *(ISO/IEC 27000 – Công nghệ thông tin – Kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Tổng quan và khái niệm)*.

ISO/IEC 27036 – Information technology – Security techniques – Information security for supplier relationships. *(ISO/IEC 27000 – Công nghệ thông tin – Kỹ thuật an toàn – An toàn thông tin cho mối quan hệ nhà cung cấp)*.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong ISO/IEC 27000, TCVN xxxx-1, và các thuật ngữ, định nghĩa sau.

3.1

Khai thác xã hội (social engineering)

Thủ thuật thao túng người dùng để tác động vào các hoạt động đang thực thi hoặc để tiết lộ thông tin bí mật.

3.2

Phần mềm độc hại (malware/malicious software)

Loại phần mềm được thiết kế với mục đích gây hại, chứa các tính năng hoặc khả năng có thể gây ra thiệt hại trực tiếp hoặc gián tiếp cho người sử dụng và/hoặc hệ thống máy tính.

3.3

Tính che chắn (opacity)

Bảo vệ thông tin có thể được dẫn xuất bằng quan sát các hoạt động mạng, như các địa chỉ đến của các điểm đầu cuối trong cuộc gọi thoại trên giao thức IP (VoIP).

CHÚ THÍCH: Tính che chắn công nhận sự cần thiết phải bảo vệ các hoạt động bổ sung thêm vào thông tin.

3.4

Thuê ngoài (outsourcing)

Mua lại các dịch vụ bởi bên mua để thực hiện các hoạt động được yêu cầu nhằm hỗ trợ các chức năng kinh doanh của bên mua.

3.5 Thư rác (spam)

Gửi thư điện tử số lượng cực lớn bất hợp pháp và/hoặc không mong muốn.

4 Ký hiệu và thuật ngữ

AAA	Xác thực, ủy quyền và kiểm toán	Authentication, Authorization and Accounting
DHCP	Giao thức cấu hình máy chủ động	Dynamic Host Configuration Protocol
DNS	Dịch vụ tên miền	Domain Name Service
DNSSEC	Mở rộng an toàn dịch vụ tên miền	DNS Security Extention

DoS	Từ chối dịch vụ	Denial of Service
FTP	Giao thức truyền tệp	File Transfer Protocol
GUI	Giao diện người sử dụng đồ họa	Graphical User Interface
ID	Nhận dạng	Identification
IDS	Hệ thống phát hiện xâm nhập	Intrusion Detection System
IP	Giao thức Internet	Internet Protocol
IPSec	Giao thức an toàn IP	IP Security Protocol
OAM&P	Vận hành, Quản trị, Bảo trì và Cung cấp	Operations, Administration, Maintenance & Provisioning
OSI	Kết nối hệ thống mở	Open Systems Interconnection
PDA	Trợ giúp dữ liệu cá nhân	Personal Data Assistant
PSTN	Mạng điện thoại công cộng	Public Switched Telephone Networks
QoS	Chất lượng dịch vụ	Quality of Service
SIP	Giao thức khởi tạo phiên	Session Initiation Protocol
SMTP	Giao thức chuyển thư điện tử đơn giản	Simple Mail Transfer Protocol
SNMP	Giao thức quản lý mạng đơn giản	Simple Network Management Protocol
SSL	Tầng cổng an toàn (Giao thức mã hóa và xác thực)	Secure Socket Layer (Encryption and authentication protocol)
VLAN	Mạng cục bộ ảo	Virtual Local Area Network
VoIP	Thoại trên giao thức IP	Voice over IP
VPN	Mạng riêng ảo	Virtual Private Network
WLAN	Mạng cục bộ không dây	Wireless Local Area Network

5 Cấu trúc

Cấu trúc của tiêu chuẩn này bao gồm:

- Điều 6: Tổng quan phương pháp tiếp cận đề cập đến an toàn cho từng kịch bản tham chiếu được đưa ra trong tiêu chuẩn này.
- Điều 7-15 mô tả cho mỗi kịch bản tham chiếu:
    - Các nguy cơ cho kịch bản tham chiếu.
    - Các kiểm soát và kỹ thuật an toàn dựa trên các phương pháp trong điều 6.

Các kịch bản trong tiêu chuẩn này được sắp đặt theo từng khung với 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;
- **Loại tài nguyên thông tin truy cập**, nguồn tài nguyên mở, bị giới hạn hay thuê ngoài.

Do đó, khung này trợ giúp thể hiện một cấu trúc thống nhất, và tạo ra các bổ sung của các kịch bản mới có khả năng quản lý, cũng như điều chỉnh sự cần thiết đối với các kịch bản khác nhau đưa ra trong tiêu chuẩn này.

Bảng 1 – Khung cho các kịch bản mạng được sắp đặt

		Người sử dụng		
		Nhân viên truy cập từ bên trong	**Nhân viên truy cập từ bên ngoài**	**Khách hàng, đối tác**
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 kết nối mạng cho nhà riêng và văn phòng kinh doanh nhỏ	- Truyền thông di động - Hỗ trợ kết nối mạng cho người sử dụng đang 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 tiêu chuẩn này 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 kết 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 đang di chuyển (điều 14);
- Các dịch vụ thuê ngoài (điều 15).

6 Tổng quan

Tiêu chuẩn này hướng dẫn cho từng kịch bản mạng tham chiếu đã xác định dựa trên các cách tiếp cận sau:

- Soát 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 được phát hiện;
- 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, mong muốn một phương pháp tiếp cận một cách hệ thống và cung cấp đánh giá toàn trình. Độ phức tạp của một 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 rãi thành các tài sản hạ tầng, dịch vụ và ứng dụng. Tuy nhiên, doanh nghiệp có thể lựa chọn để xác định các thể loại của riêng mình, nhưng việc phân định rõ ràng là quan trọng, vì rằng phơi bày 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 hỗ trợ mạng khác nhau, như các hoạt động quản lý; các bản tin điều khiển/ báo hiệu; và dữ liệu người sử dụng cuối (hiện diện cố định hay đang di chuyển). 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 dự đoán ID quản trị và mật khẩu). Tự bản thân lưu lượng quản lý cũng

là chủ thể của 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 một bộ đã biết các nguy cơ để chắc chắn rằng nguy cơ nào có khả năng ứng dụng. Phụ lục B cung cấp một danh sách các nguy cơ đã biết cho doanh nghiệp. Mặc dù danh sách này không phải là hoàn toàn đầy đủ, nó cung cấp xuất phát điểm đầu tiên cho bất kì phân tích nào. Một khi đưa ra mô tả sơ lược của nguy cơ đối với mạng, phân tích các điểm yếu 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 này 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 thể hiện 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 chống chối bỏ và tính tin cậy cũng có thể được xem xét đến.

Sau đây sẽ là bộ các thuộc tính an toàn được sử dụng trong tiêu chuẩn này 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 tính 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 đã 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. Soát xét tính bí mật, tính toàn vẹn, tính sẵn sàng sẽ không gây ảnh hưởng đến một số khuyến nghị khác;

- Xác thực liên quan đến 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 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 bảo đảm được 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 đáp ứng 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 đến 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 chống chối bỏ liên quan đến duy trì kiểm định, sao cho nguyên bản dữ liệu hay nguyên nhân của sự kiện hay hành động không thể bị chối bỏ. 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 sự cần thiết phải bảo vệ các hành động bổ sung thêm vào thông tin. Bảo vệ thông tin được đề cập bằng tính bí mật. Bảo vệ 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 tiêu chuẩn này, 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 2 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 lựa chọn để giảm thiểu rủi ro tiềm năng.

Bảng 2 – 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 chống 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 tiêu chuẩn này, các xem xét trên được kế thừa trong thiết kế và triển khai đưa ra trong bối cảnh của từng kịch bản mạng tham chiếu. Nói chung, tổ chức sẽ lựa chọn các kiểm soát liên quan trong TCVN 27002 để đáp ứng mục tiêu kinh doanh của họ, và hướng dẫn trong tiêu chuẩn này nhằm cung cấp các xem xét mức mạng được yêu cầu để thực hiện các kiểm soát đã chọn.

7 Dịch vụ truy cập Internet cho nhân viên

7.1 Khái quát

Các tổ chức cần cung cấp các dịch vụ truy cập Internet cho nhân viên của mình phải xem xét kịch bản này để đảm bảo truy cập cho các mục đích đã được xác định và được ủy quyền rõ ràng, không phải cho truy cập mở nói chung. Các tổ chức cần quan tâm đến việc quản lý truy cập để tránh mất băng thông mạng, tính đáp ứng và phải đối mặt với trách nhiệm pháp lý khi các nhân viên truy cập mà không thể kiểm soát các dịch vụ.

Kiểm soát truy cập của nhân viên vào Internet là mối quan tâm ngày càng lớn, dẫn đến phải có một loạt các qui định Internet cấp thiết. Do đó các tổ chức phải có trách nhiệm trong thiết lập, giám sát và tuân thủ chính sách người sử dụng Internet rõ ràng bằng cách đánh giá các kịch bản và cung cấp các thông báo liên quan trong chính sách:

- Truy cập Internet được cho phép cho các lý do nghiệp vụ;
- Nếu truy cập Internet cũng được cho phép chính thức (giới hạn) cho các mục đích riêng, các dịch vụ được cho phép sử dụng;
- Nếu dịch vụ hợp tác được cho phép;
- Nếu nhân viên được cho phép tham gia các kênh chat, diễn đàn …

Khi chính sách được soạn thảo thể hiện như một ngăn cản đáng kể đối với việc sử dụng Internet sẽ không được chấp thuận, tổ chức vẫn còn phải chịu các rủi ro an toàn thông tin lớn. Trong mục dưới đây, các nguy cơ an toàn và các tư vấn về các kỹ thuật thiết kế và kiểm soát an toàn nhằm giảm thiểu các rủi ro này được mô tả cho việc sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

7.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan đến dịch vụ truy cập Internet cho các nhân viên là:

- Các tấn công bằng virus và đưa ra phần mềm độc hại:
    - Các nhân viên sử dụng Internet cũng là mục tiêu chủ yếu của phần mềm độc hại, có thể dẫn đến mất hay bị phá hủy thông tin và mất điều khiển hạ tầng IT, và là rủi ro cực lớn cho an toàn mạng của tổ chức;
    - Tệp hay chương trình tải về của người sử dụng có thể chứa mã độc. Với tính chất mọi lúc mọi nơi của các ứng dụng như tin nhắn tức thời, chia sẻ tệp ngang hàng, và thoại IP, các nhân viên có thể vô tình tải về và cài đặt ứng dụng độc hại có thể né tránh các bảo vệ mạng sử dụng các kỹ thuật như vượt cổng (nhẩy qua một trong những cổng mở) và mã hóa. Thêm nữa, các ứng dụng ngang hàng có thể bị khai thác hoạt động như các kênh ngầm cho mạng ma botnet;
    - Các điểm yếu trên trình duyệt web hay các ứng dụng web khác có thể bị khai thác bởi phần mềm độc hại, và kết quả là bị nhiễm virus và bị cài Trojan. Một khi đã bị nhiễm, tính sẵn sàng có thể bị tác động nghiêm trọng do các hoạt động lan truyền virus dẫn đến quá tải mạng. Trojan có thể cho phép truy cập từ bên ngoài bất hợp pháp dẫn đến vi phạm tính bí mật.
- Rò rỉ thông tin: các ứng dụng cho phép tải lên thông tin tới các máy chủ web có thể dẫn đến chuyển dữ liệu không kiểm soát được từ bên trong tổ chức ra Internet. Nếu các phiên mã hóa được sử dụng (như TLS) thì thậm chí việc ghi lại hoạt động này cũng có thể không thực hiện được. Các rủi ro an toàn tương tự được đưa ra khi mã di động không được thẩm định thực hiện trong hệ thống bên trong tổ chức;
- Sử dụng và truy cập bất hợp pháp: mất kiểm soát hạ tầng, hệ thống và ứng dụng có thể gây ra gian lận, từ chối dịch vụ, và lạm dụng các phương tiện;
- Trách nhiệm do không tuân thủ quy định:
    - Trách nhiệm pháp lý do không tuân thủ nghĩa vụ pháp luật và quy định;
    - Không tuân thủ chính sách người sử dụng của tổ chức có thể dẫn đến không tuân thủ quy định.
- Giảm tính sẵn sàng của mạng do băng thông không đủ hay các vấn đề tính ổn định: sử dụng liên tục các dịch vụ băng thông cao như phương tiện trực tuyến hay chia sẻ tệp ngang hàng có thể dẫn đến quá tải mạng.

7.3 Các kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến các dịch vụ truy cập Internet của nhân viên được đưa ra trong Bảng 3.

Đối với rủi ro nhất định, mỗi thuộc tính an toàn được xem xét cho khả năng áp dụng làm giảm rủi ro và sau đó ví dụ thực hiện kỹ thuật tương ứng được biểu diễn trong cột thứ hai. Ví dụ, tính toàn vẹn, kiểm soát truy cập và xác thực có khả năng áp dụng để bảo vệ chống lại mã độc.

Bảng 3 – Các kiểm soát an toàn cho kịch bản truy cập Internet của nhân viên

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Các tấn công virus và đưa ra phần mềm độc hại	
• Tính toàn vẹn • Kiểm soát truy cập • Xác thực	• Chỉ cung cấp các dịch vụ Internet liên quan nghiệp vụ cho nhân viên. Sử dụng danh sách đen cho các dịch vụ hợp pháp, để không cho phép các kênh chat hoặc các dịch vụ thư điện tử web, hoặc các giao thức mạng ngang hàng. • Sử dụng phần mềm chống virus trên các cổng ra Internet để quét tất cả lưu lượng vào và ra Internet. Quét phải bao gồm tất cả giao thức mạng được quyền sử dụng. Đảm bảo rằng cập nhật chống virus được cài đặt tự động hoặc người sử dụng được thông báo khi cập nhật đã sẵn sàng. • Sử dụng phần mềm chống virus trên tất cả các hệ thống khách hàng, đặc biệt cho các hệ thống được sử dụng cho truy cập Internet của nhân viên. • Quét tệp và tất cả thông tin lưu giữ đối với các virus và Trojan và các dạng phần mềm độc hại khác. • Xác minh tính toàn vẹn của dữ liệu/ tệp sử dụng các thuật toán như hàm băm/ kiểm tra tổng, chứng thư. • Ngăn chặn cửa sổ pop-up và các quảng cáo web. • Định tuyến lưu lượng sử dụng cho các dịch vụ truy cập Internet thông qua số lượng ít các cổng an toàn được kiểm soát. • Hoạt động xác thực nội dung.
Rò rỉ thông tin	
• An toàn truyền thông • Tính toàn vẹn	• Triển khai các bộ lọc cho mã di động trên các cổng nối ra Internet. • Chấp nhận mã di động chỉ từ các vị trí không quan trọng,

• Kiểm soát truy cập	trong danh sách trắng. • Chỉ chấp nhận mã di động chữ ký số được ký từ các ủy quyền chứng thực được phê duyệt hoặc từ các nhà cung cấp được phê duyệt, cho phép các tùy chọn cấu hình tương ứng trên phía khách hàng, ví dụ như bằng cách chủ động quản lý và thực thi danh sách trắng mã cho phép ký ủy quyền chứng thực.
Truy cập và sử dụng bất hợp pháp	
• Kiểm soát truy cập • Chống chối bỏ	• Chỉ cung cấp các dịch vụ Internet liên quan nghiệp vụ cho nhân viên. Sử dụng danh sách đen cho các dịch vụ bất hợp pháp, ví dụ như các kênh chat hay dịch vụ thư điện tử web. Triển khai các bộ lọc cho các giao thức trái phép, ví dụ như các giao thức kết nối mạng ngang hàng. • Giới hạn sử dụng các dịch vụ dễ có khả năng chuyển tải lượng dữ liệu lớn. • Bảo đảm luôn đăng nhập và giám sát đúng cho tất cả các dịch vụ được phép có khả năng chuyển tải dữ liệu ra Internet. • Xác định rõ ràng việc sử dụng truy cập Internet hợp pháp và bất hợp pháp trong chính sách dành riêng (xem ví dụ trong Phụ lục A). • Đảm bảo nhận thức người sử dụng thông qua giáo dục và đào tạo đầy đủ.
Trách nhiệm pháp lý do không tuân thủ quy định	
• Chống chối bỏ	• Sử dụng các bản ghi, dấu thời gian. • Nhận thức và đào tạo người sử dụng.
Giảm tính sẵn sàng của mạng	
• Tính toàn vẹn • Tính sẵn sàng	• Quản lý các điểm yếu đúng đắn và sửa lỗi các điểm yếu hệ thống đã biết trong phạm vi khung thời gian dựa trên tính nghiêm trọng của điểm yếu. • Trọng tâm của quản lý điểm yếu phải là tất cả các hệ thống nhận lưu lượng Internet, bất kể trên mức truyền tải hay mức ứng dụng, bao gồm tất cả các hệ thống sử dụng

	trong bối cảnh của các cổng sử dụng ra Internet cũng như các hệ thống người sử dụng cuối được dùng cho các dịch vụ truy cập Internet, đặc biệt nếu chúng sử dụng hệ điều hành window. • Điều tiết băng thông cho phương tiện trực tuyến (chỉ khi cho phép trên từng chính sách nghiệp vụ). • Các tài nguyên mạng và hệ thống phải được giám sát (IDS, bản ghi, kiểm toán…) để phát hiện các sự kiện hệ thống, an toàn và vận hành.

8 Dịch vụ doanh nghiệp tới doanh nghiệp

8.1 Khái quát

Các tổ chức thiết lập giao dịch với các tổ chức khác, như nhà sản xuất, bán buôn, bán lẻ phải xem xét kịch bản này.

Theo truyền thống các dịch vụ doanh nghiệp tới doanh nghiệp đã được triển khai bằng cách sử dụng các đường thuê kênh riêng hoặc các đoạn mạng riêng. Internet và các công nghệ liên quan cung cấp nhiều tùy chọn hơn, nhưng cũng đưa ra các rủi ro an toàn mới liên quan đến triển khai những dịch vụ này. Mô hình thương mại điện tử doanh nghiệp tới doanh nghiệp phát triển cho phép các tổ chức tiến hành kinh doanh trên Internet, và các ứng dụng tập trung sử dụng Internet, extranet, hoặc cả hai để nâng cao quan hệ đối tác kinh doanh mà các thực thể đã biết rõ về nhau và tất cả người sử dụng được đăng ký, không giống như kịch bản doanh nghiệp với người tiêu dùng.

Nói chung các dịch vụ doanh nghiệp tới doanh nghiệp có các yêu cầu riêng của họ. Ví dụ, tính sẵn sàng và tính tin cậy là các yêu cầu rất quan trọng do các tổ chức thường xuyên phụ thuộc trực tiếp vào hoạt động của các dịch vụ doanh nghiệp tới doanh nghiệp.

Khi sử dụng Internet như kết nối mạng cơ bản để thực thi dịch vụ doanh nghiệp tới doanh nghiệp, các yêu cầu như tính sẵn sàng và tính tin cậy cần phải xử lý khác so với trước. Các đánh giá đã được kiểm chứng như chất lượng dịch vụ giả định đã sử dụng, như cùng với đường thuê kênh riêng, không còn thích hợp nữa. Các rủi ro an toàn mới cần được giảm thiểu bằng các kỹ thuật thiết kế và kiểm soát phù hợp. Trọng tâm là tăng cường tin cậy giữa các tổ chức bằng cách ngăn chặn truy cập vào dữ liệu trái phép và duy trì phân biệt các hệ thống doanh nghiệp.

Trong mục sau, các nguy cơ an toàn và tư vấn về các kỹ thuật thiết kế, kiểm soát an toàn để giảm nhẹ các rủi ro liên quan được mô tả cho việc sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

8.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan đến các dịch vụ doanh nghiệp tới doanh nghiệp là:

- Các tấn công bằng virus và đưa ra phần mềm độc hại:
    - Phần mềm độc hại khai thác các con đường dẫn đến xâm nhập hệ thống để gây ra gián đoạn hoặc truy cập bất hợp pháp vào thông tin nhạy cảm;
    - Các điểm yếu trong trình duyệt web hay các ứng dụng web khác có thể bị khai thác bởi phần mềm độc hại, và kết quả là bị nhiễm virus và bị cài Trojan.
- Từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS) tấn công trên cổng thông tin hay extranet doanh nghiệp tới doanh nghiệp.
- Các tấn công từ bên trong bởi các đối tác doanh nghiệp hợp pháp.
- Giả mạo các nội dung giao dịch (các bản tin không đến được người nhận dự kiến hoặc dữ liệu bị xáo trộn trong truyền tải).

8.3 Các kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến các dịch vụ doanh nghiệp tới doanh nghiệp liên quan với:

Bảng 4 – Các kiểm soát cho kịch bản các dịch vụ doanh nghiệp tới doanh nghiệp

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Các tấn công virus và đưa ra phần mềm độc hại	
• Tính toàn vẹn • Kiểm soát truy cập • Xác thực	• Sử dụng phần mềm kiểm tra virus trên các cổng ra Internet để quét tất cả lưu lượng vào và ra Internet. Quét phải bao gồm tất cả giao thức mạng được quyền sử dụng. Đảm bảo rằng cập nhật chống virus được cài đặt tự động hoặc người sử dụng được thông báo khi cập nhật đã sẵn sàng. • Quét tệp và tất cả thông tin lưu giữ đối với các virus và Trojan và các dạng phần mềm độc hại khác. • Xác minh tính toàn vẹn của dữ liệu/ tệp sử dụng các thuật toán như hàm băm/ kiểm tra tổng, chứng thư. • Định tuyến lưu lượng sử dụng cho các dịch vụ truy cập Internet thông qua số lượng ít các cổng an toàn được kiểm soát. • Hoạt động xác thực nội dung.

Các tấn công từ chối dịch vụ	
• Tính sẵn sàng • Tính che chắn	• Vô hiệu hóa các cổng giao thức và dịch vụ không sử dụng nhằm ngăn ngừa chúng trả lời các tín hiệu quét/ thăm dò trái phép có tiềm năng gây ra từ chối dịch vụ do tràn ngập lưu lượng. • Loại trừ thông tin mô tả từ các cảnh báo lỗi nhằm ngăn ngừa cung cấp thông tin mục tiêu cho bên tấn công.
Các tấn công từ bên trong	
• Kiểm soát truy cập • Chống chối bỏ	• Xác định rõ ràng chính sách an toàn cho quản lý truy cập (cho quản lý quan hệ kinh doanh). • Định rõ vai trò và trách nhiệm. • Tùy chỉnh cảnh báo lỗi. • Giới hạn các đặc quyền. • Ghi lại tất cả các giao dịch người sử dụng cả quan trọng lẫn không quan trọng.
Giả mạo nội dung giao dịch	
• Chống chối bỏ	• Các bản ghi chi tiết của giao dịch. • Sử dụng chữ ký số.

9 Các dịch vụ doanh nghiệp tới khách hàng

9.1 Khái quát

Các tổ chức thiết lập giao dịch với khách hàng phải xem xét kịch bản này.

Các dịch vụ doanh nghiệp tới khách hàng, cũng còn được xem như dịch vụ kinh doanh điện tử như thương mại điện tử, ngân hàng điện tử, chính phủ điện tử. Trong các dịch vụ doanh nghiệp tới khách hàng, an toàn phải cân bằng giao dịch cho phép với giữ gìn giá trị thương hiệu và kinh doanh.

Các yêu cầu an toàn thông tin bao gồm các điểm liên quan với:

- Tính bí mật (đặc biệt cho ngân hàng điện tử);
- Xác thực;
- Tính toàn vẹn;

- An toàn truyền thông dữ liệu khi người sử dụng cuối mong muốn dịch vụ doanh nghiệp cung cấp bảo vệ đường giao dịch giữa người sử dụng và nhà cung cấp. Biện pháp bảo vệ chống lại các tấn công tinh vi, như các tấn công '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);
- Tính sẵn sàng là thước đo quan trọng cho nhà cung cấp thương mại điện tử.

Các đặc tính an toàn thông tin bao gồm:

- An toàn chỉ "bảo đảm" trên nền tảng cuối điển hình dưới sự kiểm soát của tổ chức, cung cấp môi trường tốt cho thực thi kiểm soát và duy trì an toàn mức nền tảng tốt;
- An toàn trên nền tảng khách hàng, thường là trên PC, nói chung có thể là kém. Rất khó để đạt được kiểm soát thực hiện trong môi trường như vậy, và do đó nền tảng khách hàng có thể gây ra các rủi ro đáng kể trong kịch bản này (loại trừ bộ các yêu cầu 'các điều kiện cho kết nối an toàn' trong hợp đồng, mà có thể khó áp đặt trong môi trường như vậy).

Trong mục dưới đây, các nguy cơ an toàn và tư vấn kỹ thuật thiết kế và kiểm soát an toàn để giảm thiểu các rủi ro liên quan được mô tả cho sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

9.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan đến dịch vụ doanh nghiệp tới khách hàng là:

- Các tấn công bằng virus và đưa ra phần mềm độc hại:
    - Phần mềm độc hại khai thác các con đường dẫn đến xâm nhập hệ thống để gây ra gián đoạn hoặc truy cập bất hợp pháp vào thông tin nhạy cảm;
    - Các điểm yếu trong trình duyệt web hay các ứng dụng web khác có thể bị khai thác bởi phần mềm độc hại, và kết quả là bị nhiễm virus và bị cài Trojan.
- Truy cập bất hợp pháp:
    - Truy cập bất hợp pháp vào cơ sở dữ liệu đầu cuối, như 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 kỹ thuật tấn công bằng cách chèn vào các website động những thẻ HTML hay những đoạn mã script nguy hiểm);
    - Khai thác tài khoản, có khả năng lấy được thông tin tài khoản hợp lệ phụ thuộc vào ứng dụng web trả lời xác thực người sử dụng như thế nào. Các mã script tự động thường được sử dụng để thu các ID người sử dụng và tên tài khoản hợp lệ;

- Đánh cắp danh tính trực tuyến sử dụng các tấn công khai thác xã hội thành công (thông qua sử dụng các kỹ thuật lừa đảo), như các tấn công giả mạo và các tấn công dựa trên DNS kết nối người sử dụng với máy chủ web giả mạo – trông giống như máy chủ hợp pháp nhưng thực chất là không phải;
- Truy cập trái phép vào hệ thống hay mạng với ý định gây hại như sao chép, thay đổi hay phá hủy dữ liệu;
- Giải mã nội dung bất hợp pháp dẫn đến xâm phạm bản quyền và đánh cắp dữ liệu.

- Các tấn công từ chối dịch vụ (DoS);
- Giả mạo các nội dung giao dịch (các bản tin không đến được người nhận dự định hoặc dữ liệu bị xáo trộn trong truyền tải).

9.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến các dịch vụ doanh nghiệp tới khách hàng được đưa ra trong Bảng 5.

Bảng 5 – Các kiểm soát an toàn cho kịch bản dịch vụ doanh nghiệp tới khách hàng

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Các tấn công virus và đưa ra phần mềm độc hại	
• Tính toàn vẹn • Kiểm soát truy cập • Xác thực	• Sử dụng phần mềm chống virus trên các cổng ra Internet để quét tất cả lưu lượng vào và ra Internet. Quét trên cổng phải bao gồm tất cả giao thức mạng được quyền sử dụng. • Quét tệp và tất cả thông tin lưu giữ đối với các virus và Trojan và các dạng phần mềm độc hại khác. • Xác minh tính toàn vẹn của dữ liệu/ tệp sử dụng các thuật toán như hàm băm/ kiểm tra tổng, chứng thư. • Định tuyến lưu lượng sử dụng cho các dịch vụ truy cập Internet thông qua số lượng ít các cổng an toàn được kiểm soát. • Hoạt động xác thực nội dung.
Truy cập bất hợp pháp	
• Kiểm soát truy cập	• Giới hạn cho phép các ứng dụng web khi truy cập cơ sở

• Xác thực • Tính bí mật • An toàn truyền thông • Tính toàn vẹn • Tính che chắn	dữ liệu đầu cuối. • Phân đoạn mạng và thắt chặt an toàn trong vùng cách li (DMZ) nhằm ngăn chặn các đường kết nối có hướng liên kết với các tài sản dữ liệu. • An toàn đăng ký người sử dụng đảm bảo truy cập thông tin quan trọng chỉ được cấp cho người sử dụng xác thực – như sử dụng ủy quyền đăng ký độc lập cho qui trình xử lý. • Xác thực sử dụng chứng thư số, mật khẩu, sinh trắc học hay thẻ thông minh. • Tường lửa và danh sách kiểm soát truy cập để ngăn ngừa truy nhập trái phép. • Kiểm soát truy nhập dựa trên vai trò để hạn chế chức năng người sử dụng được phép thực hiện. • Soát xét bản ghi ứng dụng web để xác định và ngăn chặn tấn công. • Đặt các mức mã hóa thích hợp cho thông tin lưu giữ. • Đảm bảo an toàn giữa trình duyệt và máy chủ web sử dụng các công nghệ như SSLv3/TLS. • An toàn truyền thông dịch vụ web, ví dụ như sử dụng các bản tin SOAP. • Xác minh tính toàn vẹn của dữ liệu/ tệp sử dụng các thuật toán như hàm băm/ kiểm tra tổng, chứng thư. • Đối với ứng dụng web bảo đảm tính toàn vẹn dữ liệu của URL, tập tin cookies hay các thành phần dạng ẩn: o Mã hóa tất cả dữ liệu (thậm chí nếu SSLv3 được sử dụng); o Sử dụng nhãn thời gian với các biến số; o Ký số hay sử dụng hàm băm được khóa cho dữ liệu nhạy cảm. • Sử dụng cổng proxy dự phòng giữa máy chủ web và mạng ngoài.

Các tấn công từ chối dịch vụ	
• Tính sẵn sàng • Tính che chắn	• Vô hiệu hóa các cổng giao thức và dịch vụ không sử dụng nhằm ngăn ngừa chúng trả lời các tín hiệu quét/ thăm dò trái phép có thể gây ra từ chối dịch vụ do tràn ngập lưu lượng. • Loại trừ thông tin mô tả từ các cảnh báo lỗi nhằm ngăn ngừa cung cấp thông tin mục tiêu cho bên tấn công.
Giả mạo nội dung giao dịch	
• Chống chối bỏ	• Các bản ghi chi tiết của giao dịch. • Sử dụng chữ ký số.

10 Các dịch vụ hợp tác nâng cao

10.1 Khái quát

Các tổ chức sử dụng dịch vụ với sự tham gia nhiều nhân viên phải xem xét kịch bản này. Ví dụ của dịch vụ này là:

- Phần mềm nhóm;
- Máy chủ tệp;
- Danh sách thư điện tử;
- Dịch vụ dựa trên nền tảng web.

Các dịch vụ hợp tác nâng cao tích hợp các truyền thông khác nhau và các khả năng chia sẻ tài liệu, là khía cạnh quan trọng cho môi trường kinh doanh. Các dịch vụ điển hình là tích hợp thoại video, thoại truyền thông với các kênh chat, hệ thống thư điện tử, cũng như chia sẻ tài liệu và các môi trường cùng hoạt động trực tuyến.

Có hai phương thức cơ bản sử dụng các dịch vụ này cho tổ chức:

- Chỉ sử dụng chúng như các dịch vụ nội bộ, nhưng có nhược điểm là các dịch vụ không thể sử dụng với đối tác bên ngoài…;
- Sử dụng chúng như các dịch vụ nội bộ và các dịch vụ ra bên ngoài tổ chức. Điều này đưa ra nhiều lợi ích sử dụng dịch vụ hơn, nhưng đồng thời cũng có nhiều rủi ro an toàn liên quan hơn so với chỉ sử dụng nội bộ.

Tương ứng với cách thực hiện, các dịch vụ có thể là:

- Thực thi tại tổ chức;
- Từ bên thứ ba.

Nếu dịch vụ được sử dụng nội bộ và ra bên ngoài, thì việc mua bán trong các dịch vụ hợp tác từ bên thứ ba có thể là giải pháp thích hợp hơn.

Trong mục bên dưới, các nguy cơ an toàn và tư vấn về kỹ thuật thiết kế và kiểm soát an toàn để giảm thiểu các rủi ro liên quan được mô tả cho việc sử dụng nội bộ và nội bộ lẫn ra bên ngoài. Các kiểm soát an toàn áp dụng cho lưu lượng quản lý, báo hiệu và người sử dụng.

10.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan đến dịch vụ hợp tác nâng cao là:

- Truy cập trái phép dẫn đến làm lộ thông tin nhạy cảm:
    - Sử dụng sai các công cụ hợp tác làm chia sẻ bất hợp pháp tài liệu có bản quyền, lấy dữ liệu bảo mật, và tiếp xúc người sử dụng với nội dung không mong muốn hoặc bị lan truyền;
    - Xâm phạm tính che chắn bằng cách giám sát các mẫu sử dụng, phát tán thư rác và các tấn công danh tính.
- Các tấn công bằng virus và đưa ra phần mềm độc hại:
    - Phân bố và thực thi phần mềm độc hại bằng cách khai thác tài nguyên chia sẻ;
- Giảm tính sẵn sàng mạng:
    - Làm quá tải mạng bằng lưu lượng bất hợp pháp;
    - Khai thác các điểm yếu giao thức sử dụng trong dịch vụ hợp tác.

10.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến các dịch vụ hợp tác nâng cao liên quan với:

Bảng 6 – Các kiểm soát an toàn cho các dịch vụ hợp tác nâng cao

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Truy cập trái phép làm lộ thông tin nhạy cảm	
• Kiểm soát truy cập • Xác thực • Tính bí mật • An toàn truyền thông • Chống chối bỏ	• Truy nhập dựa trên vai trò cho các ứng dụng, mạng và lưu trữ. • Gán người sử dụng với các vai trò khác nhau vào các VLAN với các mức cho phép khác nhau. • Các chính sách dựa trên vai trò cho quyền sử dụng và

	truy cập vào tài nguyên, như các ứng dụng mà người sử dụng có thể vận hành. • Danh sách kiểm soát truy cập. • Xác thực và ủy quyền mạnh. • VLAN cho ảo hóa mạng. • IDS dựa trên máy chủ. • Mã hóa dữ liệu.
Các tấn công virus và đưa ra phần mềm độc hại	
• Tính toàn vẹn	• Sử dụng phần mềm truyền hình ảnh màn hình như các máy chủ đầu cuối để giảm tối đa dữ liệu và phần mềm độc hại tiềm năng thâm nhập vào các môi trường hợp tác.
Giảm tính sẵn sàng mạng	
• Tính sẵn sàng	• Sử dụng các mạng cục bộ lưu trữ ảo để tăng tính sẵn sàng và an toàn của dữ liệu. • Ngăn ngừa xóa bỏ thông tin bằng cách sử dụng các công cụ phần mềm ngăn sao chép/dán thông tin, chặn các xâm phạm ghi vào phương tiện có khả năng xóa hay khả năng in. • Phần mềm giám sát để phát hiện vi phạm chính sách – như vi phạm truy cập các ứng dụng và các nguồn tài nguyên mạng khác.

11 Phân đoạn mạng

11.1 Khái quát

Các tổ chức mong muốn phân chia mạng nội bộ thành nhiều miền để gắn kết với cấu trúc tổ chức phải xem xét kịch bản này.

Phân đoạn mạng là kỹ thuật có thể được sử dụng để gia tăng kiểm soát truy cập hệ thống và ứng dụng. Phân đoạn mạng có thể được sử dụng để nhóm các loại hiện có của hoạt động, ứng dụng hay hệ thống theo cách sao cho truy cập chỉ có khả năng cho những người truy cập tới phân đoạn mạng. Bằng cách này, kiểm soát truy cập mạng gia tăng kiểm soát truy cập đầu cuối khác và cung cấp mức bổ sung chống đỡ sâu hơn. Ví dụ, phân đoạn mạng có thể được sử dụng cho:

- Tách riêng các khả năng quản trị và bảo trì ra khỏi chu trình truy cập người sử dụng đến các ứng dụng kinh doanh;
- Tách riêng các ứng dụng quan trọng ra khỏi các ứng dụng khác;
- Tách riêng cơ sở dữ liệu ra khỏi phần lớn người sử dụng.

Đối với các tổ chức đa quốc gia luật pháp cụ thể của từng nước có ảnh hưởng lớn tới các yêu cầu an toàn. Để bao hàm các yêu cầu an toàn thông tin khác nhau cho các nước mà tổ chức quốc tế hoạt động kinh doanh, phân đoạn mạng thực hiện theo biên giới quốc gia có thể là một giải pháp hiệu quả. Ví dụ, luật pháp một quốc gia đặc thù có thể yêu cầu bảo vệ cụ thể cho dữ liệu khách hàng, và không cho phép truyền tải dữ liệu đó sang các nước khác. Điều này thường đòi hỏi các kiểm soát an toàn thông tin bổ sung nhằm bảo đảm tuân thủ luật pháp như vậy.

Trong mục sau các nguy cơ an toàn và tư vấn về các kỹ thuật thiết kế và kiểm soát an toàn để giảm thiểu các rủi ro liên quan được mô tả cho việc sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

11.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan đến phân đoạn mạng để đáp ứng các yêu cầu tuân thủ của đất nước cụ thể trong tổ chức quốc tế là:

- Trách nhiệm pháp lý do không tuân thủ quy định;
- Rò rỉ thông tin:
    - Vi phạm tính bí mật, như khi dữ liệu khách hàng bị truy cập từ các đất nước khác, mà từ chúng không được phép;
    - Vi phạm các yêu cầu riêng tư đặc thù của quốc gia;
    - Các rủi ro liên quan đến uy tín liên can với việc không đáp ứng các mong muốn khách hàng về tính bí mật hay tính che chắn.

11.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến phân đoạn mạng nhằm đáp ứng các yêu cầu tuân thủ của đất nước cụ thể trong tổ chức quốc tế liên quan với:

Bảng 7 – Các kiểm soát an toàn cho phân đoạn mạng

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Trách nhiệm pháp lý do không tuân thủ quy định	
• Tính che chắn • Tính bí mật	• Chính sách và nhận thức người sử dụng o Các luật về tính riêng tư.

	o Các công nghệ mã hóa cho phép. o Các luật về lưu trữ, truyền tải số liệu. o Các luật về ngăn chặn hợp pháp.
Rò rỉ thông tin	
• Kiểm soát truy cập • Xác thực • Tính toàn vẹn	• Cổng an toàn. • Cổng kiểm soát (proxy) mức ứng dụng. • Mã hóa dữ liệu.

12 Hỗ trợ kết nối mạng cho nhà riêng và các văn phòng kinh doanh nhỏ

12.1 Khái quát

Các tổ chức cần cung cấp truy cập nguồn tài nguyên nội bộ cho nhân viên tại nhà riêng hay các văn phòng nhỏ phải xem xét kịch bản này.

Nhà riêng hay các văn phòng nhỏ thường yêu cầu mở rộng mạng nội bộ của doanh nghiệp tới các vị trí của họ. Chi phí mở rộng tới nhà riêng hay các vị trí doanh nghiệp nhỏ là một vấn đề quan trọng, do các phản ánh lợi ích vào chi phí thường không yêu cầu chi phí thực hiện cao. Điều đó có nghĩa là có các giới hạn về chi phí dành cho kiểm soát an toàn được sử dụng để đảm bảo mở rộng mạng như vậy và thường ngăn cản việc sử dụng các kiểm soát an toàn kết nối mạng được thiết lập cho kết nối các phân đoạn Intranet lớn hơn.

Trong nhiều kịch bản nhà riêng hay doanh nghiệp nhỏ, hạ tầng cũng có thể được sử dụng cho các mục đích riêng cũng như kinh doanh – chúng có thể dẫn đến các rủi ro an toàn thông tin phát sinh.

Trong các mục dưới đây, các nguy cơ an toàn và tư vấn về các kỹ thuật thiết kế và kiểm soát an toàn để giảm thiểu các rủi ro liên quan được mô tả cho sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

12.2 Nguy cơ an toàn

Các nguy cơ an toàn liên quan đến hỗ trợ kết nối mạng cho nhà riêng và văn phòng kinh doanh nhỏ là:

- Truy cập trái phép:
    - Thiết lập cấu hình yếu trong thiết bị truy cập mạng, như các bộ định tuyến SOHO (văn phòng nhỏ và văn phòng tại nhà);
    - Sử dụng kỹ thuật đường hầm phân chia (split-tunneling);
    - Kiểm soát an toàn về vật lý bị mất hay yếu;
    - Có nhiều cơ hội hơn do bản chất luôn sẵn sàng của kết nối mạng;

- Sử dụng tài khoản khách và các thiết lập mặc định.

- Tấn công virus và đưa ra phần mềm độc hại:
  - Thiết bị, bao gồm PC sử dụng trong mạng nhà riêng hay văn phòng nhỏ và vận hành với các kiểm soát truy nhập không đầy đủ, như bảo vệ chống phần mềm độc hại bị mất hay yếu …;
  - Các vấn đề xuất phát từ kết hợp các môi trường riêng và doanh nghiệp, ví dụ như sử dụng riêng các giao thức vốn có rủi ro cao, như các giao thức chia sẻ tệp ngang hàng;
  - Vá lỗi thất bại;
  - Một khi đã bị lây nhiễm, tính sẵn sàng có thể bị ảnh hưởng nghiêm trọng do các hoạt động lan truyền virus dẫn đến quá tải mạng.

- Làm lộ trái phép các thông tin nhạy cảm:
  - Thiếu mã hóa dữ liệu lưu trữ trong hệ thống và truyền tải trong mạng nhà riêng hay doanh nghiệp nhỏ;
  - Sử dụng sai các khả năng truy cập như truy cập VLAN trong mạng nhà riêng hay doanh nghiệp nhỏ;
  - Thiếu nhận thức và đào tạo thực tiễn an toàn cho người sử dụng cuối;
  - Hủy bỏ hiệu lực các giả định về bảo vệ mạng Intranet, do các cổng mạng trong môi trường nhà riêng và văn phòng nhỏ không cung cấp mức bảo vệ giống như tại các cổng sử dụng để kết nối các chi nhánh.

12.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến hỗ trợ kết nối mạng cho nhà riêng và các văn phòng kinh doanh nhỏ liên quan với:

Bảng 8 – Các kiểm soát an toàn cho kết nối mạng cho kịch bản nhà riêng và văn phòng kinh doanh nhỏ

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Truy nhập bất hợp pháp	
• Kiểm soát truy nhập • Xác thực • An toàn truyền thông	• Vô hiệu hóa các giao diện và dịch vụ mạng không sử dụng. • Thiết kế và công nghệ bảo vệ cho đường hầm phân chia.

	• Các hệ thống không được sử dụng mật khẩu trắng, không mật khẩu, hay mặc định. • Mật khẩu mạnh phải được bắt buộc cho tất cả người sử dụng. Truy nhập vô danh/khách không được cho phép. • Kiểm tra tuân thủ kỹ thuật để đảm bảo cấu hình và thiết lập đúng cho tất cả thiết bị nhạy cảm an toàn, như bộ định tuyến hay các điểm truy cập WLAN. • Công nghệ mạng riêng ảo an toàn trên các thành phần truy cập mạng như các bộ định tuyến truy cập mạng.
Tấn công virus và đưa ra phần mềm độc hại	
• Tính toàn vẹn • Tính sẵn sàng	• Duy trì phiên bản phần mềm mới nhất và các mức vá lỗi. • Bảo đảm các cập nhật chống virus được cài đặt tự động hoặc người sử dụng được thông báo khi cập nhật sẵn sàng. • Sử dụng hệ thống phát hiện thâm nhập dựa trên máy chủ (HIDS) ít nhất là để phát hiện tính toàn vẹn của phần mềm/cơ sở dữ liệu (nếu có khả năng áp dụng). • Quét tệp và tất cả thông tin lưu giữ đối với các virus, Trojan và các dạng phần mềm độc hại khác. • Sao lưu dữ liệu cấu hình và các tệp cho xử lý sự cố và khôi phục.
Làm lộ bất hợp pháp thông tin nhạy cảm	
• Tính bí mật • Tính che chắn	• Nhận thức và đào tạo người sử dụng sao cho thực hành an toàn tốt nhất. • Mã hóa dữ liệu lưu trữ và truyền tải.

13 Truyền thông di động

13.1 Khái quát

Các tổ chức cho phép sử dụng thiết bị di động cho nhân viên của mình phải xem xét kịch bản này.

Kịch bản này tập trung vào các quan tâm an toàn của doanh nghiệp sử dụng và triển khai các thiết bị và ứng dụng di động. Mặc dù động lực chính của sự phát triển nhanh chóng các tính năng mới của thiết bị di động (như điện thoại thông minh hay thiết bị hỗ trợ dữ liệu cá nhân PDA) đến từ thị

trường tiêu dùng, chúng cũng được sử dụng trong các môi trường nghiệp vụ. Thông thường các thiết bị này là sở hữu cá nhân và được sử dụng cho cả mục đích công việc lẫn cá nhân. Trong một vài trường hợp công ty cung cấp các thiết bị và cho sử dụng cá nhân. Vì vậy, các thiết bị hướng đến thị trường nghiệp vụ cần phải có các đặc tính cho thị trường tiêu dùng, do hãng cung cấp muốn đạt càng nhiều lợi ích kinh doanh càng tốt trong thị trường cạnh tranh.

Các thiết bị truyền thông di động cho phép người sử dụng từ xa đồng bộ cơ sở dữ liệu cá nhân và cung cấp truy cập vào các dịch vụ mạng như thư điện tử, duyệt web, và truy cập Internet không dây. Khi cá nhân sử dụng cùng một thiết bị cho các mục đích kinh doanh cũng như cá nhân, sẽ có xu hướng phá vỡ hay bỏ qua các chính sách sử dụng, do đó tạo ra các rủi ro an toàn thông tin đáng kể cho doanh nghiệp.

Trong mục dưới đây, các nguy cơ an toàn và các tư vấn về các kỹ thuật thiết kế và kiểm soát an toàn nhằm giảm thiểu các rủi ro này được mô tả cho việc sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

13.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan đến thiết bị truyền thông di động là:

- Truy cập bất hợp pháp thông tin lưu giữ trong thiết bị di động do:
    - Kiểm soát hay bảo vệ truy cập thông tin nhạy cảm không đầy đủ;
    - Thiếu nhận thức và mật khẩu không thích hợp;
    - Cấu hình yếu;
    - Tấn công cướp quyền bằng thiết bị giả mạo;
    - Thiếu kiến thức về các yêu cầu bảo vệ an toàn thông tin của người sử dụng cuối, như lẫn lộn thông tin cá nhân và kinh doanh.
- Làm lộ bất hợp pháp dữ liệu nhạy cảm và thông tin vị trí:
    - Các dịch vụ dựa trên vị trí có thể làm lộ thông tin vị trí người sử dụng cho bên thứ ba bất hợp pháp, do đó dẫn đến các liên quan tính riêng tư;
    - Bị nghe lén;
    - Sự tham gia của các bên thứ ba được bảo vệ không đầy đủ trên đường truyền thông;
    - Sử dụng dữ liệu gốc hay các giao thức truyền tải không được bảo vệ đầy đủ;
    - Các thủ tục xử lý không đúng.
- Thay đổi/xóa bỏ bất hợp pháp thông tin lưu trữ (bao gồm phần mềm) do:

- Đưa ra phần mềm độc hại bằng cách cài đặt phần mềm từ các nguồn không được ủy quyền;
- Khai thác các điểm yếu trong hệ điều hành đang hoạt động.

- Thư rác dẫn đến:
  - Tăng cước dịch vụ;
  - Cho phép các tấn công lừa đảo;
  - Các tấn công DoS.
- Bị đánh cắp hay vô ý bị mất, cả hai đều có thể dẫn đến:
  - Mất dữ liệu nhạy cảm được lưu trữ trong thiết bị không được dự phòng ở đâu đó;
  - Các vấn đề về tính bí mật khi dữ liệu nhạy cảm được lưu trữ trong thiết bị không được bảo vệ đầy đủ;
  - Đảm bảo dự phòng dữ liệu.

13.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn thông tin liên quan đến các thiết bị truyền thông di động cá nhân liên quan với:

Bảng 9 – Các kiểm soát an toàn cho kịch bản truyền thông di động

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Truy cập bất hợp pháp thông tin lưu giữ trong thiết bị di động	
• Kiểm soát truy cập • Xác thực • Chống chối bỏ	• Nhận thức của người sử dụng về kiểm soát vật lý. • Tránh các cấu hình lỗi. • Xác thực mạnh. • Cho phép tùy chọn đăng nhập. • Khóa bộ đếm thời gian không hoạt động. • Tường lửa. • Chính sách an toàn tổ chức cho mật khẩu và sử dụng kinh doanh (giới hạn sử dụng cá nhân cho các thiết bị sở hữu của doanh nghiệp).
Làm lộ bất hợp pháp dữ liệu nhạy cảm và thông tin vị trí	

• Tính bí mật • Xác thực • An toàn truyền thông • Tính che chắn	• Mã hóa dữ liệu lưu trữ và truyền tải (không dây). • Bảo vệ mật khẩu. • Tránh các dịch vụ của bên thứ ba mà dịch vụ này yêu cầu văn bản rõ ràng để truy cập vào dữ liệu truyền tải, hoặc nếu không khả thi thì phải đảm bảo rằng tính bí mật của dữ liệu được xử lý theo yêu cầu. • Đảm bảo thủ tục đồng bộ an toàn. • An toàn VPN cho các kết nối truy cập từ xa. • Thủ tục xử lý đúng cho dữ liệu nhạy cảm với xóa bỏ. • Sử dụng tại các vị trí phải có sự đồng ý của người sử dụng.
Thay đổi/xóa bất hợp pháp thông tin lưu trữ (bao gồm phần mềm)	
• Tính bí mật • Tính sẵn sàng • Tính toàn vẹn	• Vô hiệu hóa các giao diện, dịch vụ, ứng dụng không dây không sử dụng. • Vá lỗi bản mới nhất cho OS. • Thủ tục xử lý đúng cho dữ liệu nhạy cảm với xóa bỏ. • Đảm bảo rằng các phiên bản chống virus được cập nhật tự động hay người sử dụng được thông báo khi phiên bản cập nhật sẵn sàng. • Tải về phần mềm chỉ được từ hệ thống phân bố phần mềm doanh nghiệp (tránh cài đặt phần mềm không bản quyền). • Chữ ký số để xác minh nguồn tải về.
Thư rác	
• Kiểm soát truy cập	• Lọc nội dung. • Tăng cường nhận thức người sử dụng.
Mất cắp hay vô ý bị mất	
• Tính bí mật • Tính sẵn sàng	• Quản lý tài sản từ xa (thiết bị vô hiệu hóa/bị khóa). • Dự phòng an toàn định kỳ. • Quản lý tập trung đối với tài sản và tuân thủ chính sách.

14 Hỗ trợ kết nối mạng cho người sử dụng đang di chuyển

14.1 Khái quát

Các tổ chức cho phép nhân viên đang di chuyển truy cập vào tài nguyên doanh nghiệp phải xem xét kịch bản này.

Các giải pháp và đề xuất trong lĩnh vực này thường tập trung trên khía cạnh tính năng và được hướng đến đầu tiên cho thị trường tiêu dùng. Từ quan điểm an toàn thông tin, các mức tính năng đề xuất đưa ra các rủi ro mới, như bởi tác động hay chấm dứt giả định về an toàn thông tin. Ví dụ, giả định về bảo trì Intranet được kiểm soát (từ bên ngoài) và bảo vệ tốt có thể bị nghi vấn nếu truy cập người sử dụng di chuyển vào Intranet không được thực hiện với các kiểm soát thích hợp.

Trong các mục sau các nguy cơ an toàn và tư vấn về các kỹ thuật thiết kế và kiểm soát an toàn để giảm thiểu các rủi ro liên quan được mô tả cho sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

14.2 Các nguy cơ an toàn

Các nguy cơ an toàn liên quan hỗ trợ kết nối mạng cho người sử dụng đang di chuyển là:

- Truy cập bất hợp pháp:
    - Sử dụng sai hỗ trợ mạng người sử dụng từ xa để truy cập trái phép vào Intranet của tổ chức;
    - Thỏa hiệp của cổng an toàn sử dụng trên biên mạng Intranet;
    - Truy cập bất hợp pháp vào dữ liệu lưu giữ trên thiết bị người sử dụng đang di chuyển.
- Giảm tính sẵn sàng của mạng:
    - Các vấn đề tính sẵn sàng được đưa ra khi mong muốn của người sử dụng về hỗ trợ kết nối mạng không thể đáp ứng, như khi điều này phụ thuộc vào tính sẵn sàng của nhà cung cấp dịch vụ Internet.

14.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn liên quan đến hỗ trợ kết nối mạng cho người sử dụng đang di chuyển liên quan với:

Bảng 10 – Các kiểm soát an toàn cho hỗ trợ kết nối mạng cho người sử dụng đang di chuyển

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	**Thiết kế thực hiện và các công nghệ**
Truy cập bất hợp pháp	

• Kiểm soát truy cập • Xác thực • An toàn truyền thông • Tính bí mật	• Nâng cao các kỹ thuật xác thực (chứng thư dựa trên xác thực, xác thực hai yếu tố hay xác thực ứng phó thách thức) • Các dịch vụ dành riêng cho người sử dụng di chuyển dựa trên giao diện web được bảo vệ TLS/SSLv3. • Sử dụng các công nghệ VPN đảm bảo kết hợp với các cổng an toàn thích hợp trên hệ thống khách (như tường lửa cá nhân): o Thực hiện lớp 2/3, như IPSec; o VPN mức ứng dụng, như dựa trên TLS. • Mã hóa dữ liệu người sử dụng lưu trữ.
Giảm tính sẵn sàng của mạng	
• Tính sẵn sàng	• Thuê nhà cung cấp dịch vụ với phạm vi toàn cầu và sử dụng các thỏa thuận mức dịch vụ cho tính tin cậy và hiệu năng.

15 Các dịch vụ thuê ngoài

15.1 Khái quát

Các tổ chức sử dụng các dịch vụ thuê ngoài phải xem xét kịch bản này.

Tổ chức sử dụng các dịch vụ thuê ngoài bởi vì nó được xem như chiến lược kinh doanh hữu hiệu, nhưng nó cũng đưa ra sự phức tạp về tổ chức và vận hành, đặc biệt cho đảm bảo chất lượng và an toàn của các dich vụ thuê ngoài.

Doanh nghiệp được mở rộng kế thừa các rủi ro phát sinh do sự phụ thuộc vào nhà cung cấp dịch vụ. Ví dụ, nhà cung cấp dịch vụ hay nhà sản xuất có thể yêu cầu truy cập trực tiếp vào tài sản bên trong doanh nghiệp để hỗ trợ và/hoặc quản lý các vấn đề sự cố, do đó làm lộ các tài sản quan trọng đối với rủi ro an toàn. Trong khi nhiều dịch vụ hỗ trợ yêu cầu quyền truy cập thường xuyên vào hạ tầng hỗ trợ, nhiều dịch vụ khác có thể chỉ cần truy cập tạm thời. Thông thường các dịch vụ hỗ trợ cần quyền truy cập ưu tiên cao nhằm hoàn thành nhiệm vụ của họ.

Phải yêu cầu các xem xét an toàn và giám sát trong tất cả thỏa thuận hợp đồng không phụ thuộc vào loại kịch bản thuê ngoài. Cách nhìn tổng quan các nguy cơ và liên quan được thể hiện trong tiêu chuẩn này. Thông tin sâu hơn về an toàn các dịch vụ thuê ngoài có thể xem trong ISO/IEC 27036.

Trong các mục dưới đây, các nguy cơ an toàn và các tư vấn về các kỹ thuật thiết kế và kiểm soát an toàn nhằm giảm thiểu các rủi ro này được mô tả cho việc sử dụng nội bộ và nội bộ lẫn ra bên ngoài.

15.2 Nguy cơ an toàn

Các nguy cơ an toàn liên quan đến dịch vụ thuê ngoài là:

- Truy cập bất hợp pháp đến các hệ thống nội bộ khác (khi nhà cung cấp truy cập hệ thống nội bộ để hỗ trợ và bảo trì từ xa):
    - Lạm dụng các cổng bảo trì từ xa;
    - Lạm dụng quyền quản trị.
- Làm lộ bất hợp pháp dữ liệu nhạy cảm bởi nhà cung cấp dịch vụ:
    - Thiếu tôn trọng quyền sở hữu trí tuệ;
    - Thiếu sự phân chia môi trường nhiều khách hàng;
    - Thiếu thực hành an toàn thông tin tốt nhất (ví dụ, chia sẻ mật khẩu có thể bị lan tràn);
    - Xử lý sai phương tiện lưu trữ;
    - Sử dụng các phương thức truyền thông không an toàn.
- Đưa ra phần mềm độc hại (trong các môi trường phát triển phần mềm):
    - An toàn không đầy đủ trong phát triển phần mềm và thủ tục phát hành phần mềm;
    - Truyền tệp và dữ liệu không an toàn;
    - Thực hành hợp tác trực tuyến không an toàn.
- Trách nhiệm pháp lý do không tuân thủ quy định:
    - Thiếu hiểu biết quy định riêng của quốc gia và trách nhiệm pháp luật nếu nhà cung cấp dịch vụ ở tại quốc gia khác;
    - Tính riêng tư dữ liệu hợp pháp và các yêu cầu bảo vệ áp dụng trong quốc gia mà nhà cung cấp có mặt là không đủ; điều này có thể gây hiệu quả bất lợi nghiêm trọng đến tính riêng tư dữ liệu và các yêu cầu bảo vệ áp dụng cho bên mua hàng.

15.3 Kỹ thuật thiết kế và kiểm soát an toàn

Các kỹ thuật thiết kế và kiểm soát an toàn thông tin liên quan đến các dịch vụ ngoài và thuê ngoài liên quan với:

Bảng 11 – Các kiểm soát an toàn cho các dịch vụ thuê ngoài

Các đặc tính an toàn có khả năng áp dụng cho các nguy cơ xác định	Thiết kế thực hiện và các công nghệ
Truy cập bất hợp pháp vào các hệ thống nội bộ	
• Kiểm soát truy cập • Xác thực • Chống chối bỏ	• Gán nghiêm ngặt ID dữ liệu cá nhân. • Xác thực mạnh (như xác thực hai yếu tố) cho đăng nhập gốc/quản trị. • Cổng thiết bị nhập liệu tại chỗ hay cổng thủ công được bảo vệ bằng ID người sử dụng và mật khẩu (trong trường hợp nhà cung cấp dịch vụ yêu cầu truy cập vật lý tại chỗ). • Ghi lại toàn bộ các hoạt động truy cập và soát xét bản ghi.
Làm lộ bất hợp pháp dữ liệu nhạy cảm	
• Tính bí mật	• Thực hành bảo vệ dữ liệu khách hàng tốt nhất thông qua mã hóa. • Nhận thức và đào tạo về an toàn. • Giám sát và kiểm định phương tiện và thủ tục. • Chính sách an toàn và hướng dẫn thủ tục theo thỏa thuận.
Đưa ra phần mềm độc hại	
• Tính toàn vẹn	• An toàn thực hành mã hóa. • Thay đổi các quá trình quản lý. • Đảm bảo rằng các phiên bản chống virus được cập nhật tự động hay người sử dụng được thông báo khi phiên bản cập nhật sẵn sàng.
Trách nhiệm pháp lý do không tuân thủ quy định	
• Tính bí mật • Tính che chắn	• Nhận thức các quy định nội bộ. • Sử dụng phần mềm mã hóa thích hợp. • Cơ cấu che chắn (IPSec VPN).

Phụ lục A

(Tham khảo)

Ví dụ về chính sách sử dụng Internet

A.1 Tổng quan

Mục đích của an toàn thông tin trong việc ban hành chính sách sử dụng được chấp thuận là không áp đặt các hạn chế mâu thuẫn với văn hóa Công ty đã được thiết lập về tính mở, tính tin cậy và tính toàn vẹn. An toàn thông tin được cam kết để bảo vệ nhân viên, đối tác của Công ty đối với các hành động bất hợp pháp hay có hại do các cá nhân cố ý hay vô tình gây ra.

Các hệ thống liên quan Internet/Intranet/Extranet, bao gồm (nhưng không giới hạn) thiết bị máy tính, phần mềm, hệ điều hành, phương tiện lưu trữ, tài khoản mạng cung cấp thư điện tử, trình duyệt WWW, và FTP, do Công ty sở hữu. Các hệ thống này được sử dụng cho các mục đích nghiệp vụ phục vụ cho lợi ích của công ty và của khách hàng trong quá trình điều hành thông thường. Các chi tiết xem trong chính sách nguồn nhân lực.

An toàn hiệu quả là một nỗ lực tập thể với sự tham gia và hỗ trợ của mỗi nhân viên và chi nhánh Công ty là những người liên quan đến thông tin và/hoặc hệ thống thông tin. Trách nhiệm của mỗi người sử dụng máy tính là phải biết các hướng dẫn này và thực hiện các hoạt động của họ phù hợp.

A.2 Mục đích

Mục đích của chính sách này là phác thảo việc sử dụng được chấp thuận cho các thiết bị máy tính tại Công ty. Các quy tắc được thực hiện để bảo vệ nhân viên và Công ty. Việc sử dụng không thích hợp làm cho Công ty đối mặt với rủi ro bao gồm các tấn công virus, thỏa hiệp hệ thống mạng và dịch vụ, và các vấn đề pháp lý.

A.3 Phạm vi

Chính sách này áp dụng cho các nhân viên, nhà thầu, nhà tư vấn, nhân viên tạm thời và những lao động khác tại Công ty, bao gồm tất cả các cá nhân liên kết với bên thứ ba. Chính sách này áp dụng cho tất cả thiết bị Công ty sở hữu hay thuê lại.

A.4 Chính sách

A.4.1 Sử dụng chung và quyền sở hữu

1. Khi quản trị mạng Công ty mong muốn cung cấp mức độ hợp lý tính che chắn, người sử dụng phải nhận thức rằng dữ liệu mà họ tạo ra trên các hệ thống công ty là tài sản của Công ty. Vì sự cần thiết phải bảo vệ mạng Công ty, việc quản lý không thể bảo đảm tính bí mật của thông tin lưu trữ trong bất kì thiết bị mạng nào thuộc Công ty.

2. Các nhân viên có trách nhiệm thực hiện phán quyết về tính hợp lý của sử dụng cá nhân. Các bộ phận riêng có trách nhiệm thiết lập hướng dẫn liên quan đến sử dụng cá nhân của hệ thống Internet/Intranet/Extranet. Nếu không có các chính sách này, nhân viên phải được hướng dẫn bằng các chính sách của bộ phận về sử dụng cá nhân, và nếu có bất cứ điều gì không chắc chắn, nhân viên phải tư vấn cấp trên hoặc người quản lý.
3. An toàn thông tin khuyến nghị rằng bất cứ thông tin nào người sử dụng cho là nhạy cảm hay bị yếu cần phải được mã hóa. Để chỉ dẫn phân loại thông tin, xem Chính sách nhạy cảm thông tin của an toàn thông tin. Đối với các chỉ dẫn mã hóa thư điện tử và tài liệu, xem Nhận thức an toàn thông tin.
4. Đối với các mục đích an toàn và bảo trì mạng, các cá nhân có thẩm quyền trong Công ty có thể giám sát thiết bị, hệ thống và lưu lượng mạng tại bất cứ thời điểm nào, dựa trên Chính sách kiểm định an toàn thông tin.
5. Công ty có quyền kiểm định mạng định kì để đảm bảo tuân thủ với chính sách này.

A.4.2 An toàn và thông tin thích hợp

1. Giao diện người sử dụng đối với thông tin chứa trong các hệ thống liên quan Internet/Intranet/Extranet phải được phân loại hoặc bảo mật hoặc không bảo mật, như đã được xác định trong hướng dẫn tính bí mật công ty, chi tiết của chúng có thể xem trong Chính sách nguồn nhân lực. Ví dụ về thông tin bảo mật, bao gồm (nhưng không giới hạn): tính riêng tư của công ty, chiến lược của công ty, nhạy cảm với đối thủ cạnh tranh, bí mật thương mại, các đặc tính, danh sách khách hàng, và dữ liệu nghiên cứu. Các nhân viên phải thực hiện tất cả các bước cần thiết để ngăn ngừa truy cập bất hợp pháp vào các thông tin này.
2. Giữ mật khẩu an toàn và không chia sẻ tài khoản. Người sử dụng hợp pháp có trách nhiệm giữ an toàn mật khẩu và tài khoản của mình. Các mật khẩu mức hệ thống phải được thay đổi hàng quí, các mật khẩu mức người sử dụng phải thay đổi sáu tháng một lần.
3. Tất cả các PC, máy tính xách tay và máy chủ phải được an toàn sử dụng bảo vệ màn hình. Màn hình được bảo vệ bằng mật khẩu với chế độ hoạt động tự động thiết lập 10 phút hay nhỏ hơn, hoặc bằng cách thoát khỏi đăng nhập (control-alt-delete cho người sử dụng Win2000) khi máy chủ không được giám sát.
4. Sử dụng mã hóa thông tin tuân thủ theo Chính sách sử dụng mã hóa được chấp thuận của an toàn thông tin.
5. Vì rằng thông tin chứa trong máy tính cá nhân là đặc biệt dễ bị tổn thương, cần phải quan tâm đặc biệt. Bảo vệ máy tính xách tay tuân theo Thủ thuật an toàn máy tính xách tay.
6. Việc gửi thông tin của nhân viên từ địa chỉ thư điện tử Công ty tới các nhóm tin tức phải chứa các từ chối trách nhiệm tuyên bố rằng các ý kiến trình bày chỉ giới hạn cho bản thân

họ và không liên quan đến Công ty, trừ phi việc gửi đi nằm trong quá trình thực hiện nhiệm vụ kinh doanh.

7. Tất cả các máy chủ sử dụng bởi nhân viên được kết nối Internet/Intranet/Extranet của Công ty, bất kể được sở hữu bởi nhân viên hay Công ty, phải liên tục tiến hành nâng cấp phần mềm quét virus với cơ sở dữ liệu virus mới nhất trừ phi vượt qua chính sách của bộ phận hay công ty.
8. Nhân viên phải sử dụng lưu ý đặc biệt khi mở tệp gắn theo thư điện tử nhận được từ người gửi không rõ, nó có thể chứa virus, bom thư, hay mã Trojan.

A.4.3 Sử dụng không được chấp thuận

Các hoạt động sau nói chung là bị cấm. Nhân viên có thể được miễn trừ các hạn chế này trong quá trình thực thi trách nhiệm công việc hợp pháp (như bộ phận quản trị hệ thống có thể cần vô hiệu hóa truy cập mạng của máy chủ nếu máy chủ đó làm gián đoạn dịch vụ cung cấp).

Trong bất cứ trường hợp nào cũng không thể cho phép nhân viên của Công ty được ủy quyền tham gia bất cứ hoạt động bất hợp pháp nào theo luật địa phương, quốc gia hay quốc tế khi sử dụng các nguồn tài nguyên sở hữu bởi Công ty.

Danh sách dưới đây chưa phải là hoàn chỉnh, nhưng cố gắng cung cấp khung cho các hoạt động được đưa vào thể loại sử dụng không được chấp thuận.

A.4.3.1 Các hoạt động hệ thống và mạng

Các hoạt động sau bị cấm nghiêm ngặt, không có loại trừ:

1. Vi phạm quyền của bất cứ cá nhân hay công ty được bảo vệ bởi quyền sở hữu trí tuệ đối với quyền tác giả, bí mật thương mại, bằng sáng chế và các sở hữu trí tuệ khác, hoặc các luật hay quy định tương tự, bao gồm (nhưng không chỉ giới hạn) đối với cài đặt hay phân tán các sản phẩm phần mềm vi phạm bản quyền hay các sản phẩm phần mềm khác không có giấy phép sử dụng của Công ty.
2. Sao chép bất hợp pháp tài liệu có quyền tác giả bao gồm (nhưng không giới hạn) số hóa và phân tán ảnh từ tạp chí, sách hoặc các nguồn có bản quyền tác giả khác, âm nhạc có bản quyền, và cài đặt bất cứ phần mềm bản quyền nào mà Công ty hay người sử dụng cuối không có giấy phép hợp lệ là tuyệt đối bị cấm.
3. Xuất khẩu các phần mềm, thông tin kỹ thuật, phần mềm hay công nghệ mã hóa, vi phạm luật kiểm soát xuất khẩu vùng hay quốc tế, là bất hợp pháp. Phải tư vấn bộ phận quản lý thích hợp trước khi xuất ra bất cứ tài liệu nào còn nghi ngờ.
4. Đưa các chương trình độc hại vào mạng hay máy chủ (như virus, sâu, Trojan, bom thư…).

5. Tiết lộ mật khẩu tài khoản của mình cho người khác hay cho phép người khác sử dụng tài khoản của mình. Điều này bao gồm cả người trong gia đình khi công việc được thực hiện tại nhà riêng.
6. Sử dụng tài sản tính toán của Công ty để tham gia mua sắm hay truyền tải tài liệu vi phạm văn hóa hay đối nghịch luật lệ nơi làm việc trong thẩm quyền địa phương người sử dụng.
7. Đưa ra các cung cấp giả dối về sản phẩm, linh kiện, hay các dịch vụ xuất phát từ bất cứ tài khoản nào của Công ty.
8. Công bố về bảo đảm, rõ ràng hay ám chỉ, trừ phi là một phần của nhiệm vụ thực thi thông thường.
9. Tác động vi phạm an toàn hay làm gián đoạn truyền thông mạng. Vi phạm an toàn bao gồm (nhưng không giới hạn) truy cập dữ liệu nhân viên không phải là người nhận dự kiến hay đăng nhập vào máy chủ hay tài khoản mà nhân viên rõ ràng không được quyền truy nhập, trừ phi các nhiệm vụ thực thi trong phạm vi công việc thường xuyên. Trong phần này, 'làm gián đoạn' bao gồm (nhưng không giới hạn) nghe lén mạng, tràn ngập bằng thăm dò, giả mạo gói tin, từ chối dịch vụ, và thông tin định tuyến giả mạo cho các mục đích có hại.
10. Quét cổng hay quét an toàn bị cấm hiển nhiên trừ phi thiết lập trước thông báo cho An toàn thông tin.
11. Thực hiện bất cứ dạng giám sát mạng nào ngăn chặn dữ liệu không dành cho máy chủ nhân viên, trừ phi hoạt động này là một phần của nhiệm vụ thực thi công việc thông thường của nhân viên.
12. Phá vỡ xác thực người sử dụng hoặc an toàn của bất cứ máy chủ, mạng hay tài khoản nào.
13. Can thiệp hay từ chối dịch vụ tới bất kì người sử dụng nào khác với máy chủ nhân viên (ví dụ, tấn công từ chối dịch vụ).
14. Sử dụng bất cứ chương trình/đoạn mã/lệnh hoặc gửi bản tin bất cứ dạng nào, với mục đích can thiệp, hoặc vô hiệu hóa phiên đầu cuối người sử dụng, thông qua bất cứ phương tiện cục bộ nào hay thông qua Internet/Intranet/Extranet.
15. Cung cấp thông tin về các nhân viên Công ty, hay danh sách của các nhân viên Công ty cho các bên ngoài Công ty.

A.4.3.2 Các hoạt động thư điện tử và truyền thông

1. Gửi các bản tin thư điện tử không mong muốn, bao gồm gửi thư rác hay các tài liệu quảng cáo khác tới các cá nhân không yêu cầu tài liệu này (thư rác - spam).

2. Bất cứ hình thức quấy rối nào thông qua thư điện tử, điện thoại hay nhắn tin, bất kể qua ngôn ngữ, tần số, hay độ dài bản tin.
3. Sử dụng bất hợp pháp hay giả mạo thông tin tiêu đề thư điện tử.
4. Chào mời gửi thư điện tử cho bất cứ địa chỉ thư khác nào mà khác với tài khoản đã đăng ký, với ý định làm phiền hay thu thập các trả lời.
5. Tạo ra hay chuyển tiếp thư chuỗi, sơ đồ Ponzi hay kim tự tháp bất cứ dạng nào.
6. Sử dụng thư điện tử không mong muốn xuất phát từ bên trong mạng Công ty của nhà cung cấp dịch vụ Internet/Intranet/Extranet khác nhằm đại diện hay để quảng bá bất cứ dịch vụ nào do Công ty sở hữu hay kết nối qua mạng Công ty.
7. Đăng tải các bản tin không liên quan đến nghiệp vụ giống nhau hay tương tự nhau cho số lượng lớn các nhóm tin sử dụng Net (thư rác nhóm tin).

A.4.4 Viết blog

Blog là tạp chí trực tuyến cá nhân được thường xuyên cập nhật và hướng đến công chúng nói chung.

1. Viết blog bởi nhân viên, bất kể sử dụng tài sản và hệ thống Công ty hay hệ thống máy tính cá nhân, cũng là đối tượng cho các điều khoản và hạn chế để thiết lập quy định trong chính sách này. Sử dụng hạn chế hệ thống Công ty để tham gia viết blog được chấp thuận, với điều kiện nó được thực hiện một cách chuyên nghiệp và có trách nhiệm, không vi phạm chính sách Công ty, không có hại cho lợi ích Công ty, và không cản trở thực thi nhiệm vụ thông thường của nhân viên. Viết blog từ hệ thống Công ty cũng là đối tượng của giám sát.
2. Chính sách thông tin bảo mật Công ty cũng áp dụng cho viết blog. Như nhân viên bị cấm làm lộ bất cứ thông tin bảo mật hay thông tin tương ứng của Công ty, bí mật thương mại hay bất cứ tài liệu nào khác được đưa ra trong Chính sách thông tin bảo mật Công ty khi tham gia viết blog.
3. Nhân viên không được tham gia viết bất cứ blog nào có thể gây hại hay làm hoen ố hình ảnh, danh tiếng và/hoặc thiện chí của Công ty và/hoặc bất cứ nhân viên nào của Công ty. Nhân viên cũng bị cấm bình luận phân biệt đối xử, gièm pha, nói xấu hay quấy rối khi viết blog hay tham gia thực hiện các điều bị cấm trong Chính sách của Công ty.
4. Nhân viên cũng không được gắn các tuyên bố, ý kiến hay tín ngưỡng cá nhân cho Công ty khi tham gia viết blog. Nếu nhân viên thể hiện tín ngưỡng và/hoặc ý kiến của họ trên blog, nhân viên có thể không thể hiện bản thân như nhân viên hay đại diện của Công ty, một cách rõ ràng hay ngụ ý. Các nhân viên tự đương đầu bất cứ rủi ro nào hay tất cả rủi ro liên quan đến viết blog.

5. Ngoài các luật liên quan đến xử lý và làm lộ tài liệu được kiểm soát bản quyền hoặc kiểm soát xuất ra, nhãn hiệu hàng hóa, biểu trưng của Công ty, và các sở hữu trí tuệ khác của Công ty cũng có thể không được sử dụng liên quan đến bất cứ hoạt động viết blog nào.

A.5 Thi hành

Bất cứ nhân viên nào bị phát hiện vi phạm chính sách này có thể là đối tượng phạt kỉ luật, bao gồm cả cho thôi việc.

Phụ lục B

(Tham khảo)

Danh mục các nguy cơ

B.1 Thể hiện không đúng thẩm quyền và quyền

- Trình diễn thẩm quyền giả như thể nó thực sự với ý định gây nhầm lẫn.
- Trình diễn mật khẩu, khóa hay chứng thư của người khác (như người quản trị hệ thống).
- Yêu cầu và sử dụng bất hợp pháp thông tin xác thực liên quan dịch vụ thuê bao (như id/mật khẩu người sử dụng, khóa phiên). Hạn chế thuê bao cá nhân.
- Yêu cầu và sử dụng bất hợp pháp thông tin xác thực quản trị (như id/mật khẩu người sử dụng).
- Tấn công lặp lại liên quan đến báo hiệu.

B.2 Đánh cắp dịch vụ

- Hưởng lợi trái pháp luật từ nhà cung cấp dịch vụ với ý định tước đoạt lợi nhuận hợp pháp.
- Lừa gạt nhà cung cấp dịch vụ.
- Xóa hay sửa đổi thông tin cước phí bất hợp pháp.
- Sao chép thiết bị.
- Gian lận hệ thống truy cập có điều kiện (CAS).
- Nhân rộng/phổ biến ồ ạt thông tin cho phép đánh cắp dịch vụ.

B.3 Xâm phạm tính riêng tư thuê bao và nghe trộm

- Truy vết mẫu dạng cuộc gọi nhằm phát hiện danh tính, liên kết, sự hiện diện và sử dụng.
- Bắt giữ lưu lượng – ghi lại bất hợp pháp lưu lượng bao gồm ghi lại gói tin, đăng nhập gói tin và rình mò gói tin. Bao gồm lưu lượng quản lý và báo hiệu.
- Truy cập bất hợp pháp vào dòng phương tiện thuê bao.
- Truy cập bất hợp pháp vào vận hành, quản trị, quản lý và cung cấp (OAM&P) lưu lượng.
- Truy cập bất hợp pháp vào lưu lượng báo hiệu.
- Khai thác thông tin – phương tiện bất hợp pháp bắt giữ danh tính cho phép truyền thông bất hợp pháp tiếp theo và đánh cắp thông tin. Bao gồm tập hợp các ID, có thể là số, chuỗi ký tự, URL,…

- Tái tạo lại phương tiện – giám sát, ghi lại, lưu trữ, tái tạo, nhận biết, diễn giải, dịch, và/hoặc trích lấy các đặc tính của bất cứ phần nào của truyền thông video bao gồm danh tính, sự hiện diện hay trạng thái.
- Làm lộ bất hợp pháp khả năng dịch vụ thuê bao.
- Làm lộ bất hợp pháp sử dụng hay hoạt động trước và hiện thời của thuê bao (như lịch sử xem nội dung truyền hình hay VoD của thuê bao, các hoạt động chơi game trực tuyến…).
- Các tấn công lặp lại liên quan đến phương tiện (phát lại phương tiện bắt giữ với mục tiêu thu lợi có hại, xâm phạm tính riêng tư bằng cách phát lại phương tiện cho sử dụng cá nhân).

B.4 Ngăn cản và thay đổi

- Mạo danh và chiếm cuộc gọi – xâm nhập, xóa, thêm vào, loại bỏ, thay thế hay bất cứ thay đổi của bất kì phần nào của truyền thông với thông tin làm sửa đổi bất cứ nội dung và/hoặc danh tính, sự hiện diện hay trạng thái của bất kì bên nào. Bao gồm lưu lượng quản lý và báo hiệu.
- Truy nhập bất hợp pháp, thay đổi, hay xóa thông tin số.
- Chiếm dòng lưu lượng; chèn vào, thay đổi và xóa dòng dữ liệu bằng cách bất hợp pháp.
- Bất cứ dạng nào của thư rác.
- Truyền tải tài liệu bất hợp pháp (cho lý do chính trị hay lý do khác).

B.5 Tràn ngập lưu lượng/ gói tin

- Tấn công DoS vào điểm cuối người sử dụng bằng cách gửi số lượng lớn gói tin hợp lệ gây ra gián đoạn dịch vụ, một số có thể cũng có tác động đến các thành phần mạng. Ứng dụng bị dừng do quá tải.
- Các kịch bản tràn ngập gói tin từ điểm cuối làm cho thành phần mạng, hay máy chủ sụp đổ, khởi động lại, hay kiệt quệ toàn bộ tài nguyên.
- DoS – tiêu tốn băng thông hay tài nguyên; lượng lưu lượng lớn (ví dụ như tới nhóm đa điểm).
- Có khả năng tác động tới hàng nghìn thuê bao (ví dụ như DSLAM, máy chủ hỗ trợ hàng nghìn thuê bao).

B.6 Gói tin và bản tin bị thay đổi

- Vô hiệu hóa điểm cuối với các bản tin không hợp lệ - tấn công DoS trên điểm cuối (ví dụ như các máy chủ) bằng cách gửi số lượng lớn các bản tin không hợp lệ có thể làm cho điểm cuối sụp đổ, khởi động lại, hay kiệt quệ toàn bộ tài nguyên.

- Thay đổi giao thức bản tin – gửi các bản tin giao thức bị thay đổi (ví dụ như các bản tin tràn trên hay tràn dưới) tới thiết bị làm giảm hiệu năng của nó xuống dưới điểm có khả năng xử lý bản tin bình thường.
- Các bản tin bị biến đổi gây tràn bộ đệm.
- Có khả năng tác động tới hàng nghìn thuê bao (ví dụ như máy chủ hỗ trợ hàng nghìn thuê bao).

B.7 Các bản tin giả mạo

- Tấn công DoS gián đoạn dịch vụ bằng cách gây ra kết thúc phiên sớm.
- Giả mạo các bản tin điều khiển. Lưu lượng điều khiển có hại – xâm nhập vào truyền thông làm cho ứng dụng hay máy chủ bị trục trặc hoặc gửi lưu lượng đến đích sai. Các bản tin điều khiển giả mạo được sử dụng để thay thế cấu trúc hình cây phân bố đa điểm và tác động đến phân bố dữ liệu qua chúng. DoS – bản tin phát quảng bá giả tuyên bố đang có tỉ lệ mất gói cao trên kênh hoặc bị tắc nghẽn cao; nguồn sẽ giảm tốc độ truyền làm ảnh hưởng đến thuê bao khác.
- Giả mạo bản tin sử dụng cuối và ứng dụng hay trả lời của máy chủ.
- Thay đổi địa chỉ IP và MAC để giả mạo địa chỉ IP và MAC người sử dụng khác nhằm bắt giữ dòng dữ liệu.

B.8 DoS nền tảng cơ bản

- Các điểm yếu của hệ điều hành hay phần cứng cơ bản mà ứng dụng hay dịch vụ chạy trên nó.
- Khai thác "point-and-shoot" sẵn sàng cho việc tải về tự do trên mạng.
- Các tấn công DoS làm giảm hiệu năng thiết bị.
- Khai thác các điểm yếu này có khả năng lan truyền đến hàng nghìn thiết bị (ví dụ như các thiết bị khách hàng). Có khả năng dẫn đến triển khai lại hay bảo trì hàng nghìn thiết bị.

B.9 Thỏa hiệp của phần mềm cài đặt, dữ liệu liên quan dịch vụ, hay cấu hình hệ thống

- Chèn phần mềm độc hại, phần mềm gián điệp, hay chương trình rootkit (Rootkit là một bộ công cụ phần mềm do kẻ xâm nhập đưa vào máy tính nhằm mục đích cho phép quay lại xâm nhập máy tính đó và dùng nó cho các mục đích xấu mà không bị phát hiện, bộ công cụ này cho phép truy nhập vào hoạt động của máy tính ở mức căn bản nhất).
- Sao chép, cài đặt, thay thế, xóa bất hợp pháp phần mềm và các tệp cấu hình.
- Sao chép, làm lộ, tạo ra, thay thế, xóa bất hợp pháp dữ liệu liên quan dịch vụ (ví dụ như đăng nhập hệ thống, thông tin cước, khóa mã, ổ chứa lưu trữ cho các khóa mã …).

- D-DoS sử dụng thiết bị thỏa hiệp làm sụp đổ dịch vụ.
- Tạo ra hay thay đổi bất hợp pháp thông tin liên quan dịch vụ thuê bao (ví dụ như thông tin xác thực, khóa phiên).
- Kích hoạt/chấm dứt hoạt động các cổng (giao thức) lôgic một cách bất hợp pháp hay không cần thiết.

B.10 Làm kiệt quệ nguồn tài nguyên

- Thiếu sót trên phần mềm hay phần cứng gây ra cạn kiệt tài nguyên bộ nhớ (ví dụ như bộ đệm) trong hệ thống.
- Thiếu sót trên phần mềm hay phần cứng tiêu thụ phần lớn tài nguyên CPU trong hệ thống.
- Lỗi phần cứng hay phần mềm hạn chế băng thông sẵn sàng của đường liên kết truyền thông.
- Thiếu sót trên phần mềm hay phần cứng tạo ra các bản tin không cần thiết làm giảm tài nguyên băng thông.
- Các ví dụ như vòng lặp vô hạn phần mềm, vòng lặp định tuyến.

B.11 Quét và dò tìm mạng bất hợp pháp

- Quá trình quét/ping cổng. Bên tấn công có thể chạy phần mềm quét công cộng sẵn có trên máy chủ có nối mạng. Các dịch vụ máy chủ trên thiết bị giám sát cổng sẽ trả lời, có khả năng cung cấp thông tin cho bên tấn công.
- Quét điểm yếu (như nessus), ánh xạ mạng (như NMAP). Bên tấn công có thể chạy phần mềm quét công cộng sẵn có trên máy chủ có nối mạng yêu cầu cấu hình thiết bị và topo mạng.
- Truy cập từ xa bất hợp pháp vào phần mềm hay chức năng trên thiết bị (ví dụ như sử dụng rootkit cung cấp cửa cho Trojan).

B.12 Thỏa hiệp của dữ liệu ứng dụng thuê bao

- Làm lộ, tạo ra, thay thế, sao chép, xóa bất hợp pháp dữ liệu được tạo ra và/hoặc được sử dụng bởi các ứng dụng thuê bao có khả năng truy cập.
- Bao hàm thông tin lưu trữ trong mạng nhà cung cấp dịch vụ đại diện cho thuê bao (ví dụ như nội dung video được ghi bằng nDVD).

B.13 Đánh cắp nội dung

- Bắt giữ chứng thư số để yêu cầu nội dung và thậm chí quảng bá/phân bố lại luồng đến các thuê bao khác.
- Bắt giữ gói tin tại mạng nhà và mạng con IP.

- Lấy ra từ cổng ra tương tự gửi tới thiết bị ghi chép bên ngoài.
- Lấy ra từ cổng ra số gửi tới thiết bị ghi chép bên ngoài.
- Thực hiện phát nhiều hơn so với số lượng cho phép.
- Truy cập nội dung trái pháp luật (ví dụ như nội dung bị đánh cắp).
- Gian lận hệ thống truy cập có điều kiện (CAS).
- Sao chép nội dung từ đĩa lưu trữ trên máy chủ hay thiết bị người sử dụng cuối.

B.14 Truy cập vào nội dung không thích hợp

- Truy cập vô tình.
- Truy cập cố ý.

B.15 Thỏa hiệp thông tin thuê bao

- Khai thác xã hội để lấy thông tin thuê bao.
- Làm lộ, tạo ra, thay thế, sao chép, hay xóa bất hợp pháp dữ liệu thuê bao (ví dụ như địa chỉ, số điện thoại, thông tin thẻ tín dụng, đăng nhập DNS/ENUM …).
- Giới hạn thành thuê bao cá nhân.

B.16 Chiếm điều khiển phiên và giả dạng dịch vụ

- Mạo nhận nhà cung cấp dịch vụ hợp pháp. Bắt giữ chứng thư số từ nhà cung cấp để thay đổi luồng và bất cứ thông tin nào họ muốn.
- Mạo nhận thiết bị mạng, máy chủ video, máy chủ game, máy chủ DRM hợp pháp.
- Tấn công người ở giữa (MITM).
- Chuyển hướng luồng video sang thiết bị bất hợp pháp.

B.17 Quản lý bất hợp pháp

- Sử dụng bất hợp pháp ứng dụng ban quản lý hay thực hiện các lệnh quản lý. Ví dụ, điều khiển cấu hình modem để chặn các dịch vụ cụ thể.
- Các bản tin giao thức quản lý giả mạo/bị thay đổi. Ví dụ, điều khiển cấu hình modem để chặn hay cho phép giao thức cụ thể (như SNMP).
- Thay đổi các bản tin quản lý từ xa (như MITM).
- Các hoạt động tự cung cấp trái pháp luật của thuê bao. Ví dụ, cấu hình lại STB nhằm loại bỏ giới hạn băng thông để tạo kết nối chậm cho các thuê bao khác hay tăng băng thông cho bản thân mình.
- Tác nhân quản lý hợp pháp thực hiện các hành động bất hợp pháp.

- Quản lý nội dung bất hợp pháp, ví dụ như tải về, xóa nội dung hay thay đổi ngày kích hoạt (ngày mà nội dung trở nên sẵn sàng cho xem rộng rãi).
- Quản lý thuê bao bất hợp pháp, ví dụ như các hoạt động cung cấp cho thuê bao bất hợp pháp bao gồm tăng/ giảm quyền ưu tiên của thuê bao.
