UỶ BAN CHỨNG KHOÁN NHÀ NƯỚC

ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CẤP CƠ SỞ

GIẢI PHÁP NHẰM NÂNG CAO TÍNH AN TOÀN CHO HỆ THỐNG MÁY TÍNH TẠI TRUNG TÂM GIAO DỊCH CHỨNG KHOÁN

MÃ SỐ ĐĂNG KÝ: CS-03

Đơn vị chủ trì: **Trung tâm Giao dịch Chứng khoán Hà Nội**

Chủ nhiệm đề tài: **Đỗ Đức Mạnh**

HÀ NỘI - 2004

THÀNH VIÊN THAM GIA
NGHIÊN CỨU KHOA HỌC ĐỀ TÀI CẤP CƠ SỞ

Đề tài: Giải pháp nhằm nâng cao tính an toàn cho hệ thống máy tính tại Trung tâm giao dịch chứng khoán

Chủ nhiệm đề tài:	***CN. Đỗ Đức Mạnh***
Thư ký đề tài:	***CN. Vũ Phúc Toàn***
Thành viên khác:	***CN. Nguyễn Việt Hà***

Mục Lục

LỜI MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong giai đoạn đầu phát triển của ngành chứng khoán Việt Nam, các trung tâm giao dịch chứng khoán chiếm một vị trí đặc biệt quan trọng, là đơn vị trực tiếp tổ chức và quản lý hoạt động giao dịch chứng khoán. Hầu hết tất cả mọi quy trình nghiệp vụ, thông tin, tài liệu đều được tin học hoá và có mức độ nhạy cảm rất cao.

Đặc biệt, trung tâm giao dịch chứng khoán Hà Nội sắp đưa vào vận hành hệ thống tin học phục vụ giao dịch chứng khoán. Bên cạnh yếu tố về trang thiết bị phần cứng và phầm mềm giao dịch, ngay từ bây giờ hệ thống phải được phân tích, đánh giá rủi ro một cách toàn diện, từ đó đưa ra giải pháp bảo đảm an toàn hệ thống thật hoàn chỉnh. Chúng ta cần có một đề tài khoa học làm cơ sở cho hoạt động này.

Tuy nhiên, trong giai đoạn hiện nay, việc đảm bảo an ninh cho hệ thống giao dịch chứng khoán tại TTGDCK Trái phiếu HCM còn có rất nhiều bất cập và hạn chế do nhiều lý do như sự tích hợp chưa cao giữa phần mềm hệ thống giao dịch với các phần mềm ứng dụng khác, cấu hình thiết bị, các lý do về an toàn, bảo mật dữ liệu cho toàn bộ hệ thống máy tính của Trung tâm Giao dịch Chứng khoán (TTGDCK) ...

Đề tài tập trung nghiên cứu các vấn đề liên quan đến hiện trạng an ninh hệ thống tại TTGDCK và đưa ra các giải pháp nhằm tăng cường an ninh cho hệ thống nhằm nâng cao hiệu quả quản lý, điều hành, các hoạt động mua bán chứng khoán tại TTGDCK, đảm bảo cho thị trường chứng khoán hoạt động có tổ chức, an toàn, công khai, công bằng và hiệu quả, bảo vệ quyền lợi hợp pháp của người đầu tư.

2. Tình hình nghiên cứu trong và ngoài nước

Cho đến nay, đã có rất nhiều công trình nghiên cứu khoa học được triển khai về vấn đề an toàn hệ thống và thực tế cho thấy đây là một lĩnh vực nghiên cứu có tính ứng dụng rất cao. Tuy nhiên, mỗi hệ thống tin học thường được tổ chức rất khác nhau, có nguồn lực và đối tượng phục vụ riêng, do vậy cần phải có một nghiên cứu cụ thể dựa trên tình hình thực tế.

3. Mục tiêu nghiên cứu

Mục tiêu nghiên cứu của đề tài là đưa ra giải pháp tối ưu để nâng cao khả năng an toàn cho hệ thống máy tính giao dịch tại TTGDCK nhằm nâng cao hiệu quả công tác quản lý, điều hành, giám sát thị trường chứng khoán của TTGDCK. Đồng thời phục vụ đắc lực cho việc quản lý nhà nước về chứng khoán và thị trường chứng khoán của Uỷ ban Chứng khoán Nhà nước.

4. Phạm vi của đề tài

Đối tượng của đề tài "Giải pháp nhằm nâng cao tính an toàn cho hệ thống máy tính tại Trung tâm Giao dịch chứng khoán" được xác định là các TTGDCK, đặc biệt là TTGDCKHN. Do đặc điểm phát triển nhanh chóng của thị trường cũng như nhu cầu cải tiến công nghệ liên tục, đề tài sẽ tập trung xây dựng một giải pháp an ninh mở, không chỉ đáp ứng được yêu cầu hiện tại, mà còn sẵn sàng nâng cấp khi điều kiện thay đổi.

Phạm vi nghiên cứu bao gồm:

- Vài nét về an toàn hệ thống và tổng quan về một số hệ thống máy tính của các nước trên thế giới.
- Thực trạng và giải pháp nâng cao tính an toàn hệ thống máy tính tại TTGDCK.

5. Phương pháp tiến hành

- Nghiên cứu tài liệu trong nước và nước ngoài;

- Điều tra, khảo sát thực trạng về an ninh hệ thống tại TTGDCK Tp HCM;
- So sánh, phân tích và đánh giá;
- Đề xuất giải pháp.

6. Kết cấu đề tài

Đề tài gồm có 80 trang. Ngoài phần mở đầu, kết luận, mục lục, danh mục tài liệu tham khảo, đề tài được kết cấu thành 3 chương gồm:

Chương 1: Những vấn đề về an toàn của hệ thống máy tính

Chương 2: Thực trạng hệ thống máy tính tại các TTGDCK Việt Nam

Chương 3: Các giải pháp nhằm nâng cao tính an toàn hệ thống máy tính tại TTGDCK

CHƯƠNG I :NHỮNG VẤN ĐỀ VỀ AN TOÀN CỦA HỆ THỐNG MÁY TÍNH

I. KHÁI NIỆM AN TOÀN HỆ THỐNG

1.1. Khái niệm an toàn hệ thống

Vấn đề an toàn - bảo mật thông tin nói chung và trên mạng máy tính nói riêng đã và đang trở thành một vấn đề bức xúc đối với các tổ chức xã hội, các cơ quan của Chính phủ, thách thức sự tồn tại và phát triển của các hệ thống thông tin. Chính vì vậy vấn đề an toàn hệ thống đã được các chuyên gia trong nhiều lĩnh vực quan tâm và tìm biện pháp giải quyết.

Một hệ thống được coi là an toàn khi hệ thống:

* Đảm bảo được sự bí mật của thông tin (Confidentality): Hệ thống phải đảm bảo thông tin trong hệ thống không được phổ biến khi không được phép.

* Đảm bảo được sự thống nhất, toàn vẹn của thông tin (Integrity): tránh được việc sửa đổi trái phép thông tin.

* Đảm bảo được khả năng hiệu lực (Availability): có thể khởi động bất kỳ lúc nào khi hệ thống cần.

* Khả năng xác nhận tính hợp lệ: (Authentication): Có khả năng xác định tính hợp lệ của người sử dụng và hệ thống ...

* Đảm bảo khả năng thừa nhận (Nonrepudiation): Đảm bảo rằng thông tin đã gửi được gửi đi và đã được đọc.

* Có khả năng kiểm soát truy nhập (Access Control): Đảm bảo chỉ có những người được phép mới có quyền truy nhập thông tin.

* Có khả năng sao lưu dữ liệu (Backup): Hệ thống Backup phải hoạt động định kỳ, đảm bảo được sự toàn vẹn thông tin.

Một hệ thống an toàn - bảo mật thông tin cao phải được xây dựng trên cơ sở xây dựng một loạt các thủ tục và kế hoạch nhằm mục đích bảo vệ tài nguyên của hệ thống khỏi sự mất mát, phá hủy.

1.2. Những mối đe doa hệ thống thường gặp

Do đặc điểm của một hệ thống mạng là có nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên (mất mát hoặc sử dụng không hợp lệ) trong môi trường mạng phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.

Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đối tượng đồng thời đảm bảo mạng hoạt động ổn định, không bị tấn công bởi những kẻ phá hoại.

Có một thực tế là không một hệ thống mạng nào đảm bảo là an toàn tuyệt đối, một hệ thống dù bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hoá bởi những kẻ có ý đồ xấu.

Các mối đe doạ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộ tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn.

1.2.1. Đối tượng tấn công mạng

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép, bao gồm:

- Hacker: là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.
- Masquerader: là những kẻ giả mạo thông tin trên mạng. Có một số hình thức như giả mạo địa chỉ IP, tên miền, định danh người dùng, ...
- Eavesdropping: là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer: sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị.

Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau như: ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận, ...

1.2.2. Các lỗ hổng bảo mật

Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp, ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống, ... Các lỗ hổng bảo mật sẽ là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp, ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Windows 95, hoặc trong các ứng dụng mà người sử dụng thường xuyên

sử dụng như word processing, các hệ databases ... Thông thường một số nguy cơ nằm ở các thành phần sau trên hệ thống: Các điểm truy nhập, không kiểm soát được cấu hình hệ thống, những nguy cơ trong nội bộ mạng, ...

Có nhiều tổ chức khác nhau tiến hành phân loại các dạng lỗ hổng đặc biệt. Theo cách phân chia của Bộ Quốc phòng Mỹ, các lỗ hổng bảo mật trên một hệ thống được chia như sau:

- Lỗ hổng loại C: các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services – Từ chối dịch vụ). Mức độ nguy hiểm thấp, không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.
- Lỗ hổng loại B: các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ nên có thể dẫn đến mất mát hoặc lộ thông tin yêu cầu bảo mật. Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống.
- Lỗ hổng loại A: các lỗ hổng này cho phép người sử dụng ở ngoài có thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá huỷ toàn bộ hệ thống.

1.2.3. Chương trình lây nhiễm (Virus)

a) Scanner

Scanner là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc cục bộ hoặc trên một trạm ở xa. Với chức năng này, một kẻ phá hoại sử dụng chương trình Scanner có thể phát hiện ra những lỗ hổng về bảo mật trên một server ở xa.

Các chương trình scanner thường có một cơ chế chung là rà soát và phát hiện những port TCP/ UDP được sử dụng trên một hệ thống cần tấn công từ đó phát hiện những dịch vụ sử dụng trên hệ thống đó. Sau đó các chương trình scanner gọi lại những đáp ứng trên hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tìm ra những điểm yếu trên hệ thống.

Các chương trình scanner có vai trò quan trọng trong một hệ thống bảo mật, vì chúng có khả năng phát hiện ra những điểm yếu kém trên một hệ thống mạng. Đối với người quản trị mạng những thông tin này là hết sức hữu ích và cần thiết; đối với những kẻ phá hoại những thông tin này sẽ hết sức nguy hiểm.

b) Password Cracker

Password cracker là một chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.

Để hiểu cách thức hoạt động của các chương trình bẻ khoá, chúng ta cần hiểu cách thức mã hoá để tạo mật khẩu. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.

Nguyên tắc của một số chương trình phá khoá có thể khác nhau. Một vài chương trình tạo một danh sách các từ giới hạn, áp dụng một số thuật toán mã hoá, từ kết quả so sánh với password đã mã hoá cần bẻ khoá để tạo ra một danh sách khác theo một lôgic của chương trình, cách này tuy không chuẩn tắc nhưng khá nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng thường tuân theo một số chuẩn tắc để thuận tiện khi sử dụng. Đến giai đoạn cuối cùng, nếu thấy phù hợp với mật khẩu đã được mã hoá, kẻ phá khoá sẽ có được mật khẩu dạng text thông thường.

Biện pháp khắc phục đối với cách thức phá hoại này là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

c) Trojans

Trojans là một chương trình chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Những chương trình này thực hiện những chức năng mà người sử dụng hệ thống thường không mong muốn hoặc không hợp pháp. Thông thường, trojans có thể chạy được là do chương trình hợp pháp đã bị thay đổi mã của nó bằng những mã bất hợp pháp.

Các chương trình virus là một loại điển hình của trojans. Những chương trình virus che dấu các đoạn mã trong các chương trình sử dụng hợp pháp. Khi những chương trình này được kích hoạt thì những đoạn mã ẩn dấu sẽ được thực thi để thực hiện một số chức năng mà người sử dụng không biết.

Xét về khía cạnh bảo mật trên Internet, một chương trình trojans sẽ thực hiện một trong những công việc sau:

- Thực hiện một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó.
- Che dấu một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó.

Một vài chương trình trojans có thể thực hiện cả hai chức năng này. Ngoài ra, một số chương trình trojans còn có thể phá huỷ hệ thống bằng cách phá hoại các thông tin trên ổ cứng.

Ví dụ: Virus Melisa lây lan qua đường thư điện tử.

Các chương trình trojans có thể lây lan qua nhiều phương thức, hoạt động trên nhiều môi trường hệ điều hành khác nhau (từ UNIX tới Windows, DOS). Đặc biệt, trojans thường lây lan qua một số dịch vụ phổ biến như

Mail, FTP, ... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet.

Việc đánh giá mức độ ảnh hưởng của các chương trình trojans hết sức khó khăn. Trong một vài truường hợp, nó chỉ đơn giản là ảnh hưởng đến các truy nhập của khách hàng như các chương trình trojans lấy được nội dung của file password và gửi email tới kẻ phá hoại. Tuy nhiên, với những trường hợp nghiêm trọng hơn, là những kẻ tấn công tạo ra những lỗ hổng bảo mật thông qua các chương trình trojans.

d) Sniffer

Đối với bảo mật hệ thống sniffer được hiểu là các công cụ (có thể là phần cứng hoặc phần mềm) " bắt " các thông tin lưu chuyển trên mạng và từ các thông tin " bắt " được đó để lấy được những thông tin có giá trị trao đổi trên mạng.

Hoạt động của sniffer cũng giống như các chương trình " bắt " các thông tin gõ từ bàn phím (key capture). Tuy nhiên các tiện ích key capture chỉ thực hiện trên một trạm làm việc cụ thể còn đối với sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.

Các chương trình sniffer (sniffer mềm) hoặc các thiết bị sniffer (sniffer cứng) đều thực hiện bắt các gói tin ở tầng IP trở xuống (gồm IP datagram và Ethernet Packet). Do đó, có thể thực hiện sniffer đối với các giao thức khác nhau ở tầng mạng như TCP, UDP, IPX, ...

Mục đích của các chương trình sniffer đó là thiết lập chế độ promiscuous (mode dùng chung) trên các card mạng ethernet – nơi các gói tin trao đổi trong mạng – từ đó " bắt " được thông tin. Một hệ thống sniffer có thể kết hợp cả các thiết bị phần cứng và phần mềm, trong đó hệ thống phần mềm với các chế độ debug thực hiện phân tích các gói tin "bắt" được trên mạng.

Phương thức tấn công mạng dựa vào các hệ thống sniffer là rất nguy hiểm vì nó được thực hiện ở các tầng rất thấp trong hệ thống mạng. Với việc thiết lập hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng. Các thông tin đó có thể là:

- Các tài khoản và mật khẩu truy nhập
- Các thông tin nội bộ hoặc có giá trị cao, ...

Ngoài ra còn rất nhiều chương trình được viết ra nhằm tấn công hệ thống bất hợp pháp. Trên đây chỉ là một số chương trình điển hình gây ra sự mất an toàn và bảo mật của hệ thống.

1.2.4. Một số vấn đề khác

Ngoài một số nguyên nhân do yếu tố bên ngoài, còn phải kể đến những nguyên nhân chủ quan khi xây dựng hệ thống CNTT không tính đến như:

- Thông tin bị tấn công trên đường truyền do không có cơ chế mã hoá dữ liệu, hoặc bị giả mạo;

- Hệ thống không có cơ chế dự phòng, sao lưu phục hồi dữ liệu. Do vậy khi phát sinh sự cố thì không phục hồi lại được dữ liệu;

- Chính sách quản trị hệ thống quá đơn giản, thiếu khoa học sẽ dẫn đến những vấn đề về bảo mật hệ thống;

- Hệ thống nhanh chóng bị quá tải do không tính toán được khả năng đáp ứng của hệ thống..

II. KINH NGHIỆM XÂY DỰNG HỆ THỐNG MÁY TÍNH PHỤC VỤ GIAO DỊCH CHỨNG KHOÁN TẠI MỘT SỐ NƯỚC TRÊN THẾ GIỚI

2.1. HỆ THỐNG MÁY TÍNH TẠI THỊ TRƯỜNG KSE – HÀN QUỐC

2.1.1. Tổng quan về thị trường chứng khoán Hàn Quốc

Thị trường chứng khoán Hàn Quốc nói chung được chia làm 3 thị trường chính:

- Sở giao dịch chứng khoán Hàn Quốc (KSE)

- Thị trường KOSDAQ

- Thị trường OTC

a. Thị trường KSE

Chứng khoán niêm yết

Chứng khoán giao dịch trên thị trường KSE chủ yếu là các doanh nghiệp lớn có vốn điều lệ từ 5 tỷ won trở lên, có thời gian hoạt động từ ba năm trở lên, có ít nhất 10% số cổ phiếu được phát hành ra công chúng...

Các công ty hội đủ các điều kiện niêm yết của KSE muốn được niêm yết trên thị trường sẽ làm thủ tục xin niêm yết gửi cho KSE.

b. Thị trường KOSDAQ

Chứng khoán niêm yết

Chứng khoán giao dịch trên thị trường KOSDAQ chủ yếu là của các doanh nghiệp vừa và nhỏ, các công ty trong lĩnh vực công nghệ cao có vốn điều lệ từ 500 triệu won trở lên, đã hoạt động trong thời gian ít nhất 3 năm, được sự chấp thuận của KSD (Trung tâm lưu ký Hàn Quốc), có ít nhất 30% số cổ phiếu đang lưu hành hoặc 10% và không ít hơn 1 triệu cổ phiếu được nhiều hơn 500 cổ đông thiểu số nắm giữ nắm giữ...

c. Thị trường OTC

Thị trường OTC BB được thiết lập vào tháng 3/2000 giành cho các công ty mà chứng khoán của nó không được niêm yết trên thị trường KSE cũng như KOSDAQ. Các công ty này đăng ký niêm yết với Hiệp hội chứng khoán Hàn Quốc (KSDA) và các chứng khoán của nó được giao dịch bằng hệ thống Bulletin Board của thị trường KOSDAQ. Thị trường OTC BB được thành lập với mục đích:

- Đảm bảo sự công bằng, an toàn cho các giao dịch của các chứng khoán không được niêm yết trước đây bằng cách tập trung vào hệ thống có tổ chức của OTC BB

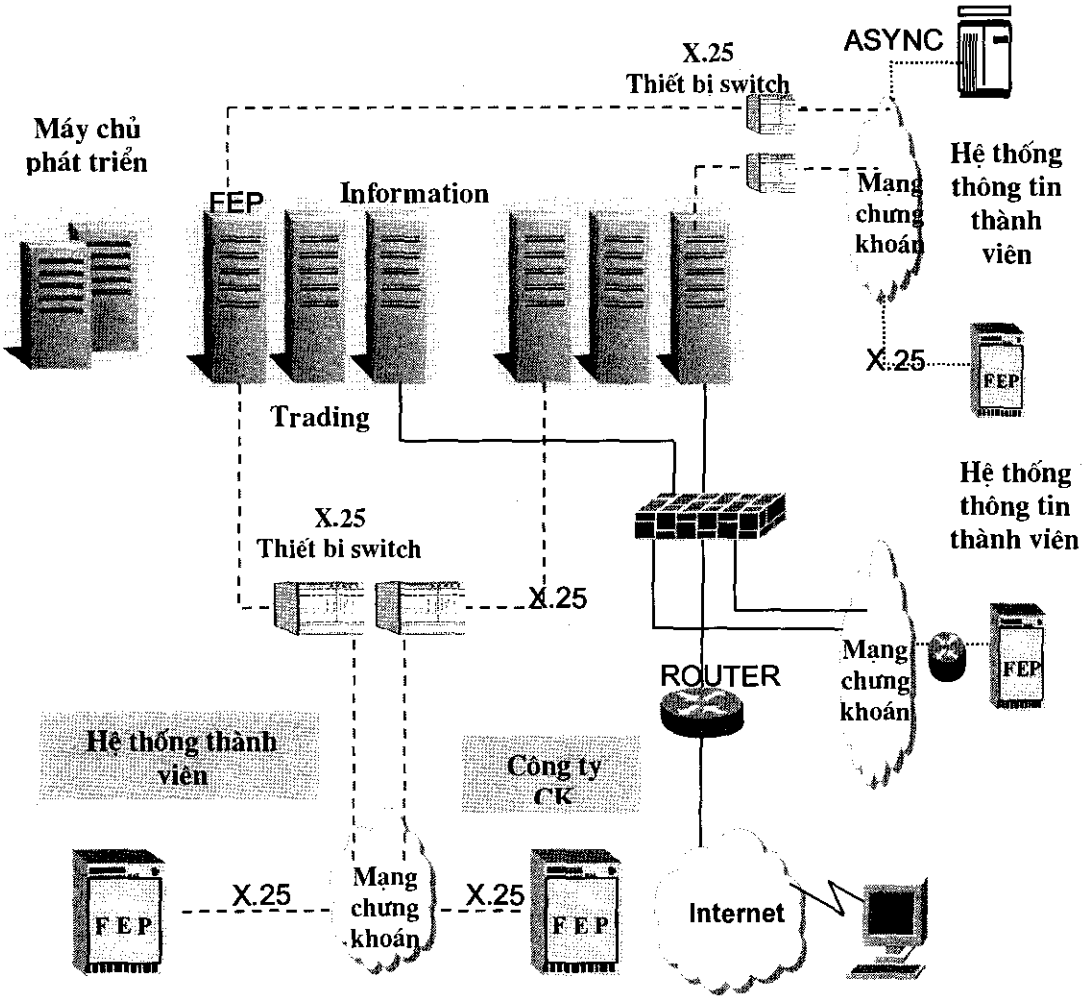
- Tăng tính thanh khoản cho các chứng khoán của các công ty không đủ tiêu chuẩn niêm yết trên thị trường KSE và KOSDAQ hoặc các chứng khoán bị huỷ bỏ niêm yết từ KSE và KOSDAQ. Điều này có nghĩa là thị trường OTC tạo cơ hội cho các công ty nói trên huy động vốn trực tiếp từ thị trường tài chính.

- Tạo cơ hội cho người đầu tư có thể mua chứng khoán của các công ty có triển vọng khi chúng chuẩn bị trên con đường niêm yết trên thị trường KSE và KOSDAQ. Điều này có nghĩa là cùng với KSE, KOSDAQ,OTC BB tạo nên một hệ thống thị trường phong phú, đa dạng, người đầu tư có thể có những cơ hội lựa chọn đầu tư tốt hơn.

2.1.2. Hệ thống máy tính tại thị trường Hàn Quốc

Hệ thống máy tính tại thị trường chứng khoán Hàn Quốc hiện do công ty máy tính KOSSCOM đảm nhiệm. KOSCOM là công ty tin học hoạt động chuyên về lĩnh vực chứng khoán. Qua nhiều năm hoạt động, công ty KOSCOM đã có nhiều kinh nghiệm trong việc xây dựng hệ thống giao dịch cho ngành chứng khoán..

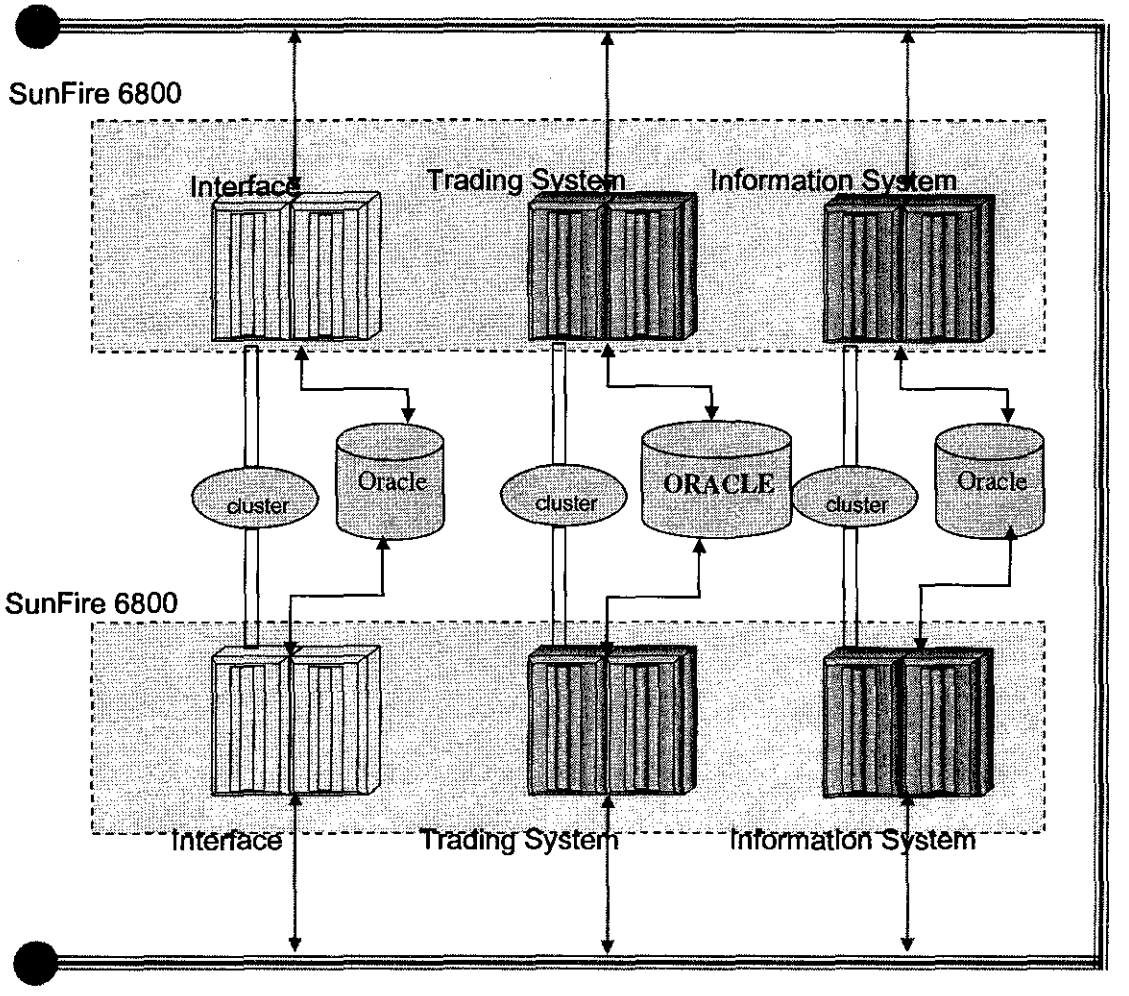
➢ ***Hệ thống giao dịch ECN*** (Electronic Communications Network – Giao dịch điện tử qua mạng)



Hình vẽ: Mô hình hệ thống ECN

Đây là một hệ thống giao dịch hiện đại, phù hợp với điều kiện phát triển thị trường trong tương lai tại Việt Nam. Thị trường ECN là một mạng viễn thông điện tử phục vụ cho giao dịch chứng khoán thông qua internet. Thị trường này là một loại hình Hệ thống giao dịch bổ sung (ATS - Alternative Trading System), bổ trợ cho chức năng thị trường của KSE và KOSDAQ thông qua việc cung cấp dịch vụ giao dịch trực tuyến ngoài giờ giao dịch chính thức. Thị trường ECN làm trung gian cho các giao dịch chứng khoán điện tử qua mạng, với mục tiêu tăng cường tính hiệu quả thị trường và tính cạnh tranh của thị trường vốn. Hình thái thị trường giống như thị trường OTC. Theo quy định hiện hành tại Hàn Quốc, thị trường ECN được phép giao dịch và làm môi giới qua mạng cho 250 loại cổ phiếu, bao gồm 200 loại cổ phiếu thuộc KOSPI 200, và 50 loại cổ phiếu thuộc KOSDAQ 50. Thị trường ECN hiện do công ty Korea ECN Securities Co., Ltd. quản lý, hiện bao gồm các thành viên là 28 công ty chứng khoán lớn trong nước.

Hệ thống giao dịch của ECN chạy trên nền hệ điều hành UNIX của hãng SUN, sử dụng CSDL Oracle phiên bản 8i. Đây là một hệ thống giao dịch hiện đang được vận hành trên một hệ thống mạng hiện đại, với khả năng chịu đựng sai sót của hệ thống, khả năng đối phó với các trục trặc, lỗi xảy ra với các phần cứng bên trong máy, làm cho hệ thống không bị ngưng hoạt động. Đây là một hệ thống có thể đáp ứng một cách tốt nhất cho các yêu cầu mà một hệ thống giao dịch chứng khoán cần có, " non stop ". Hệ thống ECN giao dịch ổn định, có thể mở rộng và kiểm soát lỗi một cách nhanh chóng với hệ thống sửa lỗi bằng Clustering. Hệ thống phần mềm dựa trên hệ điều hành UNIX OS mở, với phương thức giao tiếp chuẩn X25. Hệ thống ECN tại Hàn Quốc bao gồm hệ thống giao dịch, hệ thống thông tin được chạy trên máy SunFire 6800 của hãng SUN với cấu hình máy có tối đa 24 CPU, bộ nhớ tối đa 192 GB. Hệ thống giao dịch có firewall (bức tường lửa) ngăn chặn sự tấn công từ bên ngoài, có router kết nối thông tin với bên ngoài và thiết bị chuyển mạch switch cho hệ thống mạng tại trung tâm.

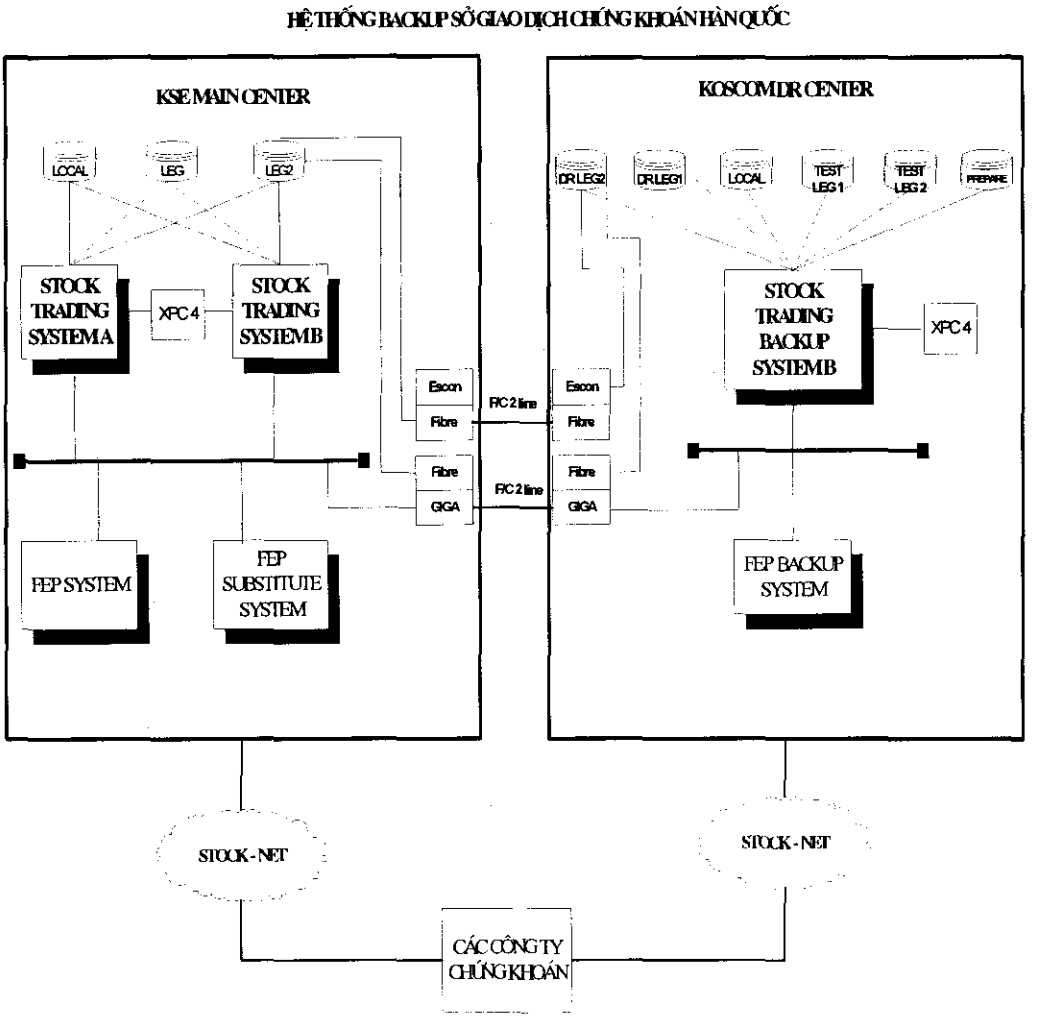


Hình vẽ: Cấu hình thiết bị phần cứng của hệ thống ECN

Ngày nay, yêu cầu bảo vệ thông tin, tài nguyên máy tính có ý nghĩa rất quan trọng đặc biệt với những thông tin nhạy cảm như tài chính, ngân hàng, quân sự... Nhận biết được vấn đề này ngay từ khi hoạt động, Koscom đã rất chú ý xây dựng và phát triển riêng một hệ thống bảo mật thông tin cho mình bằng việc áp dụng nhiều công nghệ, thiết bị bảo mật mới nhằm đảm bảo hoạt động của thị trường. Hiện nay, koscom đang sử dụng thiết bị và phần mềm bảo mật theo mô hình sau:

Các lớp bảo mật hệ thống thông tin của Koscom

	Access control	**Detection**	**Virus**
Network	Firewall	**Network – based IDS**	Viruswall
Server	File access control	Host – based IDS	Server Anti-Virus
PC	PC Firewall	PC IDS	PC Anti –Virus
Encryption	**VPN, File Encryption**		
Email	Mail Gateway, Virus Wall		
Management	EMS (Enterprise Sercurity management)		



Hệ thống giao dịch trên thị trường KOSDAQ (Thị trường phi tập trung):

- Hệ thống KETRA (KOSDAQ Electronic Trading System) được tổ chức từ thị trường OTC (7/1996) theo tiêu chuẩn của NASDAQ thực hiện việc kinh doanh cổ phiếu cho những giao dịch mạo hiểm. Khả năng đáp ứng được 5 triệu giao dịch/ngày. Hệ thống máy tính: sử dụng máy chủ Tandem Himalaya S74000.

- Hệ thống OTCBB: Được khai trương vào tháng 3/2000 thực hiện việc kinh doanh cổ phiếu cho thị trường thứ 3. Khả năng có thể đáp ứng được 250.000 giao dịch/ngày. Hệ thống máy tính sử dụng máy chủ Tandem Himalaya S74000 và các máy chủ khác.

- FOT: Hệ thống giao dịch lựa chọn và Hợp đồng tương lai được khai trương vào tháng 5/1996 (Hợp đồng tương lai) và tháng 7/1997 (các lựa chọn) dựa vào danh mục KOSPI 200. Thực hiện việc nhận và tổng hợp lệnh.

Thực hiện việc kinh doanh, thanh toán, kiểm soát hoạt động thị trường. Khả năng đáp ứng được từ 150.000 - 250.000 giao dịch/ngày. Hệ thống máy tính: sử dụng hệ thống máy chủ GS160, GS140, ES40.

2.2. HỆ THỐNG MÁY TÍNH TẠI THỊ TRƯỜNG ĐÀI LOAN

2.2.1. Tổng quan về thị trường chứng khoán Đài Loan

Thị trường chứng khoán Đài Loan gồm có:

- TSE là sở giao dịch giành cho chứng khoán vừa và lớn

- Greitai là thị trường OTC cho chứng khoán nhỏ và vừa. Thị trường này chia thành 2 hệ thống giao dịch:

+ Chứng khoán được niêm yết trên thị trường OTC sẽ giao dịch qua hệ thống khớp lệnh

+ Chứng khoán không được niêm yết trên Sở hoặc thị trường OTC và trái phiếu sẽ đăng ký giao dịch qua hệ thống thoả thuận.

Hệ thống giao dịch khớp lệnh

Với sự bổ sung của các thủ tục mới, việc giao dịch trên GTSM cũng tương tự như trên TSE. GTSM thuê lại hệ thống thiết bị máy tính từ TSE. Hệ thống giao dịch này ngoài các chức năng thông thường như nhập lệnh, khớp lệnh, tự động truyền tin ... còn có chức năng cảnh báo. Theo đó, nếu có các sai sót về lệnh nhập vào hệ thống thì hệ thống sẽ tự động cảnh báo. Sử dụng hệ thống máy tính khớp lệnh đã tạo hiệu quả cho việc giao dịch. Đơn vị khớp lệnh qua hệ thống này là 1000 cổ phiếu và mỗi lệnh không vượt quá 500 đơn vị giao dịch. Giới hạn dao động giá hàng ngày là ±7%, ngày thanh toán là T+2.

Giao dịch thoả thuận qua hệ thống tạo lập thị trường

Cổ phiếu của các công ty không niêm yết (công ty mới nổi) được đăng ký giao dịch theo phương thức thoả thuận, không sử dụng hệ thống máy tính khớp lệnh. GTSM cung cấp 1 bảng báo giá điện tử cho tất cả công chúng được tiếp cận và xem thông tin.

Trong 3 phút sau khi giao dịch thực hiện, báo cáo được gửi tới hệ thống yết giá của trung tâm điều hành GTSM, và thanh toán 1 ngày sau khi giao dịch (T+1). Nhà giao dịch có thể lựa chọn sử dụng hình thức thanh toán ngay theo từng giao dịch cho việc thanh toán đặc biệt.

Giao dịch thoả thuận trực tiếp

Đối với các chứng khoán niêm yết trên GTSM, các giao dịch trên 100 lô hoặc lớn hơn, hai bên tham gia giao dịch có thể thoả thuận một giá chấp nhận được khác với giá tham chiếu nhưng trong giới hạn giao động 7% của giá đóng cửa ngày giao dịch trước.

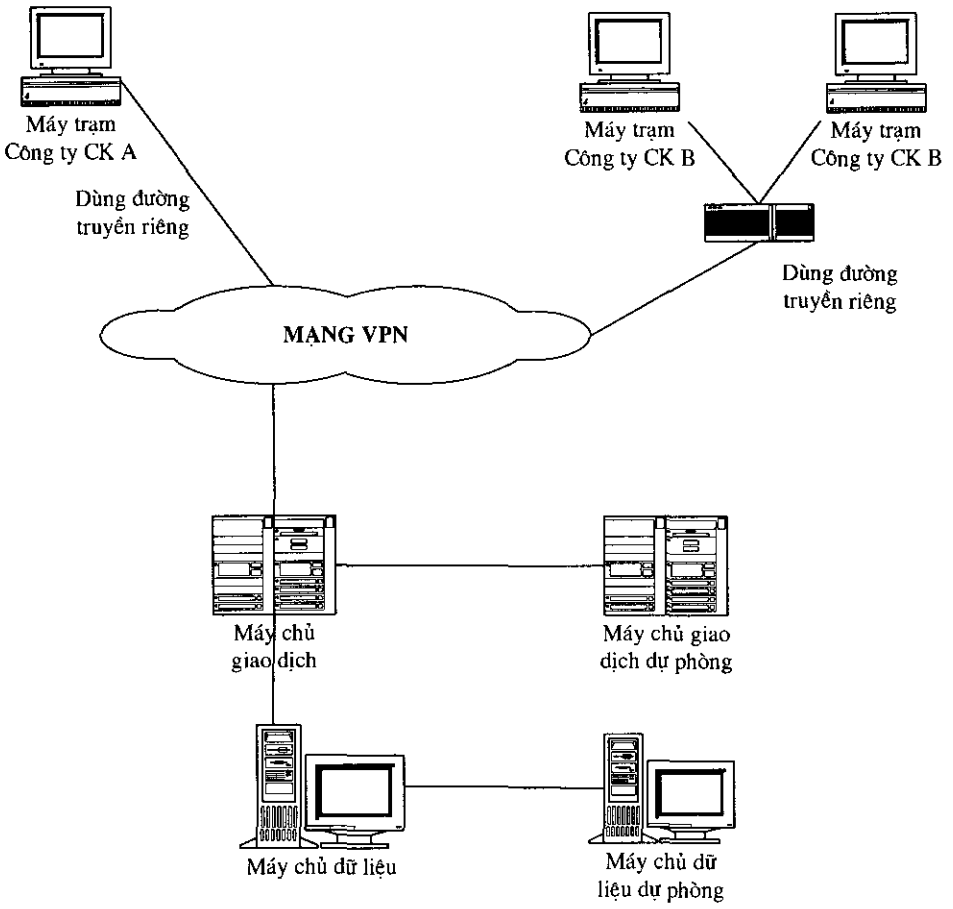
Công bố thông tin

Về cơ bản hệ thống công bố thông tin của GTSM cũng giống hệ thống công bố thông tin của chứng khoán khớp lệnh.

- GTSM đưa ra một hệ thống giám sát thuận lợi nhất với các cổ phiếu trên hệ thống cổ phiếu mới nổi, nhà đầu tư được quyền có được những thông tin đầy đủ trợ giúp họ đưa ra những quyết định đầu tư. Các công ty đăng ký trên hệ thống cổ phiếu mới nổi tuân thủ nghiêm ngặt chính sách công bố thông tin. Một mặt, các công ty này phải chỉ rõ trong bản cáo bạch của mình quá trình hoạt động, rủi ro ngành và rủi ro về thị trường. Mặt khác, họ phải được nhà bảo lãnh phát hành của mình đánh giá xem xét định kỳ tình hình hoạt động và tài chính. GTSM đồng thời công bố thông tin tới công chúng thông qua Internet và hệ thống thông tin thực thời.

2.2.2. Hệ thống máy tính tại thị trường Đài Loan

Hệ thống máy tính gồm các máy chủ hiện đại dòng SUN và hệ điều hành Solaris. Tại trụ sở GTSM, có các máy chủ giao dịch trái phiếu, máy chủ giám sát và thông tin thị trường. Máy chủ giao dịch cổ phiếu đặt tại trụ sở Sở giao dịch chứng khoán Đài Bắc (TSEC). Các thiết bị truyền thông chủ yếu gồm các CISCO Routers. Hệ thống máy tính dự phòng (đầy đủ cả phần cứng và phần mềm) do GTSM được thiết lập tại 2 địa điểm khác nhau để đảm bảo an toàn cho hoạt động của thị trường. Ngoài ra, GTSM còn có hợp đồng backup dữ liệu với Công ty máy tính IBM tại Đài Bắc.



Hình vẽ: Mô hình hệ thống mạng máy tính giao dịch

III. ĐÁNH GIÁ CHUNG VÀ BÀI HỌC KINH NGHIỆM CHO VIỆT NAM

3.1. Đánh giá chung

Trong giai đoạn đầu phát triển của ngành chứng khoán Việt Nam, các trung tâm giao dịch chứng khoán chiếm một vị trí đặc biệt quan trọng. Hầu hết tất cả mọi qui trình nghiệp vụ, thông tin, tài liệu đều được tin học hoá và có mức độ nhạy cảm rất cao. Chính vì lý do này, một trong những yêu cầu cấp thiết cho các trung tâm giao dịch chứng khoán hiện nay đó là tìm ra được các giải pháp nhằm đảm bảo an toàn cho hệ thống máy tính, đảm bảo cho thị trường chứng khoán hoạt động có tổ chức, an toàn, công khai, công bằng và hiệu quả, bảo vệ quyền lợi hợp pháp của người đầu tư.

Vấn đề quan trọng nhất của việc thiết kế bảo mật đó là phải xây dựng được chính sách bảo mật. Việc xây dựng chính sách bảo mật cho một mạng thông tin sẽ cho phép người có trách nhiệm có thể thấy được các nguy hiểm trong mạng của mình và đưa vào các biện pháp để bảo đảm an toàn thông tin của mình.

3.2. Bài học kinh nghiệm cho Việt Nam

Với tư cách là đơn vị quản lý hệ thống giao dịch chứng khoán, cả hai trung tâm giao dịch chứng khoán của ta ở thành phố Hồ Chí Minh và sắp tới ở Hà Nội đều là những đơn vị có những số liệu đặc biệt quan trọng. Hầu hết tất cả mọi qui trình nghiệp vụ, thông tin, tài liệu đều được tin học hoá và có mức độ nhạy cảm rất cao. Đặc biệt, trung tâm giao dịch chứng khoán Hà Nội sắp đưa vào vận hành hệ thống tin học phục vụ giao dịch chứng khoán. Bên cạnh các yếu tố về trang thiết bị phần cứng và phần mềm giao dịch, hệ thống sẽ được phân tích, đánh giá rủi ro một cách toàn diện, từ đó đưa ra giải pháp đảm bảo an toàn cho hệ thống thật hoàn chỉnh. Tuy nhiên, vì nhiều lý do khách quan việc đảm bảo an ninh cho hệ thống giao dịch chứng khoán tại thành phố Hồ Chí Minh còn có rất nhiều bất cập và hạn chế như sự tích hợp chưa cao giữa phần mềm hệ thống giao dịch với các phần mềm ứng dụng khác, cấu hình thiết bị, ... nên qua các phân tích đánh giá về hệ thống máy tính tại các nước trên thế giới và hệ thống máy tính hiện tại đang có tại hai trung tâm giao dịch chứng khoán chúng ta có thể rút ra được những bài học kinh nghiệm vô cùng quí giá cho việc đảm bảo an toàn cho hệ thống máy tính trong giao dịch chứng khoán:

Thứ nhất: về mô hình quản lý hệ thống

- Có những mức truy cập khác nhau cho người dùng;

- Hệ thống hỗ trợ việc thiết lập phân quyền truy nhập người dùng khác nhau dựa vào sự cho phép và phân loại người dùng;

- Hệ thống yêu cầu người sử dụng thay đổi mật khẩu theo định kỳ tối thiểu để nâng cao tính an toàn;

- Hệ thống cần ghi lại dấu vết về sự xâm phạm hệ thống vô tình hay cố ý;

- Giải pháp bảo mật cần được cập nhật thường xuyên về các hình thức tấn công, các mối đe doạ mới, và tất nhiên là cách thức phòng chống

- Hệ thống thiết lập các bảo mật với các hệ thống ngoài, truy cập từ xa, cung cấp các khả năng mã hoá dữ liệu;

- Hệ thống có khả năng giám sát, theo dõi và phát hiện các hành động cố tình vi phạm bên trong hệ thống;

- Phân quyền truy nhập hệ thống thông tin phù hợp đối với các đơn vị liên quan nối vào mạng của TTGDCK.

Thực tế cho thấy, trang bị các thiết bị phục vụ truyền dữ liệu bao gồm Router có cấu hình đủ mạnh như CISCO Router 3662 đi kèm các thiết bị, giải pháp phần cứng và phần mềm bảo mật như CISCO PIX FireWall, VPN ... có khả năng đảm bảo các yêu cầu nêu trên.

Thứ hai: Xây dựng chính sách an ninh mạng

Các chính sách an ninh mạng chỉ có thể phát huy hiệu quả cao nhất khi có một chính sách an ninh mạng hợp lý. Đó là những qui định cụ thể về các biện pháp an ninh. Đối với hệ thống mạng tại thị trường giao dịch chứng khoán Việt Nam, chính sách an ninh mạng cần qui định cụ thể về những ai sẽ được quyền truy cập vào hệ thống thông tin nào, quyền truy cập đó ra sao (được phép thay đổi nội dung hay chỉ đọc, ...), qui định về hệ thống nhật ký (Log file) và báo cáo về hoạt động của những người sử dụng trên mạng, qui định về các hành động cần thiết khi xảy ra hiện tượng bùng nổ virus.

Thứ ba: Lựa chọn các giải pháp cho hệ thống an ninh mạng

- Giải pháp chống truy nhập bất hợp pháp
- Giải pháp bảo vệ hệ thống phần cứng
- Giải pháp bảo mật hệ điều hành
- Giải pháp bảo mật phần mềm ứng dụng
- Giải pháp bảo mật CSDL
- Giải pháp phân quyền người sử dụng
- Giải pháp mã hoá dữ liệu

Thứ tư: Xây dựng hệ thống Backup và an toàn dữ liệu

Tính liên tục trong hoạt động của hệ thống giao dịch là một khía cạnh cấp thiết đặt ra cho việc giao dịch tại trung tâm giao dịch chứng khoán. Nhằm tạo điều kiện để vận hành hệ thống thông tin liên tục và đảm bảo an toàn dữ liệu chúng ta cần phải đưa ra một chính sách tổ chức và vận hành dữ liệu. Chính sách này đảm bảo cho hệ thống thông tin của trung tâm giao dịch chứng khoán vẫn tiếp tục hoạt động trong trường hợp bất trắc hay khẩn cấp như mất điện, hệ thống hỏng hoặc không thể thâm nhập tới các hệ thống hoặc văn phòng.

Thứ năm: Xây dựng chính sách quản trị hệ thống hợp lý, phù hợp với điều kiện ứng dụng CNTT tại Việt Nam

Thứ sáu: Xây dựng kế hoạch đào tạo dài hạn nguồn nhân lực về CNTT trong lĩnh vực chứng khoán.

CHƯƠNG II:THỰC TRẠNG HỆ THỐNG MÁY TÍNH TẠI CÁC TRUNG TÂM GIAO DỊCH CHỨNG KHOÁN VIỆT NAM

I. THỰC TRẠNG HỆ THỐNG MÁY TÍNH TTGDCK TpHCM

1.1. Tổng quan hệ thống máy tính TTGDCK tpHCM

1.1.1 Mô hình hệ thống

TTGDCK TpHCM là thị trường giao dịch chứng khoán tập trung theo hình thức khớp lệnh định kỳ, nhập lệnh trực tiếp tại sàn.

Hệ thống tin học của TTGDCK TpHCM gồm 3 hệ thống chính là hệ thống giao dịch, hệ thống lưu ký và hệ thống công bố thông tin. Sở dĩ gọi các phần nói trên là "hệ thống" bởi vì chúng được hình thành không đồng bộ và không tích hợp hoàn toàn được với nhau

Hệ thống giao dịch

Hệ thống giao dịch chứng khoán hiện tại do sở giao dịch chứng khoán Thái Lan hỗ trợ Việt Nam, các chuyên gia Thái Lan trực tiếp sang Việt Nam khảo sát bài toán, cung cấp phần mềm và thiết bị.

Phân hệ giao dịch do Sở Giao dịch chứng khoán Thái Lan hỗ trợ TTGDCK TpHCM xây dựng, phía Thái lan cung cấp máy chủ giao dịch, phần mềm giao dịch, hỗ trợ hoàn toàn về mặt kỹ thuật, cử chuyên gia sang tận nơi để xây dựng phân hệ này.

Nhược điểm lớn nhất của hệ thống này là khả năng tích hợp rất kém với các hệ thống khác, được phát triển về sau như lưu ký và thông tin. Người vận hành hệ trực tiếp lại không thực sự làm chủ được hệ thống nên gặp rất nhiều khó khăn khi quản trị. Qua hơn ba năm hoạt động, đã có lúc những thao tác trên hệ thống không có tác dụng mặc dù các chức năng của phần mềm đã được quy định, chỉ khi các chuyên gia Thái Lan truy cập từ xa vào hệ thống và có những can thiệp nào đó thì những thay đổi mới thực sự có hiệu lực. Bên cạnh đó, phần mềm đã bộc lộ những khiếm khuyết, hạn chế về chức năng gây trở ngại cho quá trình vận hành và hoạt động quản lý giao dịch.

- Hệ điều hành: VMS Alpha 64 bite (máy chủ) , Win98 (máy trạm);
- Máy chủ: 2 máy Compaq DS 10 dùng chung ổ cứng ngoài, 1 chạy, 1 dự phòng;
- Cơ sở dữ liệu: Oracle;
- Ngôn ngữ phát triển: C for DOS;
- Giao thực mạng: TCP/IP, Netbios ;

- Hình thức nhập lệnh: Nhập lệnh trực tiếp tại sàn, không hỗ trợ truyền lệnh từ xa;
- Hình thức khớp lệnh: Khớp lệnh định kỳ, tối đa 3 đợt /phiên;

Hệ thống lưu ký – đăng ký – thang toán bù trừ

Hệ thống lưu ký – đăng ký – thang toán bù trừ (gọi tắt là Hệ thống lưu ký) do TTGDCK TpHCM phối hợp với công ty FPT xây dựng. Hệ thống lưu ký không tích hợp hoàn toàn được với hệ thống giao dịch Thái Lan, mọi trao đổi thông tin giữa hai hệ thống phải được thực hiện qua một máy trạm trung gian. Cuối mỗi phiên giao dịch, máy chủ giao dịch đẩy kết quả giao dịch ra máy trạm trung gian dưới dạng file text. Máy chủ lưu ký đọc kết quả giao dịch này và đẩy vào CSDL Oracle.

- Hệ điều hành: Windows 2000 Server;
- Máy chủ: 2 máy IBM Netfinity
- Cơ sở dữ liệu: Oracle 8i
- Ngôn ngữ phát triển: Visual Basic 6; Crytal Report
- Giao thức mạng: TCP/Ip, FTP
- Import kết quả giao dịch từ máy trạm trung gian vào database để sử lý.
- Kết quả thanh toán bù trừ được kết xuất ra file Text và chuyển tới ngân hàng chỉ định thanh toán qua đường điện thoại Dialup bằng giao thức FTP (file transfer protocol)

Hệ thống công bố thông tin

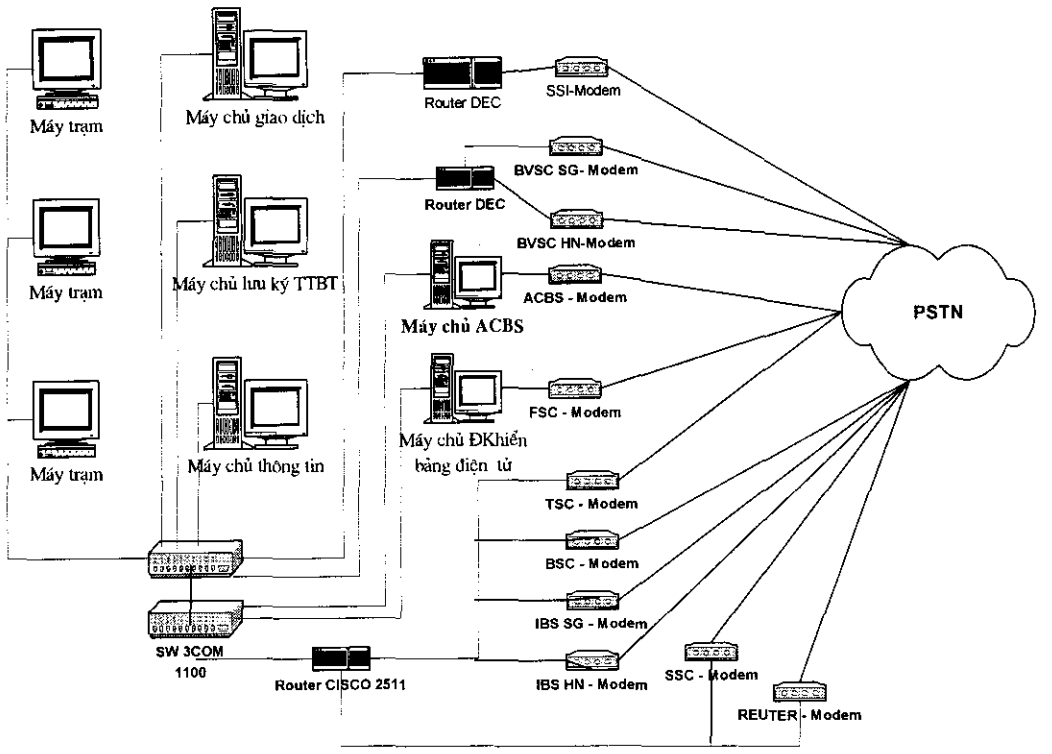
Hệ thống CBTT do TTGDCK TpHCM tự đầu tư trên cơ sở phần công bố thông tin vốn có của hệ thống Thái Lan.

Theo thiết kế ban đầu, hệ thống giao dịch Thái Lan có một phân hệ công bố thông tin. Các CTCK kết nối vào qua các Router đặc chủng do Thái Lan cung cấp và tải file kết quả giao dịch về. Đưa lên bảng điện tử cũng bằng phần mềm của Thái Lan.

Khi quy mô thị trường tăng lên, xuất hiện nhiều dạng nhu cầu nhận thông tin công bố. Hình thức công bố thông tin kể trên không còn phù hợp. Vì vậy TTGDCK TpHCM đã phát triển hệ thống Công bố thông tin lên một mức mới như sau:

- Đầu tư máy chủ công bố thông tin, CTCK kết nối vào máy chủ này để lấy kết quả giao dịch
- Thông tin công bố dưới hai dạng, file text và CSDL Oracle, file text được giữ nguyên như khi hệ thống giao dịch Thái Lan đẩy ra, còn CSDL đọc file text này và nạp vào database;

- CTCK được cung cấp một phần mềm đọc file text là chương trình 3 giá cho TTGDCK TpHCM viết chuyên dùng đẩy thông tin ra máy chiếu. Chương trình 3 giá hiển thị thông tin trạng thái thị trường, kết quả khớp lệnh dự kiến, đưa ra 3 giá chào mua, chào bán tốt nhất với khối lượng tương ứng



Hình vẽ: Mô hình kết nối thông tin tại TTGDCK TpHCM

1.1.2 Trang thiết bị phần cứng

+ Trading Srver (02): Máy chủ giao dịch thực hiện chức năng nhận lệnh giao dịch, khớp lệnh, kết xuất dữ liệu giao dịch ra dạng files text.

+ Clearing Server (và máy chủ dự phòng): Máy chủ lưu ký thực hiện chức năng quản lý tài khoản của các công ty chứng khoán, nhà đầu tư. Thực hiện xác nhận, thanh toán bù trừ cho các giao dịch chứng khoán, nhận số liệu kết qủa giao dịch từ máy hệ thống giao dịch, chuyển số liệu thanh toán sang ngân hàng chỉ định thanh toán.

+ BroadCast Server: thực hiện nhiệm vụ nhận dữ liệu từ máy chủ giao dịch để chuyển tới bảng điện tử của các công ty chứng khoán thông qua giao thức TCP/Ip, Message Queue, hiện tại có 2 công ty sử dụng bảng điện tử của Thái Lan cần nguồn dữ liệu này là Bảo Việt và Sài Gòn.

+ Information Server: Máy chủ công bố thông tin sử dụng hệ CSDL Oracle, lấy dữ liệu từ máy chủ giao dịch bằng phần mềm SecuOnline do

phòng Cnth tự phát triển, xử lý và truyền dữ liệu tới các công ty chứng khoán dưới dạng Text hoặc kết nối trực tiếp Oracle.

+ Router Cisco 2511: thực hiện quản lý truy cập từ xa, hiện có 16 cổng Asynch và 2 cổng Leased line, đã sử dụng hết.

Các kết nối này phục vụ cho việc lấy dữ liệu dạng file text hay Oracle thông qua Net8 hay TCP/Ip, riêng đường kết nối với UBCKNN để chạy Terminal theo dõi giao dịch, tuy nhiên hiện tại rất ít được sử dụng.

+ 02 Router DEC đặc chủng là của công ty chứng khoán SSI và BVSC phục vụ kết nối dự liệu bảng điện tử thông qua 3 bộ NTU (Modem Sync-Motorola) và máy chủ Broadcast server

+ 03 Switch 3COM 1100 (24 port) dùng để chuyển mạch mạng LAN.

+ 04 UPS Powereware 10 kva đảm báo cung cấp điện cho các máy chủ trong vòng 135 phút (120 phút giao dịch cộng với 15 phút khởi động hệ thống)

Các máy trạm liên quan trực tiếp đến hệ thống giao dịch bao gồm:

+ 2 máy của IT phục vụ Operator

+ 1 máy Backup cho máy chủ công bố thông tin

+ 22 máy của đạidiện giao dịch tại sàn (mỗi công ty thành viên được cấp 2 máy)

+ 3 máy của giám sát, quản lý giao dịch chạy MRTERM

1.1.3 Phần mềm

Chương trình giao dịch chứng khoán do Thái Lan viết gồm 3 phần lớn:

- DCTerm: chương trình thực thi nhập, xuất lệnh giao dịch của công ty chứng khoán từ sàn giao dịch
- MrTerm: Giám sát và kiểm tra giao dịch
- KearTerm: Vận hành, điều khiển hệ thống giao dịch

Chương trình lưu ký và thanh toán bù trừ:

- Môi trường phát triển: Windows 2000 server;
- Cơ sở dữ liệu: Oracle8i
- Ngôn ngữ phát triển: Visual Basic 6.0; Crytal report
- Thực hiện các chức năng quản lý tài khoản các công ty chứng khoán, xác nhận giao dịch, thanh toán bù trừ cho các giao dịch chứng khoán, nhận kết quả giao dịch từ hệ thống giao dịch, chuyển số liệu thanh toán sang Ngân hàng chỉ định thanh toán, cho phép kết nối từ các máy trạm trong mạng cục bộ TTGDCK thông qua TCP/IP và Net8

Chương trình SecuOnline

- Hệ điều hành: Windows 2000 server, Win9x; CSDL Oracle 8i
- Ngôn ngữ phát triển: Visual Basic
- Dùng để nạp dữ liệu giao dịch vào CSDL Oracle trên máy chủ công bố thông tin, nguồn dữ liệu là các file text do máy chủ giao dịch đẩy ra

Chương trình chuyển dữ liệu ra bảng điện tử cho các công ty chứng khoán (hay còn gọi là chương trình 3 giá)

- Hệ điều hành: Windows 2000 server, Win9x; CSDL dạng Text
- Ngôn ngữ phát triển: Visual Basic
- Dự liệu dạng file text được truyền tới một thư mục Sharing riêng trên máy chủ công bố thông tin, các công ty chứng khoán sẽ kết nối lên để tải về.

Chương trình 8cSend: chạy trên máy PC truyền dữ liệu ra bảng điện tử đặt tại sàn giao dịch.

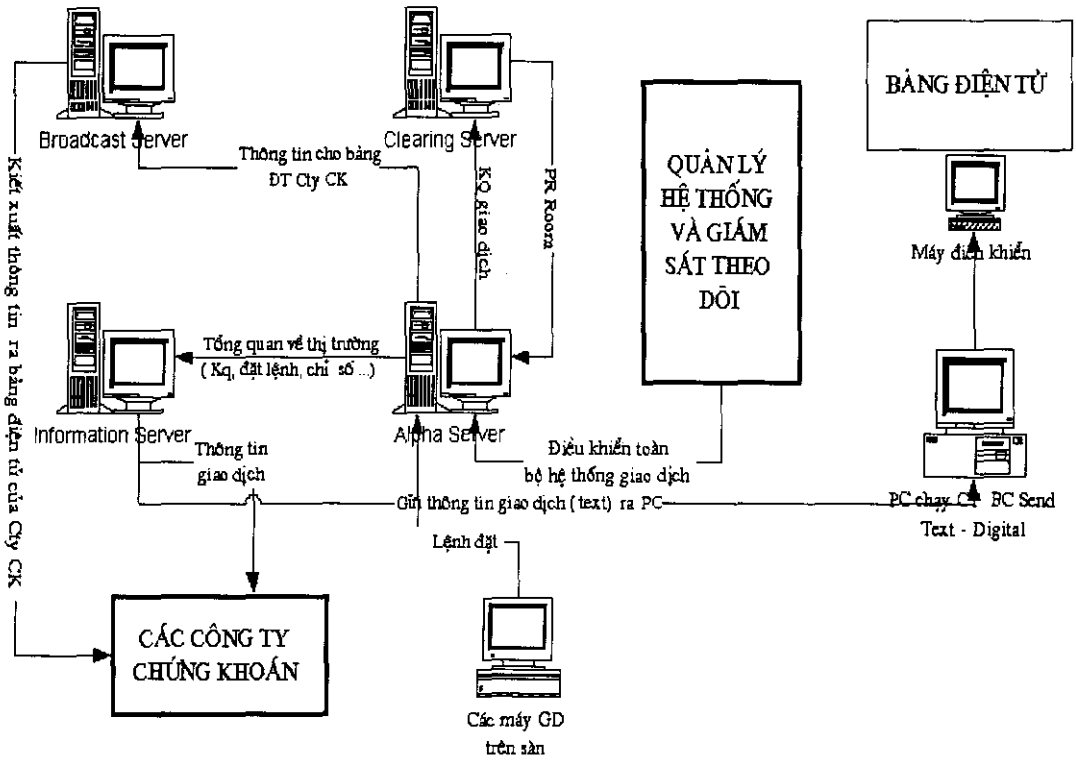
Chương trình CiscoSecure EasyACS: chạy trên trình duyệt Netcape Nevigator đưa ra danh sách các User đang kết nối vào hệ thống, thời gian kết nối v.v... Tuy nhiên không thể ngăn chặn được các kết nối này ngay cả khi chúng là bất hợp pháp.

Ngoài ra còn có các chương trình quản lý kho lưu ký, chương trình đấu thầu trái phiếu do UBCKNN viết.

1.2 Vấn đề an toàn dữ liệu

1.2.1 Lưu trữ dữ liệu

SƠ ĐỒ CHU CHUYỂN DỮ LIỆU GIAO DỊCH



Hình vẽ: sơ đồ chu chuyển luồng dữ liệu giao dịch

Hai máy chủ giao dịch sử dụng chung một bộ lưu trữ ngoài External, toàn bộ CSDL giao dịch được lưu tập trung tại đây. Khi máy chủ chính gặp sự cố, máy chủ dữ phòng được khởi động thay thế mà không cần phải thao lắp ổ cứng thủ công.

Các phân hệ trong hệ thống không trao đổi thông tin trực tiếp với nhau mà qua một máy trạm trung gian, dữ liệu trao đổi dạng file text:

- Cuối mỗi đợt, phiên giao dịch, máy chủ giao dịch đẩy kết quả giao dịch, sổ lệnh ra máy trạm trung gian
- Máy chủ lưu ký đọc dữ liệu từ file text và đẩy vào CSDL oracle SATS trên máy chủ lưu ký.
- Máy chủ lưu ký xử lý kết quả giao dịch, gửi kết quả thanh toán bù trừ bằng file text đến Ngân hàng chỉ định thanh toán
- Cuối mỗi ngày, máy chủ lưu ký đẩy dữ liệu đầu ngày (Foreign room) vào máy trạm trung gian, từ đó chuyển cho máy chủ giao dịch.

- Định kỳ, máy chủ công bố thông tin nạp kết quả giao dịch vào CSDL Oracle công bố thông tin.
- Máy chủ Công bố thông tin copy kết quả giao dịch (file text) từ máy trạm trung gian vào một thư mục cố định, phân quyền đọc cho CTCK
- CTCK kết nối từ xa đề lấy file text hoặc kết nối với cơ sở dữ liêu công bố thông tin (Oracle) trên máy Công bố thông tin

1.2.2 An toàn dữ liệu

Để đề phòng sự cố xảy ra, tất cả các dữ liệu quan trong đều được backup theo nhiều cách khác nhau:

Đối với dữ liệu trên máy chủ giao dịch

- Cuối mỗi phiên giao dịch, những thay đổi dữ liệu trong ngày sẽ được Backup vào Tapebackup dưới dạng File Text
- Cuối mỗi tuần, những thay đổi dữ liệu trong tuần sẽ được backup vào TapeBackup, nhìn chung khối lượng dữ liệu là không lớn chỉ khoản vài trăm Kb

Đối với dữ liệu trên máy chủ Lưu ký và thanh toán bù trừ: Cuối mỗi ngày, dữ liệu từ Oracle được Export và nén dưới dạng File *.Zip theo chương trình do FPT viết, các file Backup này được lưu trên các máy tính khác (không có đĩa CD hay Tapebackup) để khôi phục khi cần thiết. Phương pháp đang sử dụng hiện nay là rất khó khăn do tổng dung lượng một file Zip backup hiện đã lên đến khoảng trên 200Mb.

1.3. Vấn đề an ninh, bảo mật

Hệ thống mạng giao dịch tại TTGDCK tpHCM không có thiết bị bảo mật cũng như mã hoá thông tin, không có tường lửa chặn trước và chặn sau do đó rất dễ bị tấn công từ bên ngoài. Hiện tại chỉ có một chương trình phần mềm duy nhất là CiscoSecue Easy ACS cho phép ghi lại thời điểm, tên User kết nối vào hệ thống, nhưng lại không cho phép ngăn chặn các kết nối này khi cần thiết.

Hệ thống giao dịch được tách riêng với các hệ thống khác và với bên ngoài. Dữ liệu giao dịch được máy chủ giao dịch đẩy sang một máy máy trạm trung gian và các phân hệ khác chỉ truy xuất thông tin gián tiếp trên máy trạm này.

Biện pháp bảo vệ chủ yếu hiện nay là phân quyền truy cập đến từng người tham gia vào hệ thống. Hệ thống giao dịch có các loại quyền truy cập như sau:

- Quyền Supper Admin: Quyền truy cập hệ thống tối cao do phía Thái lan nắm giữ.

- Quyền Admin: do cán bộ tin học nắm.
- Các loại quyền khác như quyền trưởng nhóm, quyền User thông thường cấp cho từng người với chức năng, nhiệm vụ khác nhau.
- Các công ty chứng khoán được kết nối vào hệ thống và tới máy chủ công bố thông tin thông qua modem riêng và Router 2511 đặt tại TTGDCK. Việc bảo mật thông tin và quản lý người truy cập này trước mắt chỉ bằng Username và Password do trung tâm cung cấp.

II. Thực trạng hệ thống máy tính tại TTGDCKHN

2.1. Tổng quan hệ thống máy tính tại TTGDCKHN

2.1.1 Mô hình hệ thống

Hệ thống tin học tại TTGDCKHN là hệ thống giao dịch cổ phiếu các doanh nghiệp vừa và nhỏ. Theo đó các doanh nghiệp có vốn điều lệ từ 5 tỷ đến dưới 30 tỷ đồng và từ 30 tỷ đồng trở lên nhưng không đủ điều kiện niêm yết tại Trung tâm GDCK Tp. Hồ Chí Minh sẽ được đăng ký giao dịch tại Trung tâm GDCK Hà Nội.

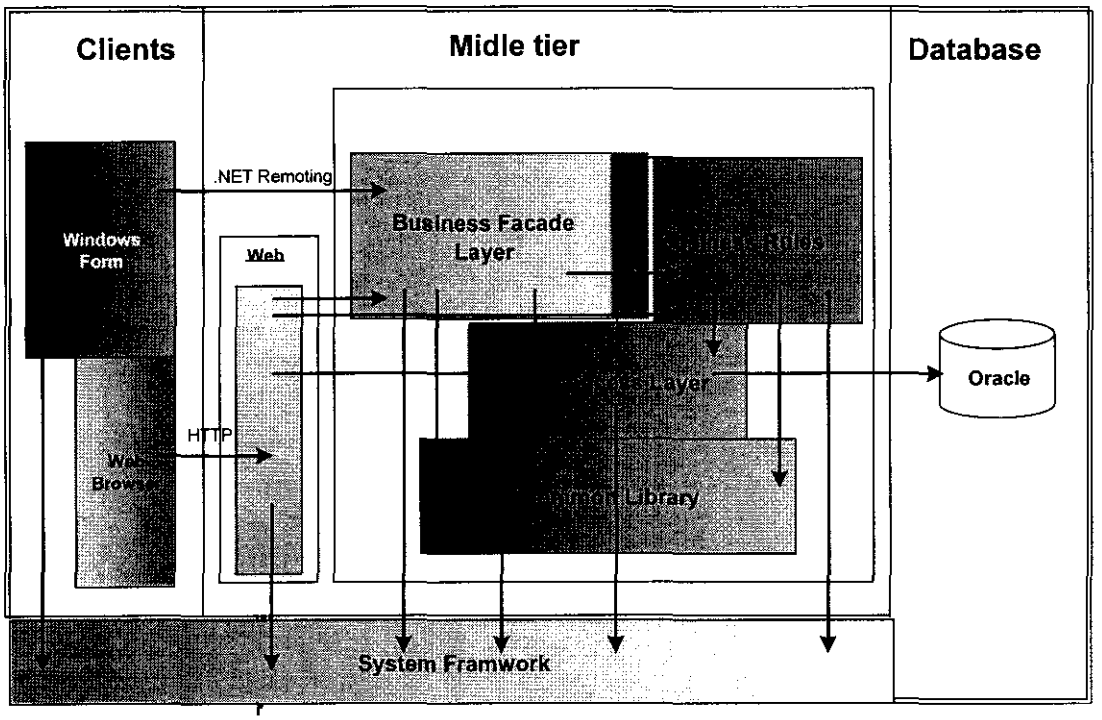
Cơ chế giao dịch trước mắt được xác định là nhập lệnh trực tiếp thông qua đại diện giao dịch tại sàn, thực hiện theo nguyên tắc báo giá trung tâm và giao dịch thoả thuận. Báo giá trung tâm là hệ thống giao dịch chính, áp dụng cho các giao dịch lô chẵn (100 cổ phiếu hoặc 100 trái phiếu). Giao dịch thoả thuận ngoài giờ thực hiện các giao dịch lô lớn (từ 10.000 cổ phiếu hoặc trái phiếu trở lên).

Hệ thống giao dịch được chia làm hai phần chính, phần mạng LAN phục vụ giao dịch tại sàn và phần kết nối mạng WAN phục vụ công bố thông tin đến công ty chứng khoán. Dữ liệu từ trong mạng LAN sẽ truyền một chiều ra ngoài cho các công ty chứng khoán, không có chiều ngược lại. Cơ chế này đảm bảo hệ thống bên trong không bị lây nhiễm virus hay bị Harker tấn công từ bên ngoài.

Ngoài ra, Trung tâm còn có một mạng văn phòng nội bộ, có kết nối internet nhưng tách riêng hoàn toàn với các hệ thống khác.

Mạng LAN giao dịch tại TTGDCKHN

Toàn bộ Hệ thống được xây dựng trên nền hệ điều hành Windows 2003 advance Server, cơ sở dữ liệu Oracle 9i, theo mô hình 3 lớp Client-WEB(Application) Server-Database. Đây là một mô hình hiện đại, có tính mở rất cao. Khi điều kiện cho phép có thể dễ dàng nâng cấp và mở hệ thống giao dịch từ xa mà không cần phải thay đổi kiến trúc mạng.



Hình vẽ: Kiến trúc hệ thống tại TTGDCKHN

Trung tâm của mô hình này là một máy chủ ứng dụng Application server. tất cả các yêu cầu xử lý từ máy trạm sẽ chuyển về đây. Application server sẽ quản lý hàng đợi và phân phối yêu cầu sử lý cho từng máy chủ database.:

- Máy trạm đại diện giao dịch, quản lý giao dịch đồng bộ sử lý với máy chủ ứng dụng bằng cơ chế đồng bộ Net Remotting của Net framework 1.1;
- Máy trạm công bố thông tin, máy trạm giám sát sử dụng giao diện WEB, khi đó Máy chủ Application -server đóng vai trò là WEB-server
- Các sử lý sẽ được máy Application server chuyển tiếp cho máy chủ database của 4 phân hệ, sử lý trực tiếp trên database.
- Kết quả sử lý được trả về cho máy Application server rồi chuyển tiếp cho máy trạm.
- Giao thức mạng: TCP/IP, Oracle Net 8i/9i.

Mạng WAN kết nối đến CTCK

Phần kết nối mạng đến công ty chứng khoán là một bộ phận rất quan trọng trong tổng thể hệ thống tin học của TTGDCKHN, cho phép các CTCK có thể kết nối lên TTGDCKHN để lấy thông tin công bố.

- Sổ lệnh giao dịch trực tuyến

- Kết quả giao dịch
- Các loại thông tin thị trường khác

Do hệ thống của TTGDCKHN hiện chưa triển khai hỗ trợ giao dịch từ xa nên TTGDCKHN không quy định bắt buộc cũng như không triển khai đường kết nối đến tận các CTCK. TTGDCKHN chỉ hỗ trợ bằng cách cung cấp sẵn các cổng kết nối trên Router cho CTCK tự kết nối vào.

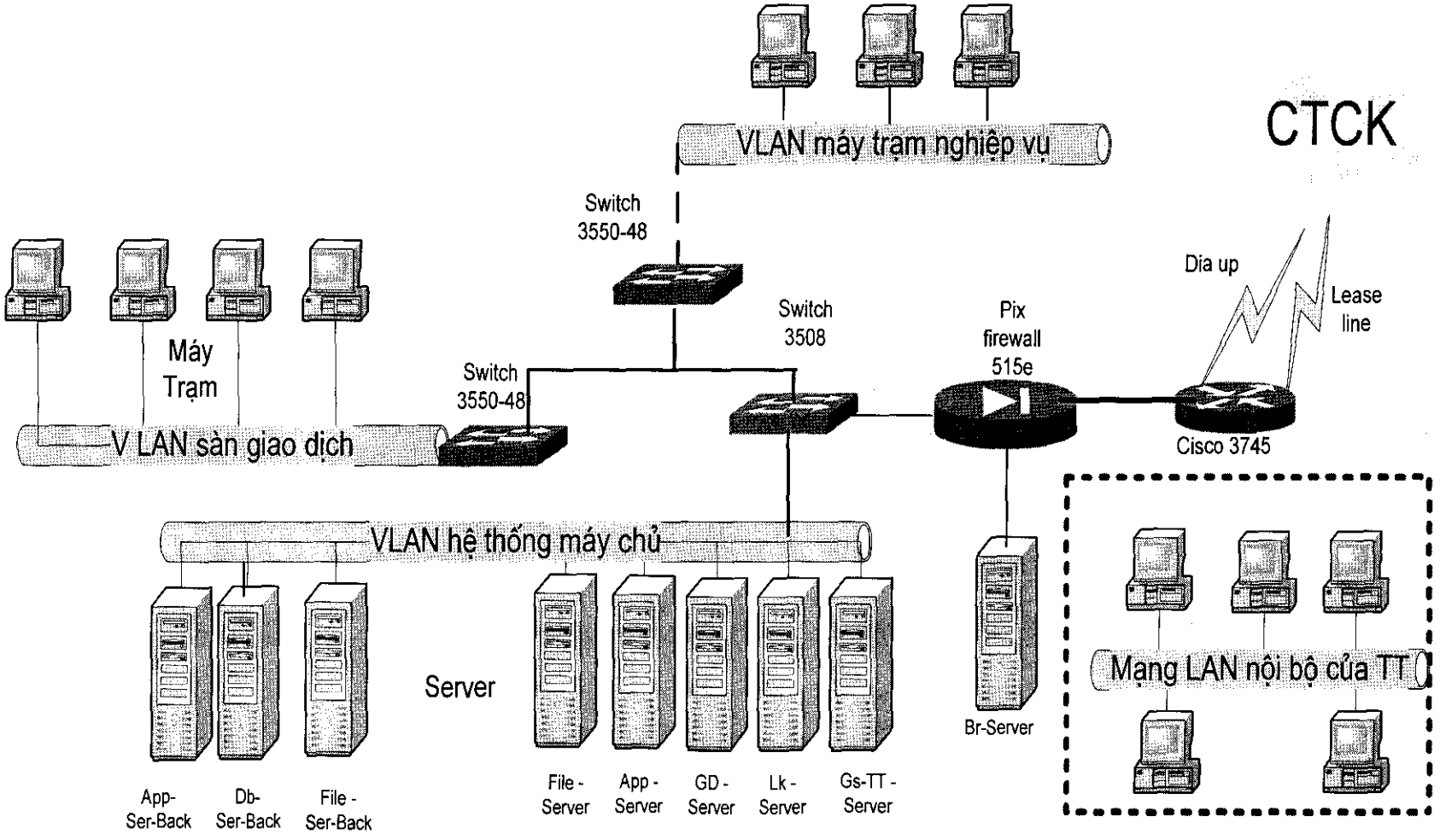
Thiết bị trung tâm phục vụ kết nối WAN tại TTGDCK Hn là Router Cisco 3745, gồm có 3 modul chính

- 02 synchronous Modul 8 port: tổng cộng 16 cổng kết nối cho đường Leased line
- 01 asynchronous modul 16 port: tổng cộng 16 cổng cho kết nối điện thoại Dialup.

Các thiết bị hiện có đã sẵn sàng, cho phép công ty chứng khoán tự lựa chọn một trong hai hình thức kết nối phổ biến tại Việt Nam là Leased line và Dialup. Không những thế, năng lực hiện tại của Router còn cho phép nâng cấp đường truyền WAN lên sử dụng công nghệ Frame Relay hoặc công nghệ kết nối điểm- đa điểm E1.

Ngoài ra để đảm bảo vấn đề an ninh, TTGDCKHN còn sử dụng thiết bị PixfireWall 515e và phần mềm ACS 3.2 để quản lý kết nối của CTCK. Đảm bảo phân quyền cho các công ty chứng khóan chỉ cho phép kết nối đến máy chủ công bố thông tin chứ không được truy xuất trực tiếp vào hệ thống các hệ thống khác (chi tiết xin xem ở mục .....-Vấn đề an ninh-bảo mật).

MÔ HÌNH TỔNG THỂ HỆ THỐNG TIN HỌC TTGDCKHN



2.1.2 Trang thiết bị phần cứng

Hệ thống máy chủ:

Gồm 9 máy chủ:

- 02 Máy chủ quản trị mạng và dự phòng: HP ML 350: thực hiện chức năng quản trị mạng, Domain Controller, ngoài ra nó còn quản lý danh sách truy cập hệ thống (access List) cho Router bằng phần mềm ACS 3.2
- 02 Máy chủ ứng dụng và dự phòng: HP ML 370: máy chủ trung tâm xử lý ứng dụng và quản lý truy xuất cơ sở dữ liệu;
- 01 Máy chủ Database giao dịch: HP ML 370: Lưu trữ cơ sở dữ liệu giao dịch;
- 01 Máy chủ Database lưu ký: HP ML 370: Lưu trữ cơ sở dữ liệu lưu ký;
- 01 Máy chủ Database giám sát: HP ML 350: Lưu trữ cơ sở dữ liệu giám sát và thông tin thị trường;
- 01 máy chủ database dự phòng HP ML 350: Lưu cở sở dữ liệu dự phòng cho cả 4 phân hệ.
- 01 máy chủ công bố thông tin: HP ML 350: Công bố thông tin đến các công ty chứng khoán.

Hệ thống máy trạm

Tổng cộng 41 máy, bao gồm:

- 30 máy cho CTCK
- 07 máy cho giám sát giao dịch
- 01 máy điều khiển bảng điện tử
- 03 máy điều khiển

Mỗi công ty chứng khoán được trạng bị 3 máy trạm nhập lệnh, một máy FAX và một máy In. Tổng cộng thiết bị hiện có đủ cho 10 công ty chứng khoán.

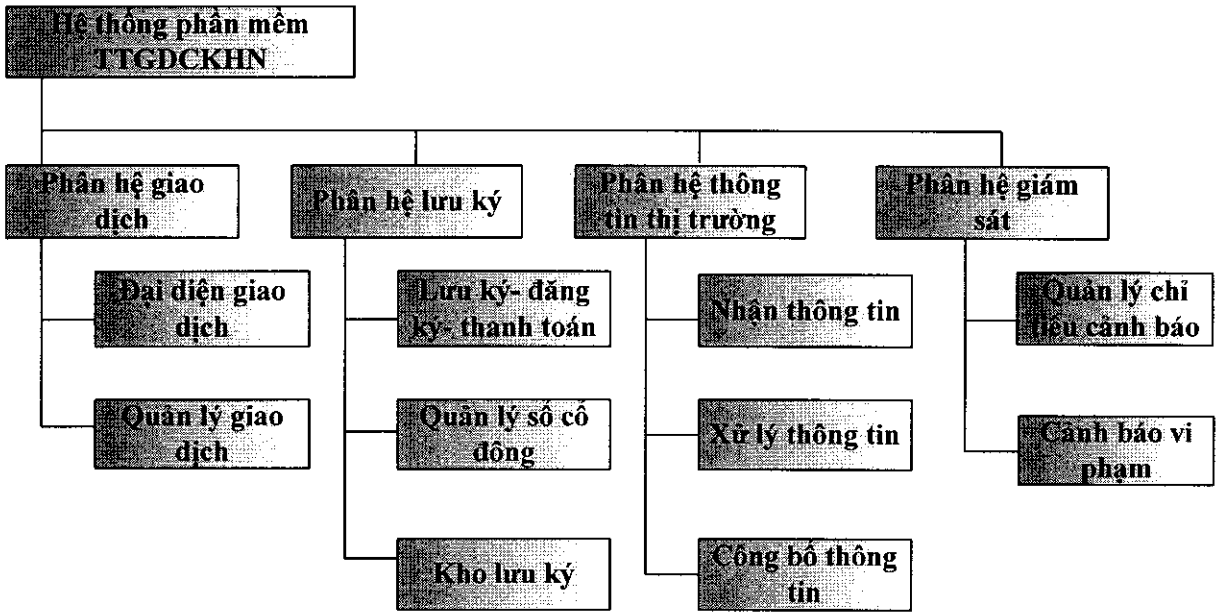
Các thiết bị mạng Khác

- 01 Router Cisco 3745
- 01 Switch 3508G dùng cho kết nối cáp quang giữa các máy chủ
- 02 Switch 3500-48port: Dùng cho kết nối các máy trạm, các thiết bị tin học khác

- 01 PIXfirewall 515e: Thiết bị bảo mật mạng

2.1.3. Phần mềm

Phần mềm giao dịch chứng khoán do Công ty FPT phát triển, TTGDCKHN là đơn vị chủ đầu tư. Gồm 4 phân hệ :



Phân hệ Giao dịch: Thực hiện chức năng giao dịch theo mô hình đã quy định. Phân hệ Giao dịch được vận hành theo hai khối tính năng sử dụng: dành cho đại diện giao dịch và dành cho cán bộ quản lý giao dịch.

+ Khối chức năng dành cho cán bộ quản lý giao dịch có nhiều tham số định nghĩa về các tiến trình giao dịch, biên độ giá giao dịch, mức trần giao dịch của các nhà đầu tư nước ngoài (foreign room), cho phép sửa hủy lệnh, theo dõi và báo cáo kết quả giao dịch trong ngày.

+ Khối chức năng dành cho đại diện giao dịch gồm các chức năng nhập, xác nhận, sửa hủy lệnh, quan sát diễn biến và kết quả giao dịch, đăng quảng cáo giao dịch thỏa thuận, phục vụ cho việc nhập lệnh vào hệ thống.

Phân hệ Giám sát: Là phân hệ được thiết kế riêng cho cán bộ Giám sát của Trung tâm, có chức năng theo dõi các tiến trình giao dịch, cài đặt tham số giám sát theo 80 tiêu chí giám sát trực tuyến có cảnh báo tức thời và giám sát, kiểm tra sau giao dịch. Ngoài ra, phân hệ giám sát có chức năng thống kê số liệu diễn biến thị trường theo thời gian định sẵn và có các báo cáo theo mẫu định dạng sẵn cũng như theo định nghĩa của người sử dụng, có khả năng kết nối để tìm kiếm và chia sẻ thông tin với các phân hệ trong hệ thống.

Phân hệ Đăng ký lưu ký và thanh toán bù trừ: Có các chức năng thực hiện nghiệp vụ xử lý sau giao dịch, bao gồm xử lý số liệu giao dịch nhận từ phân hệ giao dịch, xác nhận và thông báo chi tiết kết quả đến các thành viên lưu ký, quản lý trần giao dịch của nhà đầu tư nước ngoài và cập nhật cho phân hệ giao dịch, quản lý kho chứng khoán và sổ cổ đông, thực hiện quyền của nhà đầu tư. Phân hệ này được thiết kế linh hoạt, phục vụ cho cả ba hình thức bù trừ thanh toán đa phương, song phương và trực tiếp, đáp ứng cho các phương thức giao dịch khác nhau trên hệ thống giao dịch.

Phân hệ Thông tin thị trường: Là phân hệ có chức năng quản lý việc cung cấp thông tin cho các công ty chứng khoán, công bố thông tin cho nhà đầu tư và công chúng thông qua các giao diện trang thông tin điện tử và bảng điện tử trên sàn. Phân hệ thông tin có thể lấy các thông tin từ hệ thống giao dịch đưa ra, cũng có thể lấy các thông tin từ nguồn bên ngoài, bảo đảm sự công bằng trong việc tiếp cận thông tin của các đối tượng tham gia trên thị trường.

Phân hệ Thông tin thị trường có hai phần:

- Thông tin thị trường nội bô, phục vụ hoạt động nghiệp vụ của bản thân TTGDCKHN
- Công bố thông tin tới CTCK

2.2. Vấn đề an toàn dữ liệu

2.2.1. Lưu trữ dữ liệu

Toàn bộ dữ liệu của TTGDCKHN được lưu trữ tập trung trên hệ quản trị cở sơ dữ liệu Oracle. Mỗi phân hệ có một Database riêng nhưng có sự trao đổi với nhau. Thực chất có thể coi là một.

Hệ thống có 5 Oracle database, mỗi database có tiến trình quản lý riêng, được đặt tên khác nhau:

STS (đặt trên máy chủ CSDL giao dịch): CSDL giao dịch, lưu trữ kết quả giao dịch và sổ lệnh giao dịch trong vòng 30 ngày. Quá thời hạn trên, dữ liệu sẽ được chuyển sang lưu trữ ở TapeBackup

SUSTS (Đặt trên máy chủ CSDL giám sát-công bố thông tin): CSDL giám sát, dữ liệu đầu vào lấy từ CSDL giao dịch và dữ liệu tập hợp mà cán bộ giám sát nhập vào hàng ngày.

InfO (Đặt trên máy chủ CSDL giám sát-công bố thông tin): CSDL thông tin thị trường, lưu trữ dữ liệu của phân hệ thông tin thị trường, lấy thông tin từ CSDL tất cả các phân hệ khác.

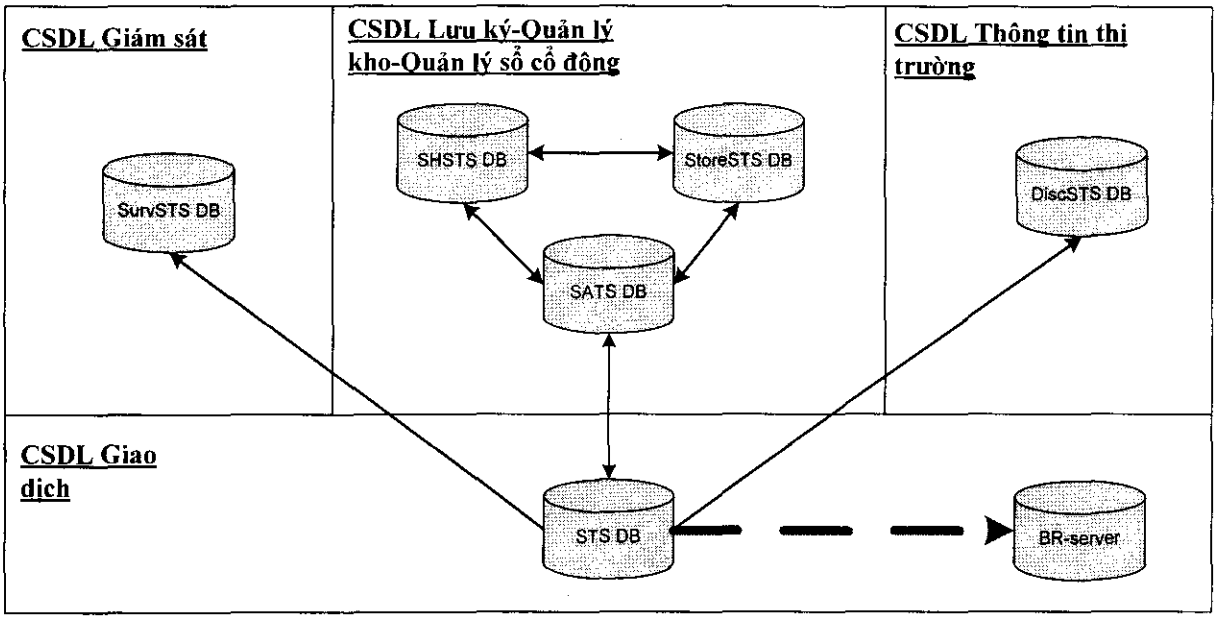
SATS (đặt trên máy chủ CSDL lưu ký): CSDL phân hệ lưu ký-đăng ký-thanh toán bù trừ: gồm 3 CSDL thành phần:

SATS- CSDL phân hệ lưu ký, cấu trúc CSDL này gần giống với dữ liệu phân hệ lưu ký của TTGDCK TpHCM, có nâng cấp cho phù hợp với TTGDCKHN.

StoreSTS: CSDL phân hệ quản lý kho lưu ký

SHSTS: CSDL phân hệ quản lý sổ cổ đông (thuộc phân hệ lưu ký), là phân hệ phát triển mới để hỗ trợ các nghiệp vụ liên quan đến lưu ký chứng khoán chưa đăng ký giao dịch tại TTGDCKHN, đặc biệt là nghiệp vụ đại lý chuyển nhượng.

Br-Server (đặt trên máy chủ CBTT): CSDL trung gian để gửi các thông tin công bố đến các CTCK. Máy chủ ứng dụng sẽ chịu trách nhiệm trích xuất dữ liệu từ các phân hệ bên trong và gửi ra CSDL Br-server



Hình vẽ: Mô hình tổ chức dữ liệu tại TTGDCKHN

2.2.2 An toàn dữ liệu

Để đảm bảo cho thị trường được vận hành liên tục, dữ liệu của TTGDCKHN được Backup sau mỗi phiên giao dịch, trong thời gian sử lý cuối ngày. Có hai hình thức Backup hiện đang được áp dụng:

Backup dữ liệu định kỳ bằng Tool BACKUP MANAGER:

Tool BACKUP MANAGER do FPT phát triển nhằm mục đích thực hiện Sao lưu đầy đủ các file dữ liệu của CSDL của Oracle theo cơ chế Sao lưu lạnh. Backup toàn bộ các file CSDL hiện có ra tape Backup và mang đi lưu trữ ở chỗ khác.

Cơ chế sao lưu theo các bước sau:

- B1: Xác định Instance Oracle cần sao lưu (cả 5 Database kể trên)
- B2: Xác định các file của CSDL đó, bao gồm: Datafile, Redolog file, Control file v.v... Các thông số được khai báo trong file .INI của Tool
- B3: Khi thực hiện sao lưu các
    - Kích hoạt chức năng sao lưu
    - Instance đó sẽ được Stop lại
    - Backup các các file đã chỉ định trong .INI
    - ZIP các file đó lại
    - COPY sang Tape backup
    - Start Instance vừa sao lưu trở lại
- B4: Khôi phục dữ liệu
    - Copy file dữ liệu cần khôi phục vào thư mục dùng để khôi phục
    - Kích hoạt chức năng phục hồi
    - Instance đó sẽ tự động stop lại
    - Hệ thống sẽ gỡ nén để các file chỉ định để phục hồi
    - Copy các file đó đè nên các file đang hoạt động của CSDL
    - Start lại Instance.

Backup dữ liệu bằng phương pháp Export, Import

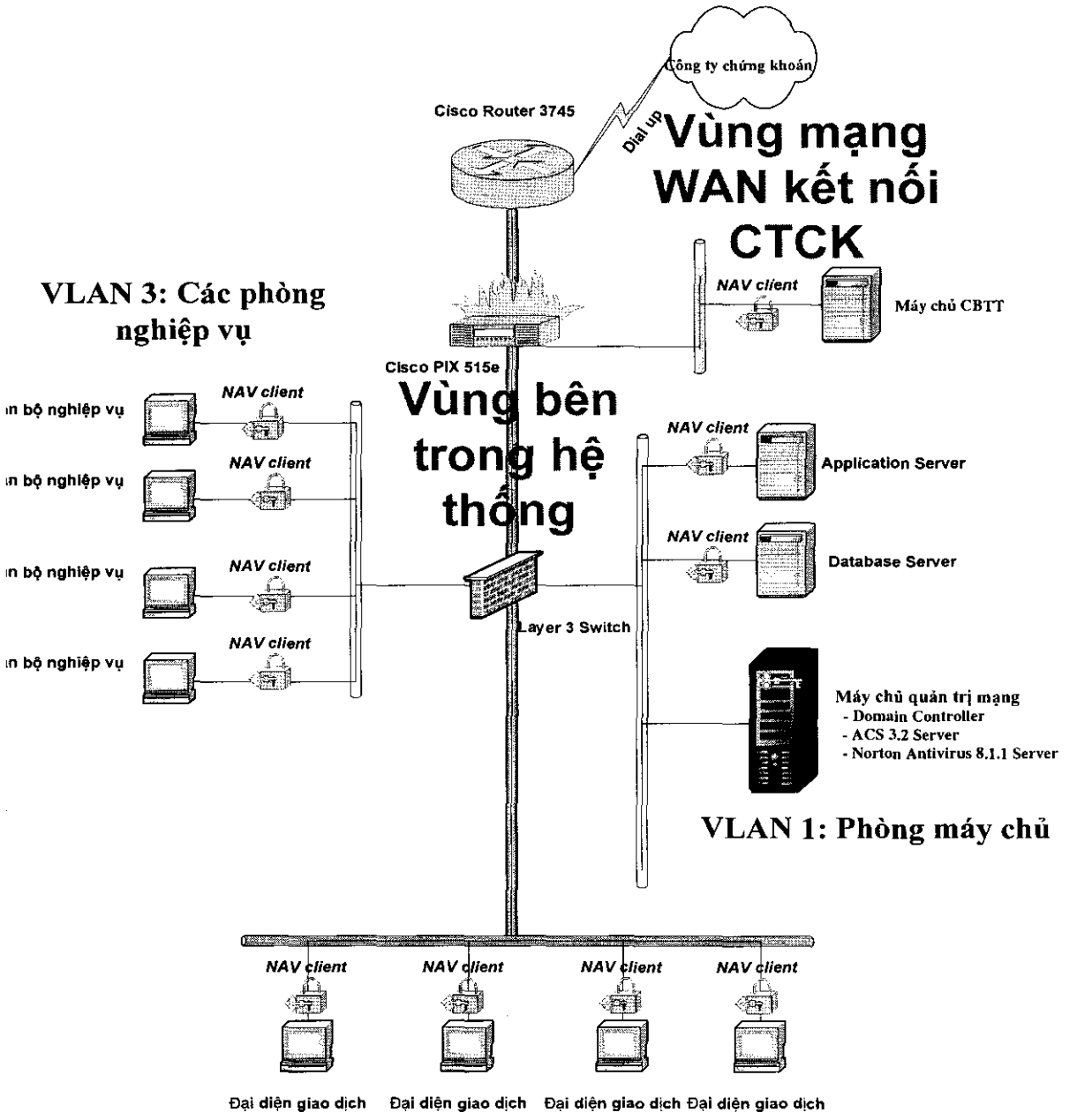
IMPORT, EXPORT thường sử dụng như một phần của kế hoạch sao lưu dữ liệu. Việc thực hiện sao lưu nóng, hay sao lưu đầy đủ thường áp dụng để sao lưu toàn bộ CSDL. Nhưng có một số trường hợp ta chỉ cần sao lưu hoặc phục hồi một bảng nào đó thì việc sử dụng giải pháp sao lưu đầy đủ là

không hợp lý. Vì vậy, chỉ có giải pháp sử dụng Import & Export là hợp lý nhất.

Trong trường hợp TTGDCKHN, Các đối tượng sau sau được thực hiện kết xuất hàng ngày:

- CSDL Giao dịch (Instance = STS,User = STS,Password)
- CSDL Thông tin (Instance = INFO,User = INFO;Password)
- CSDL Giám sát (Instance = SUSTS, User = SUSTS; Password)
- CSDL Lưu ký (Instance = SATS, User = SATS; Password)
- CSDL Sổ cổ đông (Instance = SHSTS, User = SHSTS; Password)
- CSDL Kho LK (Instance = STORE, User = STORE; Password)

2.3>. Vấn đề an ninh, bảo mật



Hình vẽ: Mô hình bảo mật của TTGDCKHN

Đặc điểm lớn nhất của hệ thống tin học tại TTGDCKHN đó là hệ thống đóng, không cho phép các CTCK đặt lệnh từ xa, cũng như không có kết nối Internet, tuy nhiên nhu cầu mở hệ thống giao dịch từ xa là tất yếu. Vì vậy chính sách an ninh bảo mật của TTGDCKHN phải đảm bảo cho nhu cầu giao dịch hiện tại, đồng thời phải có khả năng nâng cấp khi cần thiết.

Trong gian đoạn hiện nay, chính sách an ninh, bảo mật được xây dựng theo hướng giải quyết 3 vấn đề cơ bản sau:

Xác thực người dùng đối với phần kết nối WAN công bố thông tin ra CTCK: xác thực và trao quyền cho CTCK được kết nối đến đến máy chủ Công bố thông tin, nhưng không được phép truy cập sâu vào các phân hệ khác.

- CTCK phải có Username và Passwork do TTGDCKHN cấp mới kết nối vào được Router Cisco 3745

- Việc xác thực User được thực hiện động bộ qua Router Cisco và phần mềm ACS 3.2

- CTCK chỉ được kết nối vào máy chủ Công bố thông tin, qua cổng FTP. Mọi cổng kết nối khác sẽ bị Pixfirewall chặn.

- Kết quả giao dịch được đẩy một chiều từ vùng trong ra vùng bên ngoài hệ thống. Không có chiều ngược lại (Kiểm soát bằng Access list của PIX firewall 515e).

Đảm bảo an ninh nội bộ: Theo thống kê của các tổ chức nghiên cứu trên thế giới, khoảng 70% rủi ro an ninh mạng đến từ bên trong hệ thống. Một người xấu, hay thậm chí chỉ là sự tò mò vô tình thông thường của đại diện giao dịch cũng có thể làm sập hệ thống.

- Hệ thống chia thành 3 mạng LAN, mỗi VLAN có một chính sách quản trị khác nhau, tương ứng với quyền khác nhau. Khi cần người quản trị có thể cô lập tuyệt đối một VLAN bằng Access list của Layer3 Switch.

+ VLAN1: phòng máy chủ và bộ phận IT

+ VLAN2: sàn giao dịch

+ VLAN3: Các phòng nghiệp vụ

- Quản trị hệ thống dựa trên Domain

- Quản trị Username và Password tập trung theo từng nhóm. Mỗi người dùng muốn lấy thông tin phải có 2 loại tài khoản khác nhau: tài khoản của quản trị mạng cấp và tài khoản của trưởng nhóm các phân hệ cấp (sử dụng phần mềm giao dịch).

Chống Virus, Worms, Troijans: Cùng với sự tiến bộ của Internet, các loại virus máy tính xuất hiện ngày càng nhiều, càng ngày càng nguy hiểm hơn. Một số loại worm có thể lây nhiễm và làm sập hệ thống chỉ trong vòng vài Phút.

- Phòng chống Virus bằng phần mềm diệt virus Norton Antivirus Corporation 8.1, cài đặt trên tất cả các máy tính trong hệ thống, quản trị tập trung trên máy chủ quản trị mạng.

Update các bản vá lỗi (hotfix) định kỳ 1 tuần 1 lần, hoặc ngay khi nhận được cảnh báo từ nhà cung cấp.

CHƯƠNG 3:CÁC GIẢI PHÁP NHẰM NÂNG CAO TÍNH AN TOÀN CHO HỆ THỐNG MÁY TÍNH CỦA TTGDCK

I. Định hướng chiến lược xây dựng hệ thống.

Trong thời kỳ công nghệ thông tin phát triển nhanh chóng như hiện nay, việc ứng dụng CNTT vào hoạt động và quản lý của tất cả các lĩnh vực trong nền kinh tế là điều không thể thiếu. Như chúng ta đã biết trong giai đoạn hiện nay công nghệ thông tin (CNTT) là một công cụ hỗ trợ cực kỳ quan trọng trong quá trình hoạt động và phát triển của hầu hết các thị trường chứng khoán (TTCK) trên thế giới. Hầu hết mọi hoạt động của ngành chứng khoán đều được thực hiện trên hệ thống mạng máy tính và hệ thống máy tính cũng đã giúp cho công tác điều hành, quản lý lưu trữ dữ liệu được thực hiện một cách nhanh chóng. Vì vậy công tác bảo mật dữ liệu của ngành chứng khoán phải được quan tâm đặc biệt nhằm bảo vệ các thông tin quan trọng giúp cho thị trường chứng khoán hoạt động một cách an toàn và đảm bảo. Tính an toàn và bảo mật hệ thống CNTT là điều rất quan trọng liên quan đến việc bảo vệ nhà đầu tư và đảm bảo cho thị trường chứng khoán hoạt động tốt. Do đó việc điều hành, quản lý và phát triển của hệ thống với sự sử dụng kỹ thuật mã hóa, các kỹ thuật bảo mật, kèm theo các giải pháp thiết bị hợp lý sẽ là một yếu tố vô cùng quan trọng giúp cho thị trường chứng khoán hoạt động một cách an toàn và hiệu quả.

Định hướng một chiến lược xây dựng hệ thống về công nghệ thông tin nói chung và đối với lĩnh vực chứng khoán nói riêng phải có sự thống nhất, phù hợp và đặc biệt là phải gắn chặt với chiến lược phát triển của ngành. Thị trường chứng khoán Việt nam là một thị trường mới hình thành, đang từng bước phát triển, do vậy việc xây dựng một hệ thống CNTT có tính mở, ổn định, phù hợp với định hướng phát triển thị trường là rất cần thiết. Xây dựng hệ thống CNTT cần tuân theo những tiêu chí sau:

1.1. Gắn chặt việc xây dựng hệ thống CNTT với từng giai đoạn phát triển của thị trường.

Công nghệ thông tin là công cụ hỗ trợ trong hoạt động, điều hành quản lý của thị trường, do vậy khi xây dựng một hệ thống về CNTT phải cần được tính toán các yêu cầu đặt ra đối với hệ thống. Mỗi giai đoạn phát triển (về quy mô, tính chất) của thị trường sẽ kèm theo là một giải pháp CNTT phù hợp. Xây một hệ thống CNTT phù hợp với định hướng phát triển của ngành sẽ tránh được lãng phí khi đầu tư , mặt khác sẽ đảm bảo được tính ổn định, an toàn của hệ thống.

1.2. Lựa chọn công nghệ phù hợp với quy mô thị trường

Trong điều kiện tình hình thị trường chứng khoán của Việt nam hiện nay thì việc lựa chọn giải pháp công nghệ trong quá trình xây dựng hệ thống CNTT là đòi hỏi cấp thiết. Thị trường chứng khoán đang trong giai đoạn đầu phát triển, quy mô thị trường còn nhỏ, mặt khác sự phát triển về các giải pháp công nghệ thông tin luôn thay đổi và diễn ra từng ngày. Do vậy lựa chọn giải pháp công nghệ phù hợp với quy mô thị trường sẽ tiết kiệm rất nhiều trong đầu tư, đem lại hiệu quả kinh tế và hiệu suất sử dụng hệ thống

1.3. Xây dựng hệ thống có tính mở cao, sẵn sàng đảm bảo khả năng mở rộng, nâng cấp khi quy mô thị trường thay đổi.

Đây là một tiêu chí quan trọng trong quá trình xây dựng hệ thống CNTT. Một hệ thống CNTT hoàn chỉnh, hiệu quả là một hệ thống đáp ứng tốt các yêu cầu đặt ra thì còn phải có tính mở. Với sự phát triển CNTT nhanh chóng như hiện nay thì một hệ thống dù khá hiện đại tại thời điểm này đã lại lạc hậu tại thời điểm khác (chỉ khoảng vài năm). Do vậy nhu cầu nâng cấp hệ thống để đáp ứng được những yêu cầu mới là tất yếu.

1.4. Xây dựng chính sách quản lý hệ thống CNTT

Chính sách quản lý và vận hành hệ thống hợp lý sẽ tăng cường được khả năng ổn định, hiệu quả và an toàn cho hệ thống. Dù một hệ thống có hiện đại, an toàn đến đâu mà không xây dựng được một chính sách quản lý và vận hành hệ thống phù hợp thì nguy cơ rủi ro đối với hệ thống là rất lớn. Chẳng hạn như nếu không có một chính sách lưu trữ dữ liệu (backup) thì khi xuất hiện sự cố (bị mất, hỏng hệ thống) thì việc phục hồi lại dữ liệu là rất khó khăn (đặc biệt khi có dữ liệu lớn).

1.5. Chương trình đào tạo nguồn nhân lực về CNTT

Nhân lực về CNTT là một yếu tố then chốt, ảnh hưởng trực tiếp đến khả năng vận hành và hoạt động của hệ thống CNTT. Khi triển khai xây dựng một hệ thống CNTT, đi kèm theo đó là lập kế hoạch đào tạo, nâng cao trình độ của cán bộ CNTT. Xây dựng được một đội ngũ cán bộ tin học có đủ trình độ, năng lực để vận hành và khai thác có hiệu quả các hệ thống phần mềm ứng dụng phục vụ ngành chứng khoán, TTGDCK cần chú trọng đầu tư thích đáng trong công tác đào tạo, có chính sách động viên, khuyến khích cán bộ tin học an tâm phục vụ lâu dài ngành chứng khoán.

II. Các giải pháp nhằm nâng cao tính an toàn, bảo mật của hệ thống.

Bắt đầu từ năm 2000, công nghệ an toàn bảo mật thông tin đã có sự chuyển hướng rõ rệt từ an toàn và bảo mật cho mạng sang mức cao hơn là an toàn và bảo mật cho lớp ứng dụng. Trước đây khi xây dựng giải pháp an

toàn, bảo mật cho một hệ thống thông tin thì các sản phẩm về Firewall, Virtual Private Network, Anti-virus, Line Encryption thường được đề cập đến nhiều nhất và được cân nhắc để đưa vào hệ thống, còn ngày nay, các sản phẩm đó đã trở thành chuẩn cho một hệ thống thông tin và là các thành phần bắt buộc phải có. Công nghệ an toàn bảo mật chuyển sang mức ứng dụng để có thể bảo vệ tốt hơn cho người dùng, các giải pháp về Public Key Infrastructure, Authentication/Authorization, Application Firewall, Intrusion Protection System đang được quan tâm đến nhiều nhất để có thể xây dựng một hệ thống thông tin an toàn.

Hiện nay, chứng khoán là một ngành rất quan trọng của các quốc gia có nền kinh tế thị trường. Ngành chứng khoán là một ngành nhạy cảm và có ảnh hưởng vô cùng quan trọng đối với toàn bộ nền kinh tế. Vì vậy, các quốc gia trên thế giới đều có sự đầu tư rất lớn về công nghệ để không ngừng thúc đẩy sự phát triển của ngành công nghiệp chứng khoán. Nền công nghiệp chứng khoán của các nước phát triển trên thế giới đều không ngừng đổi mới công nghệ và luôn tích cực áp dụng những thành tựu mới nhất về công nghệ thông tin cho ngành chứng khoán của mình. Một trong những những ứng dụng công nghệ mới nhất mà họ áp dụng cho ngành công nghệp chứng khoán đó là ứng dụng công nghệ thông tin trong quản lý và điều hành hoạt động giao dịch chứng khoán. Việc áp dụng công nghệ thông tin đã đem lại những lợi ích vô cùng to lớn cho ngành chứng khoán.

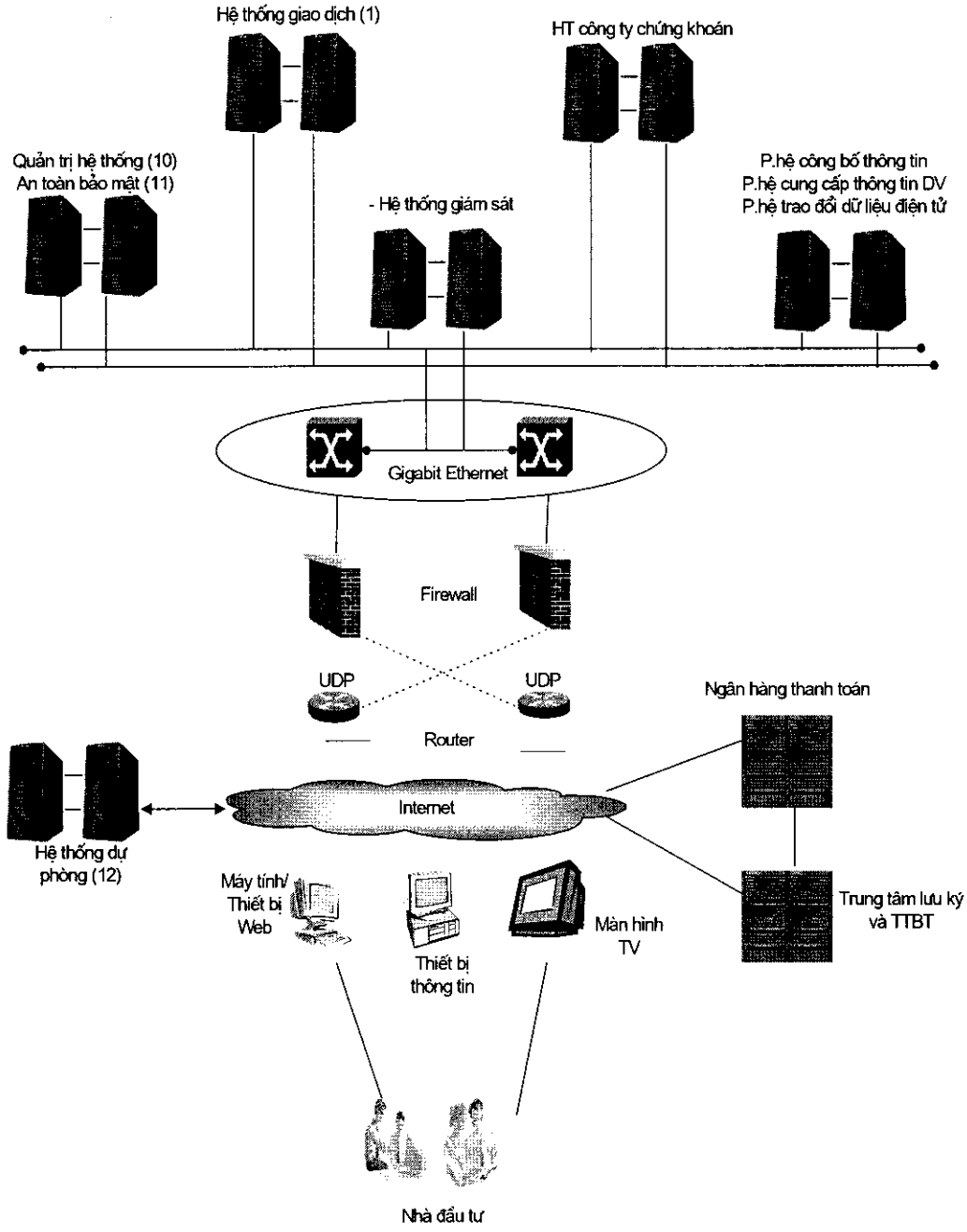
Như chúng tôi đã phân tích ở trên, các hệ thống giao dịch chứng khoán tại các TTGDCK ở Việt Nam hiện nay còn nhiều hạn chế và khả năng an toàn và bảo mật còn yếu. Trong phần giải pháp này, chúng tôi xin đưa ra một số giải pháp nhằm tăng cường tính an toàn và bảo mật cho hệ thống.

2.1. Các mục tiêu một hệ thống giao dịch chứng khoán cần đạt được

- Đảm bảo một hệ thống giao dịch quy mô phù hợp, có tính mở, khả năng tự động hoá cao (có thể đáp ứng được khả năng khớp lệnh liên tục hoặc định kỳ,kết nối mạng diện rộng với các công ty chứng khoán thành viên, đảm bảo có thể đặt lệnh từ xa qua Internet hay trang web ;
- Đảm bảo có một hệ thống giám sát tự động kết nối với các hệ thống giao dịch, công bố thông tin để hỗ trợ khả năng quản lý của trung tâm và nâng cao tính ổn định của thị trường;
- Đảm bảo khả năng liên lạc thông suốt và ổn định;
- Đảm bảo khả năng lưu trữ và bảo vệ dữ liệu an toàn, tạo dựng CSDL giao dịch đầy đủ, dễ dàng phục vụ công tác giám sát và khắc phục sự cố;
- Đảm bảo độ an toàn của toàn bộ hệ thống trước sự xâm nhập

bất hợp pháp từ bên ngoài, bên trong và cả với những biến cố thiên tai.

- Đảm bảo có một hệ thống thông tin có thể truyền phát rộng, truy cập dễ dàng cho tất cả các đối tượng tham gia thị trường. Mở rộng phạm vi thông tin công bố và thông tin chuyên biệt dựa trên hệ CSDL thông tin đầy đủ và hoàn chỉnh.



Hình vẽ: *Mô hình tổng quan hệ thống*

2.2. Giải pháp phần cứng

Hiện nay các thiết bị tin học (đặc biệt là hệ thống máy chủ, thiết bị mạng) tại các TTGDCK đều tương đối nhỏ, gồm nhiều loại cấu hình khác nhau, tốc độ xử lý thấp và không phải là các thiết bị máy chủ chuyên dụng trong lĩnh vực tài chính nên khả năng ổn định và an toàn không cao. Do đó để nâng cao tính ổn định và an toàn và bảo mật của hệ thống, các thiết bị tin học phần cứng (máy chủ, máy trạm, thiết bị mạng) tại TTGDCK phải được xây dựng dựa trên các yêu cầu và giải pháp sau:

2.2.1. Đối với hệ thống máy chủ:

Máy chủ phải là các thiết bị chuyên dụng trong lĩnh vực tài chính, có khả năng tự động phát hiện và khắc phục sự cố. Hiện nay, hầu hết các hệ thống máy tính của các thị trường chứng khoán trên thế giới đều sử dụng các máy chủ chạy trên hệ điều hành Unix/Linux. Đây là hệ điều hành được phát triển nhằm mục đích sử dụng cho các hệ thống chuyên dụng, có tính chất quan trọng và ảnh hưởng lớn đến hoạt động của ngành khi xảy ra sự cố (như tài chính ngân hàng, viễn thông..). Các máy chủ chạy trên hệ điều hành này có độ ổn định cao, khả năng bảo mật tốt hơn nhiều khi sử dụng các hệ điều hành khác (Window, Netware ....). Các máy chủ sử dụng hệ điều hành này khắc phục tối đa các lỗi gây nguy hiểm đến an toàn bảo mật của hệ thống. Chẳng hạn như với máy chủ chạy Window NT thường có các lỗi như: Internet Information Services (IIS); Microsoft SQL Server (MSSQL); Windows Authentication; Internet Explorer (IE); Windows Remote Access Services; Microsoft Data Access Components (MDAC); Windows Scripting Host (WSH); Microsoft Outlook Outlook Express; Windows Peer to Peer File Sharing (trong mạng ngang hàng P2P); Simple Network Management Protocol (SNMP).Trong số các khiếm khuyết nêu trên, phần mềm máy chủ Web Microsoft IIS được xem là một trong những nguyên nhân chủ yếu tạo ra nhiều lỗ hổng bảo mật hệ thống nhất, với 6 lỗ hổng từng được phát hiện trong năm ngoái 2002 và ít nhất 4 lỗ hổng khác từ đầu năm 2003 tới nay.

Ngoài ra, các máy chủ trên hệ thống phải có khả năng thay thế nóng (hot swap) các ổ cứng, khả năng phát hiện và cảnh báo sớm các sự cố có thể phát sinh. Các ổ cứng trên máy chủ được cài đặt theo nguyên lý dự phòng lẫn nhau. Nghĩa là khi một thiết bị ổ cứng bị lỗi, các ổ cứng còn lại sẽ tức thì đảm nhận công việc của ổ cứng đã bị hỏng. Với giải pháp này, dữ liệu sẽ được chứa trong tất cả các ổ cứng và các ổ cứng này sẽ phân chia theo các mức độ ưu tiên khác nhau theo quy định của quản trị mạng.

Với tầm quan trọng của hệ thống giao dịch chứng khoán, tính ổn định và khả năng hoạt động liên tục là yêu cầu không thể thiếu, sự ngừng hoạt động của máy chủ sẽ làm tê liệt các hoạt động giao dịch của toàn thị trường

và thiệt hại khó có thể lường trước được. Do vậy, vấn đề đặt ra là cần có một giải pháp để đảm bảo cho hệ thống vẫn hoạt động tốt ngay cả khi có sự cố xảy ra đối với máy chủ mạng, và công nghệ clustering là câu trả lời cho vấn đề này.

Trong phần này chúng tôi xin giới thiệu nguyên lý và phân tích một số giải pháp clustering đang được áp dụng cho các hệ thống mạng máy tính quan trọng hiện nay

Tổng quan về công nghệ Clustering

Clustering là một kiến trúc nhằm đảm bảo nâng cao khả năng sẵn sàng cho các hệ thống mạng máy tính. Clustering cho phép sử dụng nhiều máy chủ kết hợp với nhau tạo thành một cụm (cluster) có khả năng chịu đựng hay chấp nhận sai sót (fault-tolerant) nhằm nâng cao độ sẵn sàng của hệ thống mạng. Cluster là một hệ thống bao gồm nhiều máy chủ được kết nối với nhau theo dạng song song hay phân tán và được sử dụng như một tài nguyên thống nhất. Nếu một máy chủ ngừng hoạt động do bị sự cố hoặc để nâng cấp, bảo trì, thì toàn bộ công việc mà máy chủ này đảm nhận sẽ được tự động chuyển sang cho một máy chủ khác (trong cùng một cluster) mà không làm cho hoạt động của hệ thống bị ngắt hay gián đoạn. Quá trình này gọi là "fail-over"; và việc phục hồi tài nguyên của một máy chủ trong hệ thống (cluster) được gọi là "fail-back".

Việc thiết kế và lắp đặt các cluster cần thoả mãn các yêu cầu sau:

Yêu cầu về tính sẵn sàng cao (availability). Các tài nguyên mạng phải luôn sẵn sàng trong khả năng cao nhất để cung cấp và phục vụ các người dùng cuối và giảm thiểu sự ngưng hoạt động hệ thống ngoài ý muốn.

Yêu cầu về độ tin cậy cao (reliability). Độ tin cậy cao của cluster được hiểu là khả năng giảm thiểu tần số xảy ra các sự cố, và nâng cao khả năng chịu đựng sai sót của hệ thống.

Yêu cầu về khả năng mở rộng được (scalability). Hệ thống phải có khả năng dễ dàng cho việc nâng cấp, mở rộng trong tương lai. Việc nâng cấp mở rộng bao hàm cả việc thêm các thiết bị, máy tính vào hệ thống để nâng cao chất lượng dịch vụ, cũng như việc thêm số lượng người dùng, thêm ứng dụng, dịch vụ và thêm các tài nguyên mạng khác.

Ba yêu cầu trên được gọi tắt là RAS (Reliability-Availability-Scalability), những hệ thống đáp ứng được ba yêu cầu trên được gọi là hệ thống RAS (cần phân biệt với Remote Access Service là dịch vụ truy cập từ xa).

Cũng cần chú ý rằng hiệu quả hoạt động của hệ thống Clustering phụ thuộc vào sự tương thích giữa các ứng dụng và dịch vụ, giữa phần cứng và phần mềm. Ngoài ra, kỹ thuật clustering không thể chống lại các sự cố xảy ra do virus, sai sót của phần mềm hay các sai sót do người sử dụng. Để chống lại các sự cố này cần xây dựng một CSDL được bảo vệ chắc chắn cũng như có các kế hoạch khôi phục, backup dữ liệu.

Cấu trúc của Cluster

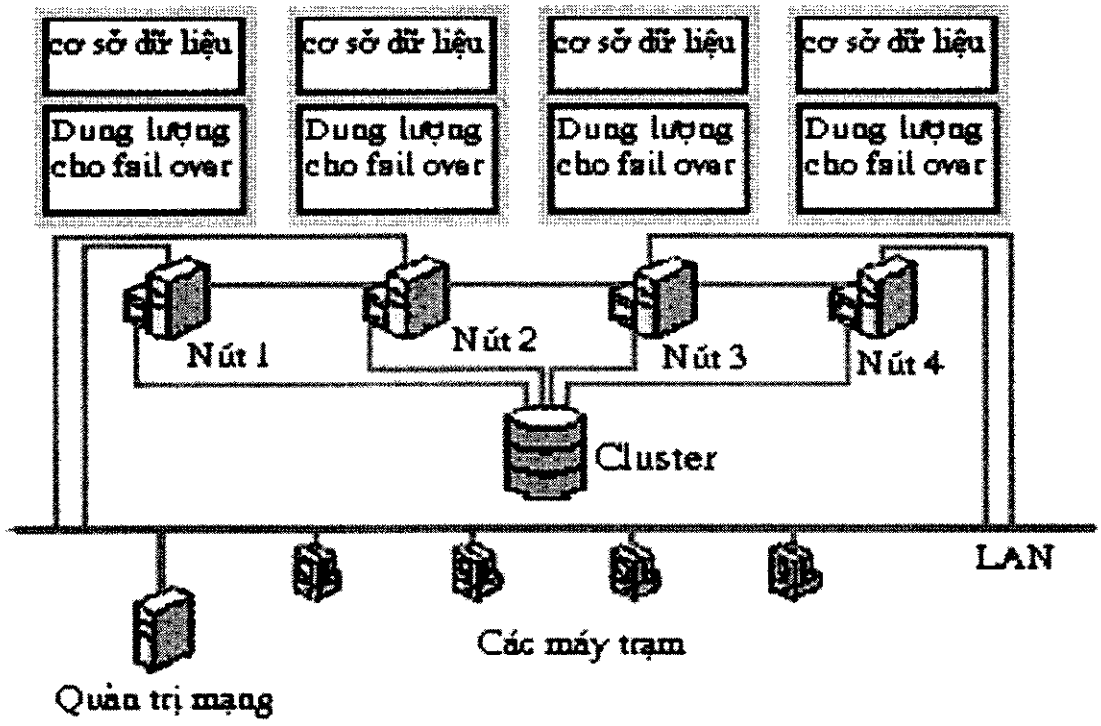
Cluster được tổ chức thành các nhóm gọi là các farm hay pack. Trong hầu hết các trường hợp, các dịch vụ ở tầng trước và giữa (front-end and middle-tiers services) được tổ chức thành các farm sử dụng các clone, trong khi đó các dịch vụ tầng sau (back-end services) được tổ chức thành các pack. Các khái niệm farm, pack và clone trong hệ thống cluster sẽ được làm rõ ngay dưới đây.

Cluster Farm là một nhóm các máy chủ chạy các dịch vụ giống nhau, nhưng không dùng chung CSDL. Được gọi là farm (trang trại) bởi vì chúng xử lý bất cứ yêu cầu nào gửi đến cho chúng bằng các bản sao CSDL (tài nguyên) giống hệt nhau được lưu giữ cục bộ, chứ không dùng chung một bản CSDL. Cũng bởi tính chất này nên các máy chủ thành viên của farm làm việc độc lập và chúng được gọi là clone (clone là máy tính được thiết kế để mô phỏng chức năng của máy tính khác).

Cluster Pack là một nhóm các máy chủ hoạt động cùng với nhau và chia sẻ với nhau các phần của CSDL. Được gọi là pack (khối) vì sự hoạt động của các máy chủ thành viên của pack có liên hệ chặt chẽ với nhau và chúng làm việc theo một phương thức thống nhất để quản lý và duy trì các dịch vụ.

Chế độ hoạt động của Cluster

Mỗi máy chủ trong cluster được gọi là một nút (cluster node), và có thể được thiết lập ở chế độ chủ động (active) hay thụ động (passive). Khi một nút ở chế độ chủ động, nó sẽ chủ động xử lý các yêu cầu. Khi một nút là thụ động, nó sẽ nằm ở chế độ dự phòng nóng (stanby) chờ để sẵn sàng thay thế cho một nút khác nếu bị hỏng. Nguyên lý hoạt động của Cluster có thể biểu diễn như trong hình 1.



Hình vẽ : Nguyên lý hoạt động của một Cluster

Trong một cluster có nhiều nút có thể kết hợp cả nút chủ động và nút thụ động. Trong những mô hình loại này việc quyết định một nút được cấu hình là chủ động hay thụ động rất quan trọng. Để hiểu lý do tại sao, hãy xem xét các tình huống sau:

- *Nếu một nút chủ động bị sự cố và có một nút thụ động đang sẵn sàng*, các ứng dụng và dịch vụ đang chạy trên nút hỏng có thể lập tức được chuyển sang nút thụ động. Vì máy chủ đóng vai trò nút thụ động hiện tại chưa chạy ứng dụng hay dịch vụ gì cả nên nó có thể gánh toàn bộ công việc của máy chủ hỏng mà không ảnh hưởng gì đến các ứng dụng và dịch vụ cung cấp cho người dùng cuối (Ngầm định rằng các các máy chủ trong cluster có cấu trúc phần cứng giống nhau).

- *Nếu tất cả các máy chủ trong cluster là chủ động và có một nút bị sự cố*, các ứng dụng và dịch vụ đang chạy trên máy chủ hỏng sẽ phải chuyển sang một máy chủ khác cũng đóng vai trò nút chủ động. Vì là nút chủ động nên bình thường máy chủ này cũng phải đảm nhận một số ứng dụng hay dịch vụ gì đó, khi có sự cố xảy ra thì nó sẽ phải gánh thêm công việc của máy chủ hỏng. Do vậy để đảm bảo hệ thống hoạt động bình thường kể cả khi có sự cố thì máy chủ trong cluster cần phải có cấu hình dư ra đủ để có thể gánh thêm khối lượng công việc của máy chủ khác khi cần.

Trong cấu trúc cluster mà mỗi nút chủ động được dự phòng bởi một nút thụ động, các máy chủ cần có cấu hình sao cho với khối lượng công việc trung bình chúng sử dụng hết khoảng 50% CPU và dung lượng bộ nhớ.

Trong cấu trúc cluster mà số nút chủ động nhiều hơn số nút bị động, các máy chủ cần có cấu hình tài nguyên CPU và bộ nhớ mạnh hơn nữa để có thể xử lý được khối lượng công việc cần thiết khi một nút nào đó bị hỏng.

Các nút trong một cluster thường là một bộ phận của cùng một vùng (domain) và có thể được cấu hình là máy điều khiển vùng (domain controllers) hay máy chủ thành viên. Lý tưởng nhất là mỗi cluster nhiều nút có ít nhất hai nút làm máy điều khiển vùng và đảm nhiệm việc failover đối với những dịch vụ vùng thiết yếu. Nếu không như vậy thì khả năng sẵn sàng của các tài nguyên trên cluster sẽ bị phụ thuộc vào khả năng sẵn sàng của các máy điều khiển trong domain.

Cluster nhiều địa điểm phân tán

Với các hệ thống mạng lớn có các người dùng phân bố rải rác, hiệu quả của việc phòng chống sự cố và nâng cao tính sẵn sàng của mạng sẽ được cải thiện hơn nhiều nếu xây dựng hệ thống cluster bố trí tại nhiều địa điểm. Kiến trúc nhiều địa điểm có thể được thiết kế theo rất nhiều cách khác nhau, trong đó phổ biến nhất là có một điểm gốc và một số điểm ở xa.

Với ***kiểu thiết kế đầy đủ***, toàn bộ cấu trúc của điểm gốc được xây dựng lại đầy đủ ở các điểm ở xa. Điều này cho phép các điểm ở xa hoạt động độc lập và có thể xử lý toàn bộ khối lượng công việc của điểm gốc nếu cần. Trong trường hợp này, việc thiết kế phải đảm bảo sao cho CSDL và các ứng dụng giữa điểm gốc và các điểm ở xa phải đồng bộ và được cập nhật sao lặp ở chế độ thời gian thực.

Với ***kiểu thiết kế thực hiện từng phần*** thì chỉ có các thành phần cơ bản là được cài đặt ở các điểm ở xa nhằm: Xử lý các khối lượng công việc quá tải trong các giờ cao điểm; Duy trì hoạt động ở mức cơ bản trong trường hợp điểm gốc site bị sự cố; Cung cấp một số dịch vụ hạn chế nếu cần.

Cả kiểu thiết kế đầy đủ hay từng phần đều dùng phương cách phân tán các máy chủ rải rác về mặt địa lý. Cluster phân tán về địa lý sử dụng mạng LAN ảo (Virtual LAN) để kết nối các mạng khu vực lưu trữ SAN (storage area network) qua những khoảng cách lớn. Để có thể duy trì hoạt động cluster một cách hiệu quả, yêu cầu đối với kết nối trong mạng LAN ảo phải có độ trễ khoảng dưới 500 ms.

Tối ưu hoá các thiết bị lưu trữ trên cluster

Các thiết bị lưu trữ trên cluster cần được tối ưu hoá trên cơ sở những nhu cầu về hiệu năng và mức độ sẵn sàng. Trong bảng 1 dưới đây cung cấp một cách khái quát những cấu hình hệ thống đĩa dự phòng RAID phổ biến có thể lựa chọn cho Cluster.

Tính mở của Cluster

Một vấn đề mà các nhà đầu tư xây dựng hệ thống cần quan tâm là khả năng mở rộng của hệ thống Clustering. Tuỳ theo yêu cầu cụ thể các cluster có thể cần phải thêm các máy chủ vào Cluster, hoặc thêm CPU và RAM cho các máy chủ để tăng khả năng đảm nhận công việc cho các máy chủ đã có.

Muốn mở rộng Cluster bằng cách thêm các server, thì cả hai yếu tố là Kỹ thuật clustering lẫn Hệ điều hành mà server sử dụng đều quan trọng. Ví dụ như trình bày trong bảng 2 sau đây, sự khác nhau cơ bản về khả năng mở rộng của Advanced Server và Datacenter Server là số nút có thể dùng với Cluster. Với Windows 2000, số nút máy chủ của Cluster tối đa là 4, trong khi đó với Windows .NET, số nút máy chủ của Cluster tối đa là 8.

Bảng 2. Số nút tối đa tương ứng với các hệ điều hành và kỹ thuật Clustering

Hệ điều hành		***Kỹ thuật Clustering***		
Tên gọi	Phiên bản	Cân bằng tải mạng	Cân bằng tải thành phần	Dịch vụ Cluster
Windows 2000	Advanced Server	32	8	2
	Datacenter Server	32	8	4
Windows NET	Advanced Server	32	8	4
	Datacenter Server	32	8	8

Muốn mở rộng Cluster bằng cách thêm vào các CPUs và RAM thì việc đang dùng hệ điều hành nào là vấn đề rất quan trọng. Ví dụ như Hệ điều hành Window 2000 Advanced Server hỗ trợ tối đa 8 bộ vi xử lý và 8 GB RAM, trong khi đó Window 2000 Datacenter Server hỗ trợ tối đa 32 bộ vi xử lý và 64 GB RAM. Như vậy, có thể phải nâng cấp hệ điều hành từ Advanced Server lên Datacenter Server nếu yêu cầu thêm CPU và RAM vượt quá khả năng của hệ điều hành đang dùng.

Linux Cluster

Mặc dù công nghệ clustering hiện nay vẫn phổ biến dùng hệ điều hành nguồn đóng, nhưng các thống kê về thị phần và mức tăng trưởng của thị trường máy chủ cho thấy rõ ràng là sự chuyển dịch sang các hệ điều hành nguồn mở như Linux đang ngày càng trở nên hiện thực (IBM đã đầu tư khoảng 1 tỷ USD để phát triển hệ thống IBM Linux cluster. Bởi vậy khi thảo luận về công nghệ clustering, việc tìm hiểu về Linux clustering là một vấn đề rất cần thiết).

Về nguyên lý hoạt động nói chung hệ thống Linux cluster cũng giống như các hệ thống cluster dùng phần mềm nguồn đóng, tuy nhiên hệ điều hành cơ sở cho Linux cluster là hệ điều hành Linux, được cài đặt trên từng nút của cluster. Chương trình quản lý được dùng trong các Linux cluster tuỳ theo yêu cầu của khách hàng có thể hỗ trợ các chức năng bao gồm việc cung cấp giao diện dòng lệnh hoặc cửa sổ; Các chức năng quản trị từ xa như thiết đặt lại hệ thống; giám sát các tham số quan trọng; kiểm soát nguồn; xem tệp nhật ký hệ thống; thao tác đơn tác động song song đến nhiều nút v.v.

Như đã nói ở trên, Linux cluster có độ tin cậy và tính ổn định khá cao, tuy nhiên việc thiết kế một Linux cluster hay một siêu cluster không phải là đơn giản, nó đòi hỏi phải xác định được các lớp rất trừu tượng và độ phức tạp tăng theo kích thước của cluster. Các đề án về giải pháp Linux cluster phải do những người có hiểu biết cần thiết về các vấn đề này xây dựng nên. Việc xác định các nút cần thiết phải theo các nguyên tắc sau:

· Cứ 32 đến 64 nút tính toán cần có một nút đầu mối.

· Mỗi hệ thống cần có một nút quản lý

· Việc vào/ra bên ngoài cần có một hay nhiều nút lưu trữ.

Có ba mạng chức năng cần phải có:

· Mạng dành cho việc liên lạc giữa các tiến trình IPC (inter process communication) với tốc độ phụ thuộc vào bài toán được đặt ra.

· Mạng dùng cho vào/ra tệp (file I/O). Mạng IPC cũng có thể kiêm luôn nhiệm vụ này

· Mạng phục vụ cho việc quản lý hệ thống, thường là mạng được thiết lập bởi các chuyển mạch 10/100 Ethernet. Cũng cần phải có cả máy chủ phục vụ đầu cuối trong mạng này.

Kết luận

Clustering là một kỹ thuật được áp dụng nhằm nâng cao độ tin cậy và tính sẵn sàng của hệ thống mạng máy tính. Một mạng được cấu trúc dưới dạng clustering sẽ có khả năng hoạt động bình thường ngay cả khi có sự cố xảy ra cho một máy chủ mạng trong cluster. Tuỳ theo yêu cầu cụ thể của hệ

thống mà có thể cấu trúc cluster 2 nút, 4 nút, 8 nút hoặc nhiều hơn. Các nút trong cluster có thể toàn ở thể chủ động, hoặc có nút chủ động, có nút thụ động. Mỗi cấu trúc của cluster sẽ đòi hỏi một cấu hình phần cứng của các máy chủ tương ứng. Hệ điều hành cũng là một yếu tố quan trọng cần xem xét khi thiết kế clustering cho mạng. Lựa chọn các phần mềm như Window 2000 đảm bảo hệ thống dễ thiết lập, tuy nhiên tính bảo mất thường không cao. Các hệ điều hành như Unix/Linux tuy khó thiết định nhưng lại có tính bảo mật và độ an toàn cao hơn. Bởi vậy, khi định thiết đặt một cấu trúc clustering cho hệ thống máy chủ giao dịch chứng khoán, chúng ta cần xem xét kỹ các yếu tố nêu trên để có thể quyết định lựa chọn giải pháp tối ưu cho mình.

2.2.2. Đối với hệ thống mạng

Các tiêu chí khi xây dựng hệ thống mạng:

Hệ thống mạng tại các TTGDCK khi xây dựng phải đáp ứng được các tiêu chí sau:

- Công nghệ hiện đại, phù hợp.
- Tốc độ cao, ổn định.
- Khả năng mở rộng: đáp ứng nhu cầu mở rộng và quy mô phát triển của TTGDCK.
- Độ tin cậy: Hệ thống mạng LAN TTGDCK phục vụ trực tiếp cho hoạt động và điều hành của TTGDCK . Do vậy ngoài yêu cầu khắt khe về chất lượng của các thiết bị kết nối mạng, phương pháp kết nối chúng trong hệ thống cũng phải được thiết kế khoa học, hợp lý, để hệ thống vẫn khả dụng trong các tình huống phức tạp.
- Khả năng quản trị: cho phép người quản trị theo dõi trạng thái hoạt động của các thành tố quan trọng trên mạng, đồng thời cho phép can thiệp, thiết lập cấu hình một cách mềm dẻo và dễ dàng.
- An ninh: hệ thống phải đáp ứng được các chức năng bảo mật cao, ngăn chặn các xâm nhập phá hoại cũng như cho phép cô lập thiết bị hay người sử dụng theo phạm vi chức năng.
- Hỗ trợ được đầy đủ các chức năng của hệ thống như: Chức năng quản trị mạng; Chức năng kết nối Internet; Chức năng kết nối từ xa; Chức năng khai thác thông tin WWW; Chức năng gửi thư tín điện tử; Chức năng in ấn; Chức năng sử dụng chung File; Chức năng khai thác hệ thống phần mềm...

- Hệ thống mạng phải xây dựng dựa trên một giao thức chuẩn và thống nhất. Hiện nay có rất nhiều giao thức trên mạng được áp dụng, nhưng theo đánh giá chung, giao thức TCP/IP có nhiều ưu điểm hơn cả

  - Đây là giao thức chuẩn dùng trên hầu hết tất cả các hệ thống lớn hiện nay, đặc biệt là mạng Internet.
  - Là giao thức truyền tin ổn định và độ an toàn rất cao.
  - Giảm chi phí đường truyền so với việc sử dụng nhiều giao thức cùng một lúc
  - Dễ dàng quản lý, đảm bảo tính thống nhất cao nhất so với tất cả các giao thức khác
  - Hỗ trợ tốt nhất cho việc quản trị hệ thống vì phần lớn các ứng dụng về quản trị hệ thống được xây dựng trên cơ sở hỗ trợ giao thức này
  - Hỗ trợ rất tốt các ứng dụng cấp cao như CSDL, e-mail và các ứng dụng đặc biệt khác.

Phân tích yêu cầu khi xây dựng hệ thống mạng:

Các Trung tâm Giao dịch chứng khoán là đơn vị có những số liệu đặc biệt quan trọng, ảnh hưởng rất lớn khi có sự cố phát sinh. Do vậy, khi xây dựng một hệ thống mạng phải xác định được các bước triển khai:

- Đánh giá nguy cơ và xác định các tài nguyên thông tin cần phải bảo vệ.
- Đề ra một chính sách an ninh mạng thích hợp (Security Policy).
- Từ hai bước trên, đề xuất những giải pháp an ninh mạng thích hợp.

Sau đây, chúng tôi sẽ phân tích sâu hơn về các bước triển khai trên.

a) Đánh giá nguy cơ và xác định các tài nguyên thông tin cần được bảo vệ:

Đối với bất kỳ một hệ thống nào, việc đầu tiên khi triển khai một hệ thống an ninh mạng sẽ là tiến hành đánh giá các nguy cơ tiềm tàng đối với hệ thống. Là một đơn vị đầu mối, Trung tâm Giao dịch chứng khoán là nơi lưu giữ và cung cấp cho các đơn vị khác rất nhiều thông tin quan trọng. Do vậy, nguy cơ trở thành mục tiêu tấn công của các tội phạm máy tính là rất lớn. **Các nguy cơ lớn nhất là:**

- ***Giả mạo người sử dụng:*** với việc cung cấp các kết nối cho người dùng truy cập từ xa (Các công ty chứng khoán và các đơn vị, cá nhân khác), hệ thống chỉ sử dụng giải pháp xác thực người dùng bằng mật khẩu. Đây là một giải pháp xác thực truyền thống và có rất nhiều yếu điểm. Yếu điểm lớn nhất của nó là một khi mật khẩu bị đánh cắp (được thực hiện rất dễ dàng bằng một số công cụ, kẻ xấu hoàn toàn có thể mạo danh người dùng hợp pháp để đánh cắp thông tin và có thể tiến hành trong thời gian dài mà không bị phát hiện. Đặc biệt, giả mạo người dùng có thể làm vô hiệu hoá tất cả các giải pháp an ninh thông tin khi người bị giả mạo giữ một vai trò quan trọng đối với hệ thống, đó chính là các quản trị mạng.

- ***Tấn công hệ thống từ bên trong:*** các nghiên cứu đã chỉ ra rằng có đến 70% các cuộc tấn công được bắt đầu từ bên trong hệ thống. Một máy tính khi đã bị lây nhiễm các loại worm, trjan,... cũng có thể là nguồn gốc của một cuộc tấn công. Một nhân viên xấu hoặc thậm chí chỉ là một hành động vô tình của người dùng cũng có thể để lại những hậu quả nghiêm trọng cho hệ thống. Một người truy cập từ xa, sau khi đã được xác thực qua FW cũng không có sự kiểm soát cần thiết đối với những hoạt động của họ ở bên trong mạng. Không có giải pháp cho vấn đề này sẽ tạo ra rất nhiều điểm yếu trong toàn bộ hệ thống an ninh mạng.

- ***Lây nhiễm virus, worm, trojan,...:*** trên mạng internet xuất hiện ngày càng nhiều những loại worm lây lan với một tốc độ nhanh khủng khiếp. Lấy ví dụ, worm máy tính mới xuất hiên Sasser đã lây nhiễm đến 18 triệu máy tính chỉ trong chưa đầy một tuần. Do vậy, khi bị lây nhiễm, việc phát tán các loại worm như vậy trong hệ thống sẽ chỉ mất chưa đầy một giờ đồng hồ. Mặt khác, những phần mềm spyware có thể ghi nhận hoặc gửi các thông tin trong hệ thống tới chủ nhân của nó. Nguồn lây nhiễm là từ các máy tính xách tay, những chương trình tải từ internet, những người dùng truy cập từ xa cài đặt vào hệ thống,..

Cùng với việc đánh giá các nguy cơ của hệ thống, Trung tâm Giao dịch chứng khoán cũng sẽ phải ***xác định được những tài nguyên thông tin nào cần được bảo vệ một cách thích hợp.*** Thông thường đối với một tổ chức, các thông tin trên các máy chủ, các CSDL, các ứng dụng nghiệp vụ, các thông tin trên các máy tính cá nhân,... là những thông tin mà thường trở thành mục tiêu tấn công của tội phạm máy tính. Dựa trên những yêu cầu bảo mật thông tin, tổ chức sẽ xây dựng được một chính sách an ninh (Security policy) và áp dụng các biện pháp an ninh hệ thống một cách thích hợp.

b) Xây dựng chính sách an ninh mạng

Các giải pháp an ninh mạng chỉ có thể phát huy hiệu quả cao nhất khi có một chính sách an ninh mạng hợp lý. Đó là những quy định cụ thể về các

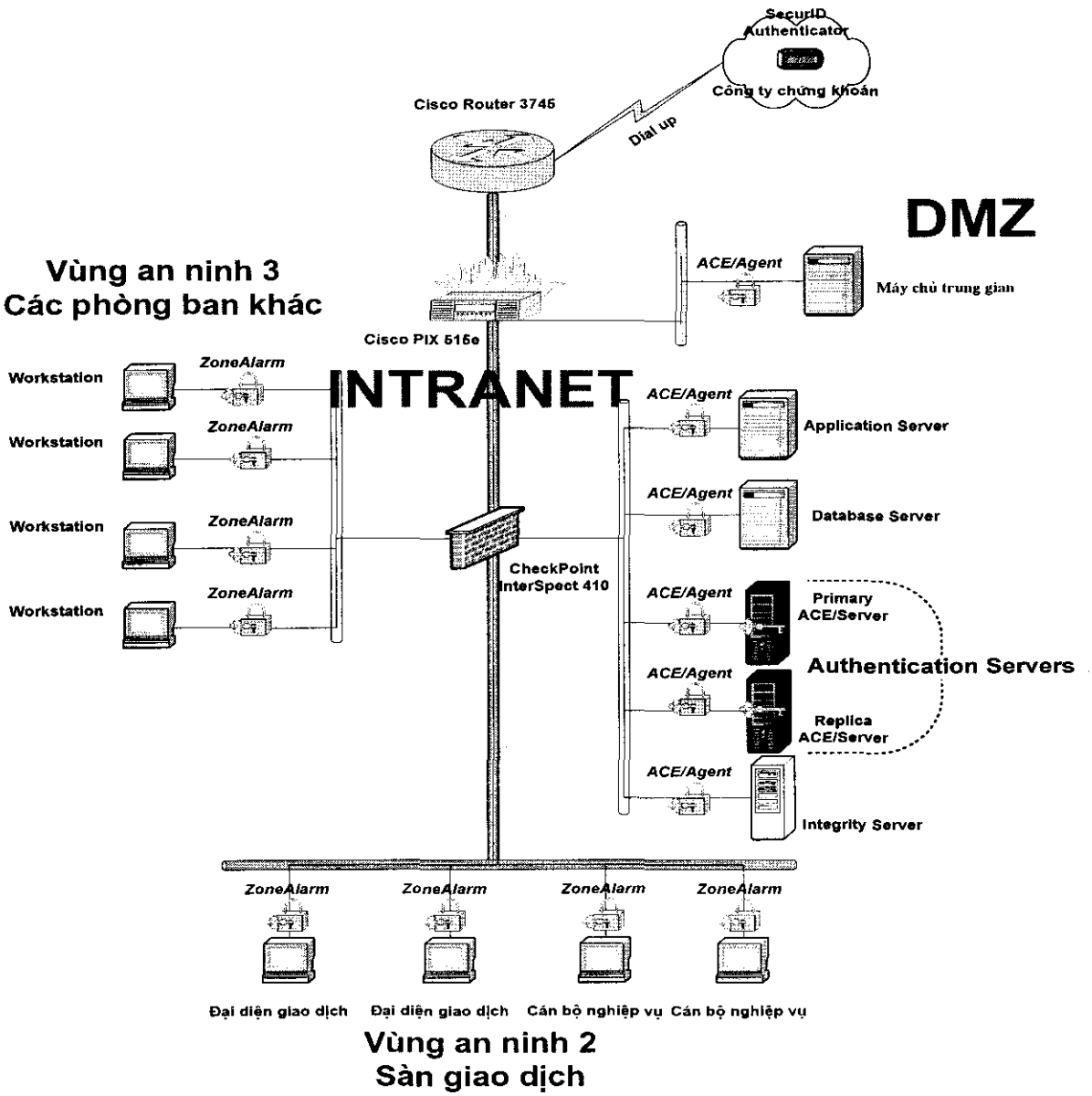
biện pháp an ninh. Ví dụ như những quy định về quyền truy cập vào những thông tin của tổ chức. Một chính sách an ninh mạng cần quy định cụ thể về những ai sẽ được quyền truy cập vào những thông tin nào, quyền truy cập đó ra sao (được phép thay đổi nội dung hay chỉ đọc,..), quy định về hệ thống nhật ký (Log file) và báo cáo về hoạt động của những người sử dụng trên mạng, quy định về các hành động cần thiết khi xảy ra hiện tượng bùng nổ virus... Nói tóm lại, chính sách an ninh mạng là cơ sở trên đó các giải pháp an ninh mạng tuân thủ theo.

Qua phân tích các nguy cơ lớn nhất đe doạ đến vấn đề an ninh thông tin của hệ thống, qua các yêu cầu đối với bảo mật thông tin của Trung tâm Giao dịch chứng khoán, chúng tôi đề xuất một số giải pháp nhằm hạn chế ngay một số các mối đe doạ có nguy cơ cao ảnh hưởng đến hệ thống như sau:

- *Xác thực người sử dụng (User Authentication)*
- *Hệ thống an ninh nội bộ (Internal Security)*
- *Bảo vệ server và các máy tính trên mạng (End-Point Security)*

2.2.3. Đề xuất lựa chọn các giải pháp cho hệ thống an ninh mạng:

Sơ đồ mạng Trung tâm Giao dịch chứng khoán sau khi nâng cấp:



➢ **Giải pháp xác thực người sử dụng RSA SecurID:**

Theo phân tích đã đề cập ở trên, hệ thống mạng của Trung tâm Giao dịch chứng khoán là nơi lưu trữ rất nhiều những thông tin vô cùng quan trọng. Hiện nay, mô hình chủ yếu sử dụng để kết nối thông tin là các công ty chứng khoán đang sử dụng những đường quay số (Dial up) tới server đặt tại Trung tâm Giao dịch chứng khoán để thu nhận thông tin và được xác thực thông qua mật khẩu. Tuy nhiên, xác thực bằng mật khẩu là không an toàn do vậy chúng tôi đề xuất sử dụng giải pháp xác thực người sử dụng dựa trên hai yếu tố SecurID.

Mỗi người sử dụng sẽ biết một số PIN (Personal Identify Number) và sở hữu một token tạo ra các con số ngẫu nhiên (không thể dự đoán được) sau

một khoảng thời gian nhất định (Thông thường là 60 s) được gọi là tokencode. Kết hợp hai yếu tố là số PIN (Số mà bạn biết) với tokencode (Số mà bạn có) sẽ tạo ra Passcode. Khi đăng nhập vào hệ thống, người sử dụng thay vì nhập một password tĩnh sẽ được yêu cầu nhập passcode (Luôn thay đổi theo thời gian). Các RSA Agent được cài đặt tại các máy chủ (Server), các điểm truy cập vào mạng (Entry Point – Gateway, RAS server,...), các tài nguyên thông tin cần được bảo vệ (Database,...) sẽ tiếp nhận thông tin UserName và Passcode của người sử dụng và gửi đến server xác thực RSA ACE/Server . Server xác thực (Authentication Server-RSA ACE/Server) căn cứ vào một số yếu tố cũng sẽ tính được con số tokencode, kết hợp với số PIN trong CSDL, server xác thực cũng sẽ có được một passcode. So sánh với passcode do người sử dụng cung cấp, server xác thực sẽ quyết định cho phép đăng nhập (Login) hay không. Các RSA ACE/Server có thể được cài đặt trên nhiều server với một máy chủ chính (Primary ACE/Server) và nhiều máy chủ bản sao (Replica ACE/Server). Các máy chủ bản sao cũng có thể hoạt động như máy chủ chính do vậy, ta có thể đặt được tại nhiều vị trí để cung cấp các dịch vụ xác thực cho người dùng tại chỗ thay vì phải kết nối đến máy chủ chính qua các đường truyền chi phí cao. Tuy vậy, chỉ có máy chủ chính mới có thể thay đổi các thông tin về cấu hình và sẽ tiến hành đồng bộ với các máy chủ bản sao. Khi máy chủ chính bị lỗi, quản trị mạng có thể lựa chon một máy chủ bản sao để nâng cấp lên thay thế máy chủ chính trong một thời gian vài phút. Điều này cho phép hệ thống xác thực hoạt động được tốt trong mọi hoàn cảnh.

Với các passcode (PIN + Tokencode) để đăng nhập hệ thống luôn thay đổi theo thời gian, các hacker sẽ không có khả năng dò đoán được hoặc ngay cả khi chặn bắt được một passcode thì cũng không thể sử dụng được vì mỗi passcode chỉ được sử dụng một lần (Thông thường sau một phút đổi một lần). Người sử dụng cũng không phải quản lý các password như trước kia nữa qua đó giảm thiểu các yêu cầu về hỗ trợ kỹ thuật. Giải pháp SecurID của RSA cũng có thể hoạt động tốt với hệ thống xác thực RADIUS và TACACS+ server.

Các phần mềm RSA ACE/Agent sẽ được cài đặt tại các điểm truy cập vào mạng (Cisco PIX 515e), tại server cung cấp thông tin cho các công ty chứng khoán và tại các server trong nội bộ của hệ thống mạng. Các Agent này đảm bảo khi người dùng truy cập tới các thông tin trong hệ thống đều phải được xác thực thông qua RSA SecurID. Do vậy, nó đảm bảo độ an toàn cao nhất cho hệ thống.

Giải pháp xác thực người dùng RSA SecurID khắc phục được tất cả các nhược điểm lớn nhất của xác thực bằng mật khẩu. Người dùng không phải quản lý nhiều mật khẩu, một hacker có chặn bắt được mã passcode trên

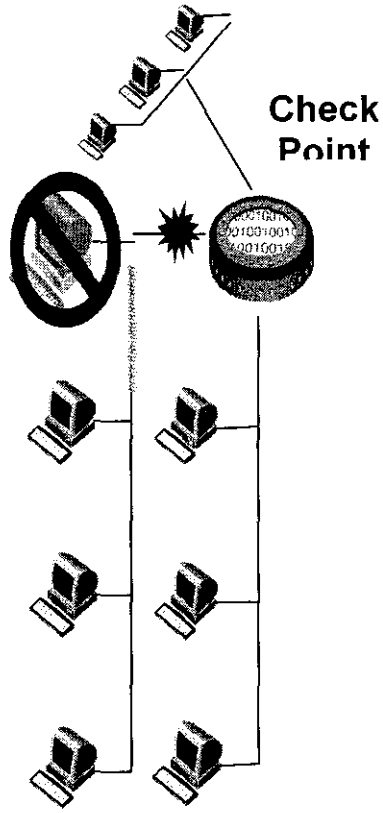
mạng cũng không thể sử dụng được bởi vì mỗi passcode chỉ có thể sử dụng được một lần. Giải pháp này cũng ghi nhận đầy đủ những lần người dùng đăng nhập vào hệ thống và có thể được sử dụng như là một bằng chứng pháp lý. RSA SecurID cung cấp cho hệ thống khả năng chống giả mạo người dùng một cách tuyệt đối.

➢ **CheckPoint InterSpect (Internal Security):**

InterSpect là một gateway cung cấp khả năng đảm bảo an ninh bên trong mạng. Nó có thể hạn chế sự lây lan các loại worm hoặc xâm nhập trái phép trong mạng và phân chia hệ thống mạng nội bộ thành nhiều vùng mạng. Dựa trên các công nghệ hàng đầu của Checkpoint như INSPECT, Stateful Inspection, Application.

Intelligence và SMART (Security Management Architecture), InterSpect được thiết kế đặc biệt nhằm cung cấp khả năng đảm bảo an ninh bên trong hệ thống. Nó có những tính năng chính sau:

- ***Phòng chống lây nhiễm worm (Intelligent worm defender):*** cung cấp khả năng phòng chống worm bằng cách áp dụng các công nghệ Stateful Inspection và Application Intelligence của Checkpoint. InterSpect được cài đặt trong hệ thống, phân tách hệ thống thành các vùng an ninh (Security zone), ngăn chặn sự lây lan của các loại worm bằng việc kiểm tra các lưu lượng thông tin trên mạng và khoá các gói tin có tính chất nguy hiểm lại.



- ***Phân vùng mạng (Network zone segmentation):*** InterSpect phân hệ thống thành các vùng an ninh khác nhau và ngăn chặn các xâm nhập trái phép từ vùng này sang vùng khác. Điều này ngăn chặn những người sử dụng hoặc các máy tính đã bị xâm nhập không truy cập được vào những thông tin không được phép. Khả năng phân vùng mạng ngăn chặn các cuộc tấn công chỉ hạn chế trong một vùng mạng.

- ***Cách ly (Quarantine):*** InterSpect có thể nhận biết các hành vi truy cập trái phép, nhận diện các máy tính đã bị lây nhiễm hoặc nghi ngờ bị lây nhiễm và tiến hành cách ly chúng ngăn không cho phần còn lại của hệ thống bị

ảnh hưởng. Khi này, người sử dụng sẽ được thông báo bằng một trang web (Có thể thay đổi - Customize) nhằm làm giảm thời gian khắc phục.

- ***Bảo vệ các giao thức mạng LAN (LAN Protocol Protection)***: InterSpect cung khả năng bảo vệ cao nhất và toàn diện nhất cho các giao thức của Microsoft như MS RPC, CIFS, MS SQL và DCOM cũng như các giao thức mạng LAN khác như Sun RPC, DCE RPC và HTTP.

- ***Phòng chống tấn công một cách chủ động (Pre-Emptive Attack Protection):*** InterSpect cung cấp khả năng phòng chống một cách chủ động và linh hoạt các cuộc tấn công đã biết và chưa biết, cho phép hệ thống bảo vệ các điểm yếu trước khi chúng bị khai thác.

➢ **ZoneLabs Integrity 5.0 (End Point Security):**

ZoneLabs Integrity 5.0 của ZoneLabs là một giải pháp bảo vệ đầu cuối toàn diện. Nó có những tính năng chính như sau:

- Đảm bảo chính sách an ninh trên toàn hệ thống. Bất cứ một người sử dụng khi đăng nhập vào mạng đều được kiểm tra để đảm bảo máy tính người sử dụng đã được cài đầy đủ các phần mềm bảo mật theo quy định (Đã được cài các bản vá lỗi, cài các phần mềm bảo mật,..).

- Đối với những người sử dụng không ở trong hệ thống (các khách hàng), khi đăng nhập vào hệ thống (qua các kết nối truy cập từ xa) sẽ được yêu cầu kiểm tra máy tính để đảm bảo không có những phần mềm spyware, worm, trojan,.. tránh nguy cơ những máy tính này trở thành nguồn lây nhiễm vào hệ thống.

- Bảo vệ các máy tính cá nhân mọi lúc, mọi nơi: với những máy tính cố định trong hệ thống, chế độ client đảm bảo tuân thủ theo những chính sách an ninh của hệ thống. Chế độ desktop bảo vệ cho những máy tính cá nhân không ở trong mạng. Đặc biệt, ZoneLabs Integrity 5.0 có chế độ Flexible kết hợp cả hai chế độ trên. Khi ở trong hệ thống mạng, Flexible hoạt động ở chế độ client mà tuân thủ theo những chính sách an ninh của hệ thống. Khi hoạt động tại môi trường bên ngoài, chế độ desktop được kích hoạt và cung cấp khả năng bảo vệ cho máy tính. Như vậy, với ZoneLabs Integrity 5.0, các hệ thống đầu cuối luôn được bảo vệ tại mọi thời điểm và trong mọi môi trường làm việc.

- Bảo vệ các máy tính tránh các tấn công dò tìm: với tính năng "Stealth", ZoneLabs Integrity cung cấp khả năng chống các hoạt động dò tìm điểm yếu trên máy tính, giảm thiểu nguy cơ bị tấn công qua việc khai thác các điểm yếu trên máy tính.

Ngoài ra xây dựng một hệ thống mạng chứng khoán chung là công việc quan trọng của công tác phát triển hạ tầng khi triển khai giao dịch trực tuyến. Khi sử dụng mạng này các công ty chứng khoán (trụ sở chính và các văn phòng chi nhánh) trên cả nước có thể nhập các lệnh mua bán chứng khoán cùng một lúc, và các nhà đầu tư có thể tiếp cận thông tin thị trường trên cơ sở thời gian thực thông qua các máy điện toán cung cấp dịch vụ thông tin trên mạng.

Chúng ta nên xây dựng đường thông tin hai chiều để tăng cường độ tin cậy và phát triển hệ thống mạng giám sát duy nhất cho việc theo dõi và quản lý tự động của hệ thống mạng. Cần xây dựng giải pháp hệ thống trao đổi thông tin trên cơ sở các máy chủ có đường truyền tải tốc độ cao và máy xử lý node cho phép tất cả những người sử dụng có thể vào mạng cùng lúc. Một hệ thống quản lý mạng cũng càn thiết được phát triển theo hướng cho phép phát hiện ra lỗi cuả hệ thống và kiểm soát toàn bộ hệ thống mạng. Hệ thống mạng chung này sẽ là nền tảng cho việc trao đổi thông tin với các hệ thống mạng khác, ví dụ mạng thanh toán liên ngân hàng...

Hệ thống mạng nội bộ trong từng công ty chứng khoán và các TTGDCK phải được thiết lập và có độ bảo mật và an toàn cao. Mỗi một công ty chứng khoán phải có một đường truyền trực tiếp tới Sở giao dịch chứng khoán. Đường truyền này phải có tốc độ cao, có độ an toàn và bảo mật tốt nhằm giảm thiểu được tối đa các sự cố trên đường truyền. Hiện nay, Việt nam chúng ta đã tiếp cận được hầu hết những công nghệ tiên tiến trong kỹ thuật truyền dẫn như là đường truyền mạch gói dựa trên giao thức X25, các đường truyền dựa trên kỹ thuật Frame Relay và ATM, mạng tích hợp dịch vụ số ISDN (Integrated Services Digital Network).

Hiện nay đa số các thiết bị mạng chuẩn (Switch, FireWall) đều đã tích hợp thêm công nghệ VLAN (mạng ảo). Với công nghệ này, người sử dụng có thể thiết lập thêm những lớp mạng khác nhau trên cùng một thiết bị để tăng cường khả năng chống truy xuất trái phép vào hệ thống. Sử dụng công nghệ VLAN sẽ cho phép phân chia mạng thành các mạng nhỏ một cách logic gọi là Virtual Lan hay gọi là Mạng ảo VLAN. VLAN là kỹ thuật cho phép chia một mạng lớn thành nhiều mạng nhỏ một cách logic. Khi thông tin cần trao đổi giữa các điểm trong một VLAN thì thông tin đó chỉ được gửi đến những điểm trong VLAN đó, do đó hạn chế rất nhiều các thông tin thừa trên đường truyền. Thường mạng được phân nhóm thành các VLAN theo đặc điểm công việc, theo bộ phận và theo nhu cầu trao đổi thông tin giữa các bộ phận, người dùng trên mạng.

Trên cơ sở phân chia hệ thống mạng, người sử dụng có thể thiết lập các mức độ bảo mật dữ liệu khác nhau và tăng tính năng của mạng cục bộ

bằng cách thiết lập tới 250 mạng riêng ảo VLAN ở mỗi switch. Điều này sẽ cho phép các gói dữ liệu sẽ được truyền đi trong phạm vi của một VLAN cụ thể, tạo ra một firewall ảo giữa các cổng dùng trong mạng. Công nghệ Uplink Fast của Cisco đảm bảo sự chuyển giao tức thời tới đường uplink thứ 2, làm tăng mức độ tin cậy và chắc chắn của mạng nói chung.

Tùy theo từng hệ thống tại các TTGDCK, có thể phân chia thành nhiều mạng VLAN khác nhau với mục đích hạn chế khả năng thâm nhập của tin tặc với mục đích xấu. Việc phân chia thành nhiều khu vực khác nhau sẽ giúp cho công tác bảo mật tại các đơn vị của TTGDCK được đảm bảo, mỗi người sử dụng chỉ có thể sử dụng trong phạm vi cho phép của mình mà không thâm nhập được vào các khu vực khác. Ngoài ra, nếu phân chia thành các mạng khác nhau sẽ giảm thiểu khả năng mất dữ liệu, giúp cho công tác bảo mật tốt hơn khi tin tặc xâm nhập được vào một khu vực do các yếu tố khách quan sẽ không xâm nhập được vào các khu vực khác của hệ thống.

Căn cứ theo hiện trạng của hệ thống GDCK tại TTGDCK ta có thể phân chia thành các VLAN thành phần như sau:

- VLAN MAYCHU bao gồm: các máy chủ trong hệ thống

- VLAN SANGIAODICH bao gồm: các máy trạm nhập lệnh của các thành viên, giám sát thị trường, quản lý giao dịch tại sàn.

- VLAN NGHIEPVU bao gồm: các máy trạm của các bộ phận tin học, quản lý niêm yết, quản lý thành viên, thông tin thị trường .

- VLAN THANHVIEN bao gồm: các công ty chứng khoán thành viên kết nối từ xa, các máy trạm thông tin.

2.3. Giải pháp phần mềm hệ thống

2.3.1. Hệ điều hành

Như đã trình bày ở phần trên, phần mềm hệ điều hành có ảnh hưởng lớn đến tính an toàn và ổn định của hệ thống. Theo quan điểm của chúng tôi, nên lựa chọn phần mềm điều hành là hệ điều hành LINUX hay SCO-UNIX và sẽ được cài đặt và sử dụng thống nhất trên toàn mạng do tính chất chuyên dụng và năng lực điều hành các mạng máy tính quy mô vừa và lớn của nó. Mặt khác, đây là hệ điều hành được sử dụng hầu hết trong các hệ thống tài chính ngân hàng trên thế giới và có tính ổn định cao, khả năng bảo mật tốt.

2.3.2. Hệ quản trị cơ sở dữ liệu

Hiện nay trên thế giới có rất nhiều chương trình quản trị CSDL khác nhau. Theo quan điểm của chúng tôi, hệ thống phần mềm Giao dịch Chứng khoán tại các TTGDCK nên sử dụng hệ quản trị CSDL ORACLE cùng các

sản phẩm đi kèm của nó như ORACLE Parallel Server làm nền tảng, vì đây là hệ quản trị CSDL có rất nhiều những tính năng mạnh, và khả năng bảo mật rất tốt như :

- Quản trị CSDL lớn: Hệ quản trị CSDL ORACLE có khả năng quản trị các CSDL từ cỡ MB đến hàng ngàn GB. Thực tế hoạt động trên thế giới đã chứng minh khả năng quan trọng của ORACLE. Các CSDL lớn ở Việt Nam đều dùng ORACLE.

- Xử lý giao dịch trực tuyến (OLTP). Đây là khả năng mạnh nhằm đáp ứng sự bùng nổ về số lượng giao dịch trực tuyến.

- Quản lý tài nguyên hiệu quả: ORACLE quản lý các tài nguyên của hệ thống như CSDL, các kết nối CSDL, bộ nhớ, v.v... một cách hiệu quả nhằm đáp ứng các CSDL lớn và số lượng giao dịch lớn

- Bảo mật: Cung cấp các khả năng bảo mật như

- Tích hợp dịch vụ thư mục vào CSDL nhằm quản lý tập trung và bảo mật các tài nguyên cũng như các đối tượng của hệ thống
- Quản lý người sử dụng với các quyền hạn chặt chẽ

- Quản lý các kết nối mạng

- Hỗ trợ các chuẩn kết nối trên Internet như: TCP/IP, HTTP, IIOP, v.v...
- Cân bằng tải tự động đối với các kết nối mạng

- Khả năng quản lý CSDL: Cung cấp các khả năng sau nhằm quản trị CSDL lớn như:

- Quản trị CSDL từ công cụ duy nhất ORACLE Enterprise Manager
- Partioning
- Tablespace có khả năng chuyển tải
- Tablespace được quản trị tại cục bộ
- Sao lưu và phục vụ dữ liệu trực tuyến

- Cung cấp công cụ ORACLE Enterprise Manager quản lý tập trung CSDL và các đối tượng khác.

2.4. Bảo mật và lưu trữ dữ liệu

2.4.1. Giải pháp bảo mật dữ liệu

➢ ***Phân loại dữ liệu***

Căn cứ theo tính chất dữ liệu

Dữ liệu tại TTGDCK được phân chia theo yêu cầu và tính chất của từng loại dữ liệu phù hợp yêu cầu sử dụng và khai thác thông tin của các nhà đầu tư, các nhà môi giới và cán bộ của TTGDCK. Các dữ liệu được phân chia theo các mảng chính như sau:

- Các thông tin của các công ty niêm yết tại TTGDCK bao gồm: bản cáo bạch, báo cáo tài chính, tình hình hoạt động sản xuất kinh doanh... Các thông tin này được công bố rộng rãi tới mọi đối tượng tham gia trên thị trường chứng khoán.

- Các thông tin của phiên giao dịch tại TTGDCK bao gồm: thông tin về các lệnh mua, bán của nhà đầu tư (số lượng, giá mua và bán...). Các thông tin này được công bố rộng rãi tới các nhà đầu tư giúp cho họ có các quyết định khi tham gia trên thị trường chứng khoán.

- Các thông tin về kết quả của phiên giao dịch bao gồm: các loại chứng khoán được giao dịch (giá, số lượng, người mua...). Các thông tin này sẽ được gửi tới các nhà môi giới tại các công ty chứng khoán.

- Các thông tin về chứng khoán được lưu ký TTGDCK bao gồm: loại chứng khoán, nhà đầu tư, mệnh giá... Các thông tin này sẽ do các cán bộ của TTGDCK sử dụng trong các nghiệp vụ về lưu ký và giao dịch

Căn cứ theo yêu cầu và tính chất của dữ liệu ta có thể phân chia mức độ bảo mật cho từng loại dữ liệu. Từ đó đưa ra các yêu cầu về bảo mật an toàn dữ liệu tại TTGDCK, giúp cho công tác quản lý các thông tin được đảm bảo nhằm bảo vệ cho các nhà đầu tư.

Căn cứ theo yêu cầu người sử dụng.

Các đối tượng sử dụng trực tiếp và gián tiếp hệ thống giao dịch chứng khoán bao gồm các nhà đầu tư tham gia trên thị trường, các nhà quản lý thị trường, các nhà môi giới, Tuỳ thuộc vào vị trí, vai trò, chức năng, nhiệm vụ mà các đối tượng tham gia sử dụng hệ thống ở các mức độ khác nhau, như:

- Khai thác thông tin.
- Trực tiếp tham gia xử lý các giao dịch.
- Giám sát kiểm tra hệ thống.
- Quản trị nghiệp vụ.
- Hỗ trợ kỹ thuật cho hệ thống.

Căn cứ theo vai trò, chức năng và nhiệm vụ của từng đối tượng sử dụng phần mềm, ta có đặc điểm của từng đối tượng người sử dụng, như sau:

- Các nhà đầu tư tham gia trên thị trường chứng khoán chủ yếu là khai thác các thông tin giao dịch của các loại cổ phiếu, trái phiếu, thông tin về các công ty niêm yết trên thị trường chứng khoán thông qua các công ty chứng khoán hoặc thông tin trên mạng INTERNET.

- Các nhà môi giới bao gồm các cán bộ, nhân viên làm việc tại các công ty chứng khoán, yêu cầu của người sử dụng này là các thông tin về giao dịch của các loại chứng khoán, thông tin về các nhà đầu tư (tài khoản chứng khoán và tài khoản tiền gửi), thông tin về tình hình lưu ký chứng khoán. Đối tượng sử dụng này được trực tiếp tham gia vào quá trình xử lý các giao dịch.

- Các cán bộ của TTGDCK thực hiện chức năng giám sát quá trình thực hiện trên hệ thống giao dịch bao gồm kiểm soát thông tin, các nghiệp vụ về chứng khoán.

- Các cán bộ tin học tại TTGDCK với chức năng nhiệm vụ vận hành và quản lý toàn bộ hệ thống giao dịch, đảm bảo an toàn và bảo mật dữ liệu cho hệ thống. Ngoài các nhiệm vụ trên các cán bộ còn phải đảm bảo hỗ trợ kỹ thuật khi có các sự cố trên hệ thống giao dịch.

Căn cứ theo chức năng và nhiệm vụ của các đối tượng sử dụng, ta có thể phân chia quyền truy cập và sử dụng hệ thống cho từng đối tượng theo các lớp bảo vệ dữ liệu của hệ thống giao dịch.

➢ **Một số giải pháp an toàn bảo mật dữ liệu:**

Để tăng cường tính an toàn và bảo mật dữ liệu cho hệ thống, cần đảm bảo các yêu cầu sau đây:

- Có những mức truy cập khác nhau cho người dùng vào từng CSDL khác nhau;

- Hệ thống hỗ trợ việc thiết lập phân quyền truy nhập người dùng khác nhau dựa vào sự cho phép và phân loại người dùng đối với từng loại CSDL;

- Hệ thống yêu cầu người sử dụng thay đổi mật khẩu theo định kỳ tối thiểu để nâng cao tính an toàn;

- Hệ thống cần ghi lại dấu vết về sự xâm phạm hệ thống CSDL vô tình hay cố ý;

- Hệ thống thiết lập các bảo mật với các hệ thống ngoài, truy cập từ xa, cung cấp các khả năng mã hoá dữ liệu;

- Hệ thống có khả năng giám sát, theo dõi và phát hiện các hành động cố tình vi phạm bên trong hệ thống;

- Phân quyền truy nhập hệ thống dữ liệu phù hợp đối với các đơn vị liên quan nối vào mạng của TTGDCK.

Hiện nay trên thế giới có rất nhiều giải pháp đảm bảo sự an toàn dữ liệu khi truyền trên mạng. Đối với mỗi giải pháp đều có nhiều phương pháp và cách thực hiện khác nhau. Song, đều sử dụng cách kết hợp giải pháp bảo vệ nhiều lớp đối với dữ liệu vì như thế thì sự an toàn của thông tin được nâng cao.

Dưới đây trình bày cụ thể một số giải pháp an toàn thông tin nhằm đảm bảo sự an toàn - bảo mật dữ liệu trên hệ thống mạng của TTGDCK khi được truyền và lưu trữ trên mạng. Phương pháp sẽ được sử dụng ở đây là phương pháp kết hợp nhiều giải pháp bảo vệ thông tin khác nhau. Điều này sẽ làm tăng thêm tính an toàn của hệ thống.

- ***Bảo vệ bằng FireWall:***

Đây là phương pháp đang được sử dụng hết sức rộng rãi trên Internet. FireWall có thể là một thiết bị phần cứng (máy tính, máy chủ...), hoặc phần mềm (chương trình) có khả năng chống lại sự truy cập bất hợp pháp từ bên ngoài vào thông tin nội bộ trong mạng của mỗi công ty, đoàn thể, tổ chức ...

- ***Bảo vệ bằng một số phương pháp mã hóa dữ liệu:***

Là phương pháp biến đổi thông tin từ dạng này sang dạng khác bằng cách sử dụng các thuật toán mã hóa. Đây là một phương pháp đã được đánh giá lá khá an toàn song lại rất phức tạp. Hiện nay, trên thế giới có rất nhiều thuật toán mã hóa khác nhau, song có một số thuật toán mã hóa đã được sử dụng rất rộng rãi. Trong các thuật toán mã hóa, người ta có thể phân làm 2 loại phương pháp mã hóa chính: Phương pháp mã hóa với khóa bí mật và phương pháp mã hóa Khóa bí mật - khóa công khai. Ngoài ra, hiện nay ta có thể phối hợp hai phương pháp này với nhau để tăng thêm độ an toàn trước sự tấn công thông tin bất hợp pháp.

- ***Bảo vệ bằng phương pháp vật lý:***

Là phương pháp an toàn - bảo mật thông tin được thực hiện một cách hoàn toàn bằng phần cứng. Ta có thể cấm những người không có quyền truy cập thông tin trên mạng không được sử dụng các máy nối mạng, tháo bỏ các thiết bị sao chép (ổ mềm, ổ đĩa CD-ROM ...) để chống virus xâm nhập và sự sao chép bất hợp pháp từ máy đó, đảm bảo hệ thống đường truyền không bị xâm phạm một cách trái phép.

- ***Bảo vệ bằng cách quản lý quyền truy nhập:***

Cung cấp cho mỗi người sử dụng một User name và Password để truy cập vào thông tin họ được phép truy cập. Người quản trị mạng sẽ phân quyền truy nhập và quản lý sự truy cập vào các thông tin. Đây cũng là một phương pháp khá đơn giản nhưng lại rất hiệu quả đối với người sử dụng. Song chúng không thể chống lại được với những Harker co kinh nghiệm khi mà hệ thống mạng của Trung tâm Giao dịch Chứng khoán được nối với Internet.

- ***Bảo vệ bằng chính sách Backup dữ liệu:***

Theo mô hình tổ chức hệ CSDL Oracle, chức năng backup hay phục hồi dữ liệu thuộc trách nhiệm của người quản trị CSDL hay còn gọi là DBAs. Oracle hỗ trợ rất nhiều mức Backup khác nhau tạo thành một chiến lược backup khá hoàn chỉnh bao gồm hai dạng chính là backup định kỳ và backup liên tục (archived logs Mode). Với các CSDL nhỏ, ít người dùng và có cường độ thay đổi thấp thì có thể chỉ cần backup địnhkỳ là đủ, còn với một hệ thống lớn người ta phải kết hợp đồng thời cả hai loại Backup này

Backup định kỳ

Là hoạt động backup định kỳ theo kế hoạch, chẳng hạn cuối mỗi phiên giao dịch hay cuối mỗi tháng trong năm v.v.. Có các phương pháp backup chủ yếu sau:

- Backup toàn bộ CSDL, còn gọi là hoạt động backup lạnh do nó chỉ thực hiện khi không một tiến trình nào của CSDL hoạt động hoặc khi CSDL chạy dưới chế độ Archives logs mode.

- Backup files hệ thống (control file): Thực chất đây chính là hoạt động backup cấu trúc của CSDL gồm tên CSDL, thời gian khởi tạo CSDL, nơi đặt các file dữ liệu và thông tin về hoạt động backup

- Backup Tablespace: Tablespace là một cấu trúc logic chứa đựng một nhóm đối tượng dữ liệu theo cách thức sắp xếp của người thiết kế (chẳng hạn dữ liệu giao dịch, dữ liệu lưu ký, tham số hệ thống). Phương pháp này được sử dụng với các CSDL lớn mà đôi khi việc backup toàn bộ CSDL là không thể, đặc biệt đối với các hệ phân tán. ta chỉ có thể backup các đối tượng nhảy cảm mà thôi.

- Backup files vật lý: dù oracle có hỗ trợ chức năng này nhưng nó không có hiệu quả lắm và ít khi người ta sử dụng.

Backup liên tục

Hay còn gọi là Archived Logs mode, khi CSDL sử dụng chế độ này, tất cả những thay đổi dữ liệu sẽ được ghi vào các files Archived RedoLogs. Các file này sẽ được lưu trữ riêng và có khoảng thời gian tồn tại tuỳ theo yêu

cầu của người quản trị CSDL (DBAs), thường là vài giờ hay vài ngày. Độ sai lệch của nó so với thực tế nếu có chỉ là khoảng thời gian giữa 2 checkpoint (thời gian cập nhật dữ liệu định kỳ khoảng vài giây).

Việc sử dụng các archived Logs mode là vô cùng hiệu quả với các CSDL lớn, nhiều người dùng và online liên tục 24/24. Đối với một hệ CSDL phân tán thì việc backup toàn bộ CSDL gần như là một điều không thể, người ta chỉ có thể backup các Tablespase hay sử dụng đình kỳ trong một khoảng thời gian nhất định. Trong khoảng thời gian giữa hai lần backup này nếu CSDL bị lỗi, ABAs khôi phục dữ liệu từ hai nguồn khác nhau, đầu tiên khôi phục dữ liệu của tablespace bị hỏng, sau đó sẽ thực hiện lại toàn bộ những thay đổi từ thời điểm backup đó đến thời điểm sảy ra sự cố bằng cách thực hiện lại những lệnh tác động vào CSDL theo thông tin lấy từ Archivedlogs files.

Ngoài phương pháp backup dữ liệu kể trên, đôi khi các DBAs còn sử dụng một phương pháp khác là export dữ liệu. Hiện nay hệ thống máy chủ lưu ký và đăng ký bù trừ tại TGDCK Tp.HCM đang sử dụng phương pháp này. Dữ liệu được backup cuối mỗi ngày ra fileZip và lưu sang máy tính khác (không có đĩa CD hay Tapebackup). Tuy nhiên dung lượng FileZip này rất lớn khoảng 200 mb và việc duy trì rất khó khăn.

TTGDCK có thể sử dụng giải pháp như sau:

- Sử dụng máy backup đối với các máy chủ quan trọng Giao dịch, ĐK-LK-TTBT, thông tin thị trường, giám sát thị trường: đây là các máy chủ quan trọng nhất của hệ thống Giao dịch. Dữ liệu và hoạt động của các máy chủ này đòi hỏi phải được đảm bảo an toàn tuyệt đối. Do đó TTGDCK cần phải đầu tư máy chủ backup cho mỗi máy chủ này.

- Sử dụng mạng lưu trữ ngoài như SAN (SAN storage Network) và công nghệ Clustering nhằm nâng cao năng lực lưu trữ cũng như khả năng sẵn sàng của hệ thống.

- Sử dụng Tape Driver hoặc thiết bị Backup chuyên dụng như cho máy chủ File Server/Giao dịch/ĐK-LK-TTBT/giám sát/thông tin thị trường: để đảm bảo việc lưu trữ dữ liệu an toàn khi các máy chủ này có sự cố.

- Cần kết hợp với công ty cung cấp phần mềm để xây dựng một chiến lược backup hoàn chỉnh đồng thời ở cả hai mức ứng dụng và mức CSDL. ở mức ứng dụng, các thay đổi giao dịch hàng ngày cần được xuất dưới dạng File Text sang máy PC hỗ trợ hay tapebackup (tương tự hệ thống giao dịch Thái Lan hiện nay).

- Ở mức CSDL, dữ liệu sẽ được Backup định kỳ phụ thuộc tính cấp thiết của CSDL. (như giao dịch: lần/ngày,...). Phương pháp sử dụng là backup toàn bộ CSDL, Tablespace vào Tapebackup định kỳ. Nên thực hiện Backup liên tục theo chế độ Archived logs mode

Mọi công việc backup và thủ tục/kế hoạch khôi phục sau rủi ro cần được kiểm định một cách kỹ càng. Người quản trị hệ thống cần phải định kỳ xem xét quá trình khôi phục dữ liệu. Khi lập kế hoạch backup và khôi phục sau rủi ro, cũng cần phải ước lượng thời gian khôi phục hệ thống trở lại tình trạng làm việc gần nhất, lượng dữ liệu có thể khôi phục được là bao nhiêu.

2.4.2. Lưu trữ dữ liệu

➢ ***Sự cần thiết***

Các chuyên gia trên thế giới nhấn mạnh, thông tin lưu trữ giờ đây phải được coi là tài sản mang tính chiến lược, chứ không phải một thứ "thêm thắt" vào hệ thống. Từ nhiều năm, các doanh nghiệp mua băng từ, ổ cứng để gắn thêm vào máy tính tuỳ theo nhu cầu. Nhưng áp lực cần bảo vệ nhiều dữ liệu hơn qua những khoảng thời gian lớn hơn đã làm bật lên tính quan trọng của việc lưu trữ.

Chính vì vậy, đây là phần không thể thiếu đối với bất kỳ hệ thống giao dịch chứng khoán nào trên thế giới. Đối với những thị trường chứng khoán phát triển, dữ liệu liên quan đến giao dịch chứng khoán là rất lớn và việc lưu trữ phải đảm bảo lưu trữ được dữ liệu tối thiểu của 5 năm trước (thậm chí là lâu hơn). Mặt khác việc lưu trữ dữ liệu tốt sẽ đảm bảo cho hệ thống hoạt động ngay sau khi sự cố xảy ra.

Dữ liệu, thông tin chứng khoán rất quan trọng. Nhưng lưu trữ, quản lý chúng như thế nào lại là cả một vấn đề? Việc luân chuyển dữ liệu phải đạt ba đúng: đúng dữ liệu, đến đúng nơi, đúng thời điểm và công sức ít nhất. Công nghệ lưu trữ mạng cho phép chúng ta đạt được những mục tiêu đó.

Lưu trữ mạng được hiểu đơn giản là lưu trữ qua mạng máy tính. Từ trước tới nay, phương pháp lưu trữ truyền thống là lưu trữ trực tiếp ngay trên máy tính lớn và máy chủ. Mỗi khi có nhu cầu gia tăng dung lượng lưu trữ, giải pháp hoặc là nâng cao cấu hình, cắm thêm đĩa lưu trữ hoặc là sắm thêm máy chủ. Công nghệ lưu trữ mạng đã thực sự làm một cuộc cách mạng trong lĩnh vực này.

Lưu trữ mạng không chỉ tiết kiệm tiền bạc cho lưu trữ, mà còn tiết kiệm cả tiền bạc dành cho máy chủ và nhân lực vận hành. Lưu trữ mạng tập trung hoá dữ liệu cho nhiều người cùng chia sẻ, vì vậy lượng thiết bị, công nghệ lưu trữ bạn cần mua và quản lý sẽ giảm xuống. Lưu trữ mạng cho phép không cần mua nhiều máy chủ file vì mạng NAS đã làm điều đó, cũng

không cần mua nhiều máy chủ để quản lý đĩa cứng, vì công nghệ SAN đã làm điều đó. Và một khi đã cần ít máy chủ hơn để lưu trữ, cần ít thiết bị lưu trữ, sẽ cần ít nhân lực hơn để quản lý lưu trữ. Một nghiên cứu của McKinsey và Merill Lynch cho thấy, công nghệ lưu trữ mạng sẽ tiết kiệm 47 cent trên một megabyte dữ liệu so với lưu trữ trực tiếp. "Lưu trữ mạng là một xu thế tất yếu, nếu các doanh nghiệp muốn bảo vệ dữ liệu của mình, chia sẻ dữ liệu của mình một cách tốt nhất. Nếu dữ liệu vẫn chỉ được lưu trữ trên các máy chủ thì việc bảo vệ rất khó khăn. Khi sử dụng công nghệ lưu trữ mạng cho phép bảo vệ dữ liệu, chia sẻ dữ liệu, như chúng ta đều biết dữ liệu đang ngày càng trở thành một tài sản quý giá đối với doanh nghiệp.

➢ ***Một số phương pháp lưu trữ dữ liệu***

Tùy theo nhu cầu sử dụng và kinh phí đầu tư, người dùng có thể lựa chọn giữa các giải pháp và công nghệ lưu trữ khác nhau. Theo mô hình lưu trữ, người ta có thể chia ra thành cơ chế lưu trữ với thiết bị gắn trực tiếp (DAS – Direct Attached Storage), lưu trữ qua mạng (NAS – Network Attached Storage) và mạng lưu trữ riêng biệt (SAN - Storage Area Network). Các thiết bị lưu trữ có thể sử dụng công nghệ lưu trữ trên đĩa cứng, băng từ hay đĩa quang từ...

Mỗi một mô hình, công nghệ lưu trữ có những ưu nhược điểm nhất định và được sử dụng cho những mục đích nhất định. Một số đặc điểm của các mô hình lưu trữ DAS, NAS, SAN như sau:

- DAS – Khái niệm DAS dùng để chỉ các thiết bị lưu trữ gắn trực tiếp vào server dùng lưu trữ dữ liệu. Với cơ chế DAS, mỗi server sẽ có một hệ thống lưu trữ và phần mềm quản lý lưu trữ riêng biệt. Ưu điểm của giải pháp DAS là khả năng dễ lắp đặt và cấu hình, chi phí thấp, hiệu năng cao. Tuy nhiên, nhược điểm của DAS là khả năng mở rộng hạn chế. Ngoài ra, việc quản lý hệ thống lưu trữ dùng DAS cũng là một vấn đề cần quan tâm khi số lượng server lớn.

- NAS – NAS là phương pháp lưu trữ dữ liệu sử dụng các thiết bị lưu trữ đặc biệt gắn trực tiếp vào trong mạng LAN như một thiết bị mạng bình thường (tương tự máy tính, switch hay router). Các thiết bị NAS cũng được gắn các địa chỉ IP cố định và được client truy nhập thông qua sự điều khiển của server. Trong một số trường hợp, NAS có thể được truy cập trực tiếp không cần có sự quản lý của server. NAS cung cấp khả năng chia sẻ tài nguyên lưu trữ cho nhiều người dùng đồng thời. Bên cạnh đó, NAS cho phép thực hiện mở rộng về dung lượng lưu trữ khi nhu cầu sử dụng tăng cao.

- SAN – SAN là một mạng riêng dùng cho việc truyền dữ liệu giữa các máy chủ tham gia vào hệ thống lưu trữ cũng như giữa các thiết bị

lưu trữ với nhau. SAN cho phép thực hiện quản lý tập trung và cung cấp khả năng chia sẻ dữ liệu và tài nguyên lưu trữ. Các giải pháp SAN thường được dùng với những SAN Switch riêng biệt có tốc độ Gigabit và cung cấp cho người sử dụng khả năng mở rộng, hiệu năng và tính sẵn sàng cao. Tuy nhiên SAN yêu cầu chi phí đầu tư ban đầu cao hơn so với hai giải pháp DAS và NAS. Các giải pháp SAN đặc biệt thích hợp cho môi trường hoạt động khi dung lượng lưu trữ và tính sẵn sàng là những ưu tiên hàng đầu.

➢ ***Giải pháp lưu trữ áp dụng cho các TTGDCK***

Mô hình tổng thể của hệ thống SAN

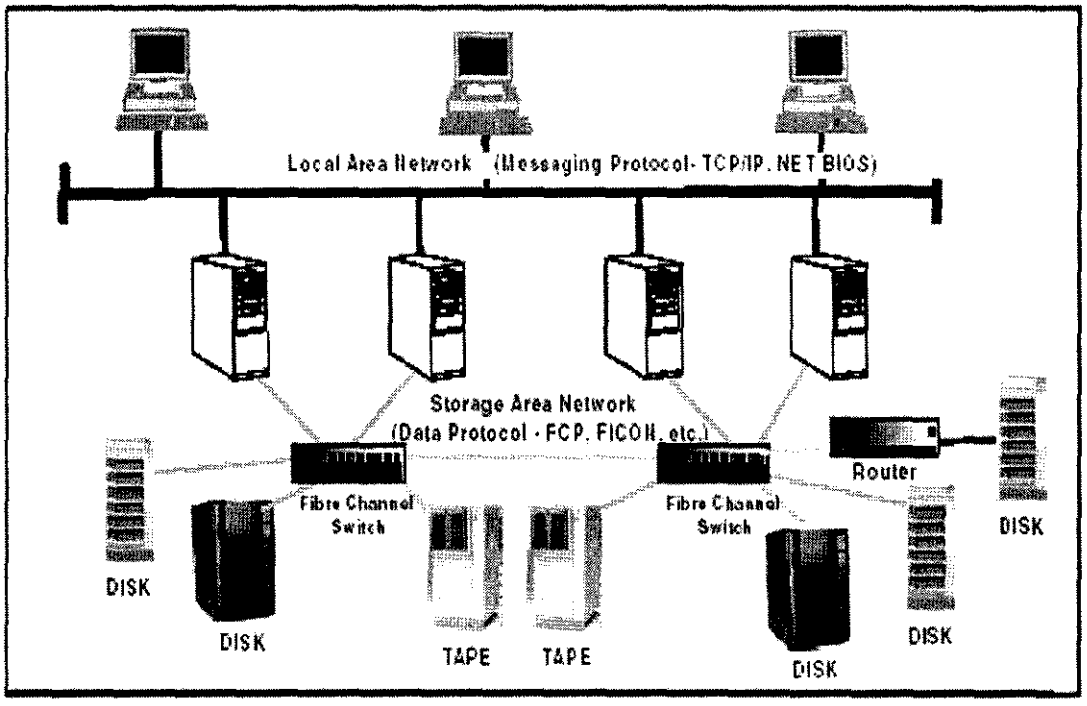


Figure 3. Storage Area Network (SAN)

Hệ thống lưu trữ SAN sẽ khắc phục được hầu hết các nhược điểm của hệ thống lưu trữ trực tiếp trên máy chủ - Thông tin được lưu trữ trên các máy chủ hoặc máy trạm riêng lẻ với hình thức phân tán về các khía cạnh sau:

- Quản trị: do thông tin lưu trữ phân tán trên các máy, việc quản trị dữ liệu sẽ yêu cầu nhiều công sức của người quản trị mạng, giảm hiệu quả làm việc của đội ngũ quản trị mạng, đặc biệt trong môi trường nhiều máy chủ phân tán.

- Tính sẵn sàng: dữ liệu lưu trữ trên các máy chủ có tính sẵn sàng không cao do phụ thuộc vào máy chủ. Ngoài ra, các công nghệ sử dụng trên máy chủ chỉ đảm bảo tính sẵn sàng của dữ liệu ở một mức nhất định.

- Bảo mật: với việc sử dụng hệ thống lưu trữ gắn liền với máy chủ, khả năng bảo mật sẽ không cao. Khả năng bảo mật là một tùy chọn khi xây dựng hệ thống SAN

- Hiệu năng: hiệu năng của hệ thống lưu trữ trực tiếp khá hạn chế do khả năng xử lý của máy chủ cũng như các công nghệ lưu trữ được sử dụng. Hiệu năng chỉ có thể được tăng lên với việc sử dụng hệ thống lưu trữ chuyên dụng có tốc độ hoạt động cao, đảm bảo khả năng phục vụ trong môi trường nặng tải

- Disaster recovery: khả năng này không được đáp ứng với hệ thống lưu trữ trực tiếp. Trong trường hợp có sự cố xảy ra với toàn bộ trung tâm dữ liệu (động đất, cháy nổ...), toàn bộ dữ liệu sẽ bị mất.

- Giới hạn khoảng cách: việc sử dụng lưu trữ với SCSI cho cự ly tối đa là 25m, với các công nghệ tương tự khác cũng giới hạn khoảng cách truy cập.

Ngoài ra, sử dụng mô hình lưu trữ San sẽ đảm bảo được khả năng lưu trữ và phục hồi (backup and restore): hệ thống lưu trữ dựa trên SAN cung cấp khả năng lưu trữ với tốc độ cao. Nó giúp tiết kiệm thời gian, giảm phức tạp trong quản lý đối với hệ thống lưu trữ cũng như tạo ra bản sao của dữ liệu để phục hồi trong trường hợp sự cố xảy ra. Việc quản lý SAN được thực hiện tập trung thông qua các công cụ hỗ trợ quản lý. Người quản lý có thể theo dõi và quản lý tất cả các thiết bị có trong SAN, bất kể vị trí các thiết bị đó như thế nào. Hệ thống quản lý SAN được kết nối thông qua các Firbe Channel switch, và qua đó kết nối đến tất cả các thiết bị có trong SAN.

Tuy nhiên, trong quá trình triển khai chi tiết xây dựng hệ thống lưu trữ mạng SAN, để có thể xây dựng hệ thống đáp ứng tốt nhất các yêu cầu mà không lãng phí, các nhân tố này cần được xem xét kỹ lưỡng khi quyết định đầu tư.

- Vị trí của các thiết bị: vị trí của các khu nhà, vị trí đặt các thiết bị mạng, server và thiết bị lưu trữ có ảnh hưởng đến yêu cầu thiết kế SAN. Với các kết nối đến thiết bị ở cự ly xa, cần có những biện pháp nhất định để tín hiệu không bị suy hao trên đường truyền, đảm bảo thông tin đến đầu thu vẫn còn tin cậy.

- Tính cục bộ của dữ liệu (data locality): nhân tố quyết định đến tính tối ưu của việc thiết kế SAN là khả năng truy cập dữ liệu giữa các thiết bị lưu trữ và các server tương ứng (server cần dữ liệu trên thiết bị lưu trữ đó). Việc thiết kế SAN phải đảm bảo các dữ liệu thường xuyên được các server sử dụng sẽ phải được đặt càng gần các server đó càng tốt (nếu như SAN trải rộng và gồm nhiều thiết bị) cũng như phải cung cấp đường truyền

tốc độ cao giữa thiết bị lưu trữ và server. Tính cục bộ (locality) liên quan đến vị trí tương đối hệ thống lưu trữ và các server truy nhập dữ liệu từ hệ thống lưu trữ đó.

- Khả năng kết nối: là tổng số cổng Fibre Channel cần thiết để kết nối các server và thiết bị lưu trữ vào SAN. Bên cạnh các cổng kết nối trực tiếp thiết bị ngoại vi vào SAN fabric (user ports), còn có các cổng thực hiện kết nối giữa các switch với nhau, tạo ra các ISL (Inter-Switch Link). Các yêu cầu về tính cục bộ của dữ liệu và vị trí vật lý của thiết bị cũng cần được xem xét để quyết định đến số lượng cổng cần thiết.

- Dung lượng lưu trữ: dung lượng lưu trữ cần được tính toán để đáp ứng được nhu cầu sử dụng cũng như sự phát triển của hệ thống trong tương lai. Có hai khái niệm liên quan đến dung lượng lưu trữ.

• Tổng dung lượng lưu trữ: được tính bằng GB hoặc TB. Tổng dung lượng lưu trữ có thể được tăng lên bằng việc sử dụng các đĩa lưu trữ có dung lượng lớn, thêm các đĩa, băng từ mới hoặc xây dựng thêm các hệ thống lưu trữ mới.

• Hiệu năng của hệ thống: với việc tăng dung lượng sử dụng của mỗi đĩa cứng thì ứng với một yêu cầu lưu trữ nhất định, số lượng đĩa cần thiết sẽ giảm đi. Tuy nhiên, có một số ứng dụng sẽ hoạt động kém hiệu quả khi giảm số lượng đĩa. Vì thế, tính toán số lượng đĩa cần thiết cho yêu cầu lưu trữ để không làm giảm khả năng hoạt động của toàn bộ hệ thống cũng là một trong những điều cần quan tâm khi thiết kế hệ thống lưu trữ.

- Khả năng mở rộng: là khả năng mở rộng hệ thống (thiết bị, cự ly, hỗ trợ các hệ điều hành và platform khác nhau) khi các yêu cầu về lưu trữ và kết nối tăng. Việc thiết kế phải tính toán đến khả năng mở rộng trong tương lai.

- Khả năng sẵn sàng của hệ thống: đánh giá độ tin cậy của hệ thống lưu trữ. Để dữ liệu luôn sẵn sàng, cần có những phương pháp sao lưu và khôi phục dữ liệu cụ thể. Việc chọn lựa phương pháp sao lưu nào phụ thuộc vào yêu cầu của từng ứng dụng. Trong một số trường hợp, việc sao lưu định kỳ là đủ để đảm bảo tính sẵn sàng của dữ liệu. Trong một số trường hợp khác, cần có nhiều đường truy cập dữ liệu giữa server và hệ thống lưu trữ để đảm bảo hệ thống luôn hoạt động cho dù một hoặc vài đường dữ liệu có vấn đề. Một số ứng dụng cũng đòi hỏi phải thực hiện sao lưu dữ liệu theo thời gian thực thay vì sao lưu định kỳ.

- Khả năng chống lại sự cố (disaster tolerance): là khả năng sao lưu và khôi phục lại dữ liệu trong trường hợp toàn bộ hệ thống bị hỏng. Những sự hỏng hóc này do những nguyên nhân không tính được trước (bão

lụt, hỏa hoạn hay hỏng toàn bộ hệ thống lưu trữ). Trong trường hợp này, việc tạo ra bản sao dữ liệu ở một hệ thống khác (cách xa về địa lý) là điều cần phải cân nhắc. Bên cạnh đó, đôi khi cần phải xây dựng nhiều hệ thống lưu trữ chạy song song để tăng khả năng chống lại sự cố.

- Khả năng lưu trữ và phục hồi (backup and restore): hệ thống lưu trữ dựa trên SAN cung cấp khả năng lưu trữ với tốc độ cao. Nó giúp tiết kiệm thời gian, giảm phức tạp trong quản lý đối với hệ thống lưu trữ cũng như tạo ra bản sao của dữ liệu để phục hồi trong trường hợp sự cố xảy ra.

2.5. Xây dựng hệ thống dự phòng

Do tính chất quan trọng của thị trường chứng khoán đối với nền kinh tế, việc ổn định, liên tục và bảo mật hệ thống là không thể thiếu. Bên cạnh đó, nhằm đảm bảo hệ thống luôn vận hành tốt khi có sự cố hoặc thiên tai xảy ra, ngoài các biện pháp như trên chúng ta nên cân nhắc đến việc triển khai xây dựng một hệ thống dự phòng được đặt tại một vị trí khác.

Giải pháp này đề xuất việc xây dựng trung tâm dự phòng làm chức năng sao lưu dữ liệu và phục hồi hệ thống đảm bảo khả năng khắc phục sự cố thảm họa đối với Trung tâm dữ liệu chính.

Chiến lược sao lưu cho hệ thống dự phòng

Chiến lược sao lưu là lựa chọn phương thức sao lưu, tần suất sao lưu dữ liệu của hệ thống

Việc hoạch định chiến lược sao lưu tối ưu phải phụ thuộc vào qui mô, tầm cỡ của hệ thống, độ quan trọng của dữ liệu và tính chất nghiệp vụ của hệ thống.

Các yếu tố ảnh hưởng trực tiếp đến chiến lược sao lưu:

- *Quy mô, tầm cỡ của hệ thống:* hệ thống càng lớn, việc phục hồi dữ liệu càng khó khăn và hầu như không thể thực hiện được nếu không có sao lưu. Chi phí và thời gian dành cho việc sao lưu cũng sẽ tỷ lệ với độ lớn dữ liệu.

- ***Độ quan trọng của dữ liệu:*** dữ liệu càng quan trọng thì việc sao lưu càng phải được thực hiện nghiêm túc, tuân thủ chặt chẽ các quy định và quy trình sao lưu dữ liệu

- *Tính trực tuyến của hệ thống:* thời gian làm việc của hệ thống, số giờ trong 1 ngày, số ngày trong 1 tuần. Tính trực tuyến của hệ thống ảnh hưởng trực tiếp đến việc quyết định thời gian và tần suất sao lưu dữ liệu

- *Tính trực tuyến của dữ liệu:* tính trực tuyến của dữ liệu ảnh hưởng đến việc quyết định tần suất và phương thức sao lưu dữ liệu. Đối với những

dữ liệu có tính trực tuyến cao, luôn luôn thay đổi, tần suất sao lưu dữ liệu cũng phải cao và việc sao lưu dữ liệu cũng phải hoạt động trực tuyến (có khả năng sao lưu dữ liệu mà không làm ngừng hoạt động của hệ thống)

- *Khả năng phục hồi dữ liệu:* là khả năng phục hồi lại dữ liệu khi không có sao lưu. Khả năng này phụ thuộc vào tính sẵn có của dữ liệu đầu vào, và phương thức cũng như thời gian nhận/nhập dữ liệu vào hệ thống.
- Yêu cầu khác

Phục hồi hệ thống

Trong trường hợp máy chủ tại TTGDCK bị sự cố vì một lý do bất khả kháng (hỏng hóc thiết bị, động đất, hoả hoạn, v.v...) không có thể tiếp tục hoạt động ngay được, cần có một quy trình phục hồi hoạt động của máy chủ này. Quy trình phục hồi hoạt động như sau:

- ***Nguyên tắc chung:*** Dùng máy chủ dự phòng thực hiện việc phục hồi.
- *Bước 0:* Cài sẵn máy chủ dự phòng từ trước. Các cấu phần cần được cài đặt trước như:
  - Cấu hình thiết bị phần cứng (theo đúng thông số đã định trước)
  - Cài đặt hệ điều hành (theo đúng thông số đã định trước)
  - Cài đặt hệ quản trị CSDL ORACLE (theo đúng thông số đã định trước)
  - Cài đặt phần mềm ứng dụng (theo đúng thông số đã định trước)
- *Bước 1:* Sau khi tiếp nhận yêu cầu khắc phục của các bộ phận, cán bộ tin học sẽ tiến hành thiết lập các thông số hệ thống của riêng bộ phận đó.
- *Bước 2*: Tiến hành phục hồi CSDL đến thời điểm bị sự cố từ các thiết bị lưu trữ dữ liệu
- *Bước 3*: Đưa máy chủ dự phòng vào hoạt động.
- *Bước 4*: Tiến hành khắc phục máy chủ đã gặp sự cố
- *Bước 5*: Sau khi khắc phục xong máy chủ gặp sự cố, tiến hành thay thế cho máy chủ dự phòng

2.6. Đào tạo nguồn nhân lực

Công tác đào tạo và phát triển nguồn nhân lực đối với cán bộ tin học trong ngành chứng khoán cần được quan tâm đúng mức: Trong vòng 5 năm tới để xây dựng được một đội ngũ cán bộ tin học có đủ trình độ, năng lực để

vận hành và khai thác có hiệu quả các hệ thống phần mềm ứng dụng phục vụ ngành chứng khoán, UBCKNN và TTGDCK cần chú trọng đầu tư thích đáng trong công tác đào tạo, có chính sách động viên, khuyến khích cán bộ tin học an tâm phục vụ lâu dài ngành chứng khoán.

Chiến lược đào tạo nguồn nhân lực công nghệ thông tin cần định hướng

- Đào tạo những chuyên gia phân tích, những người xây dựng bài toán cho các lập trình viên. Người phân tích hệ thống phân tích nhu cầu từ phía người sử dụng đưa ra, đưa ra quy trình phần mềm.
- Đào tạo lập trình viên đủ trình độ thực hiện những module do Trưởng dự án đưa ra.
- Đào tạo Kiến trúc sư phần mềm để xây dựng kiến trúc phần mềm và lắp ghép những module do lập trình viên đưa lên.
- Đào tạo các Trưởng dự án về CNTT...
- Đào tạo người quản trị hệ thống :

Người quản trị là đầu mối trước tiên cho việc liên lạc yêu cầu hỗ trợ của người sử dụng. Người quản trị cần phải vạch ra kế hoạch đào tạo, huấn luyện cho người sử dụng và các nhân viên trợ giúp về an toàn, bảo mật trong toàn tổ chức cung như trong phạm vi công việc của từng người. Điều quan trọng là phải làm cho người sử dụng cùng thấu hiểu được tầm quan trọng của vấn đề an toàn, bảo mật trong hệ thống thông tin mà họ đang làm việc. Ngoài ra, quản trị hệ thống phải xây dựng kế hoạch các công việc thực hiện thường xuyên như:

Thường xuyên cập nhật, bảo trì hệ thống: Các nhà cung cấp thường xuyên đưa ra các bản sửa lỗi cho vấn đề an toàn, bảo mật của họ. Người quản trị hệ thống cũng phải thường xuyên theo dõi sát sao và cập nhật vấn đề này. Tuy nhiên, người quản trị cũng phải đặc biệt chú ý tới những lỗ hổng, hay những ảnh hưởng của các bản sửa lỗi này nên hệ thống sẵn có trước khi định cài đặt trên hệ thống của mình.

Kiểm tra các lỗ hổng: Với vai trò là người quản trị hệ thống, bạn phải đi trước trong việc lấp các lỗ hổng cho hệ thống của mình trước khi kẻ địch có thể phá hoại. Đa số các lỗ hổng của các hệ điều hành đều được công bố rộng rãi. Việc kiểm tra và lấp các lỗ hổng về bảo mật cần phải được xem xét như là một công việc định kỳ. Bạn cần phải đưa ra kế hoạch cụ thể để đối phó với các tình huống. Cụ thể, cần phải vạch rõ kế hoạch cho các công việc:

- Rà soát các lỗ hổng.

- Phân tích, đánh giá ảnh hưởng của các lỗ hổng lên hoạt động của hệ thống.

- Thực hiện vi lấp các lỗ hổng.

- Thống kê, báo cáo, hoặc đưa ra các hướng dẫn cho việc kiểm tra các lỗ hổng.

Kiểm soát theo dõi hệ thống một cách thường xuyên: Công việc kiểm soát hệ thống cần phải được tiến hành thường xuyên. Các thao tác xoá, sửa, thay đổi quyền trên các file này cần phải được lưu giữ lại như là các bằng chứng sau này.

Tài liệu hoá và quản lý cấu hình: Một trong những yêu cầu của công việc quản trị hệ thống là việc tài liệu hoá và quản lý cầu hình. Các hệ thống, ứng dụng sẽ trở nên dễ sử dụng nếu chúng được tài liệu hoá một cách cẩn thận, tỉ mỉ. Việc quản lý, theo dõi cấu hình của phần cứng, phần mềm trong hệ thống sẽ hỗ trợ tích cức cho công đoạn khôi phục sau rủi ro, phát hiện kẻ xâm nhập trái phép vào hệ thống, gỡ rối các vấn đề liên quan, ...

Sao lưu và khôi phục sau rủi ro: Trong mọi trường hợp, dù có chuẩn bị kỹ càng đến đâu, dù có hệ thống phần cứng, phần mềm đáng tin cậy, an toàn, rủi ro vẫn có thể xảy đến đối với hệ thống. Người quản trị cần phải có kế hoạch sao lưu (backup), và vạch trước các kế hoạch đối phó với các rủi ro hay kế hoạch khôi phục lại hệ thống sau rủi ro. Đa số các hệ điều hành hiện nay đều có kèm theo các công cụ backup, công cụ khôi phục.

III Kiến nghị các điều kiện thực hiện.

3.1 Về điều kiện pháp lý

Ngành viễn thông của Việt Nam đang phát triển ở giai đoạn đầu, hạ tầng cơ sở kỹ thuật phát triển chưa đồng bộ Tuy vậy, Việt Nam có cơ hội nắm bắt và tiếp cận với những công nghệ mới nhất trên thế giới nếu được đầu tư và có chính sách hợp lý trong việc xây dựng cơ sở hạ tầng viễn thông toàn diện. Theo đó CNTT Việt Nam nói chung và lĩnh vực chứng khoán nói riêng cần xây dựng được các chính sách cụ thể như:

- Luật khung về thông tin điện tử;

- Chính sách đào tạo nguồn nhân lực và chuẩn hóa công nghệ thông tin;

- Chính sách mua sắm, sử dụng trang thiết bị và dịch vụ CNTT;

- Khuyến khích ứng dụng CNTT gắn liền với yêu cầu tiết kiệm, thiết thực, hiệu quả;

- Chính sách an ninh và bảo mật thông tin thống nhất trên toàn quốc;

- Cụ thể hóa Pháp lệnh về chuyển giao công nghệ nước ngoài vào Việt Nam trong lĩnh vực CNTT theo hướng khuyến khích, hỗ trợ, đặc biệt chú trọng đến các doanh nghiệp phần mềm;

- Cần nghiên cứu kinh nghiệm phát triển CNTT của các nước trong khu vực và trên thế giới ...

3.2 Kiến nghị đối với UBCKNN, TTGDCK

- Nhanh chóng xây dựng định hướng phát triển CNTT trong lĩnh vực chứng khoán đến năm 2010;

- Hoàn thiện hệ thống văn bản pháp luật liên quan chứng khoán và thị trường chứng khoán bao gồm:

+ Sửa đổi hoặc bổ xung các Văn bản pháp quy về chứng khoán và thị trường chứng khoán Việt Nam liên quan các doanh nghiệp vừa và nhỏ niêm yết trên thị trường chứng khoán tập trung hoặc thị trường OTC;

+ Ban hành Luật chứng khoán, trong đó có các quy định liên quan đến các vấn đề về kinh doanh điện tử.

+ Xây dựng mô hình định hướng hoạt động rõ ràng giữa 2 TTGDCK.

- Vấn đề nguồn nhân lực, đặc biệt là cán bộ tin học luôn luôn là trọng tâm của mọi tổ chức, đơn vị vì nó quyết định sự tồn tại, phát triển hệ thống CNTT tại đơn vị đó. Do đó cần phải hoạch định chiến lược về mọi khía cạnh liên quan đến nguồn nhân lực về CNTT. Xây dựng kế hoạch đào tạo dài hạn, bổ sung cán bộ Tin học cho TTGDCK.

- Nguồn tài chính và cơ sở vật chất. Có thể nói hầu như tất cả mọi vấn đề từ công tác chuẩn bị cho sự ra đời của các TTGDCK cho đến khi các TTGDCK thực sự đi vào hoạt động đều liên quan đến vấn đề tài chính. Do vậy, khi xây dựng một hệ thống CNTT đảm bảo được các yêu cầu đặt ra, cần có một cơ chế tài chính rõ ràng, bên cạnh đó, UBCKNN cũng cần phải tranh thủ mọi nguồn tài trợ và trợ giúp kỹ thuật từ các tổ chức quốc tế, các UBCK và sở giao dịch chứng khoán các nước.

KẾT LUẬN

Trên cơ sở nghiên cứu một số vấn đề về bảo mật và an toàn đối với hệ thống CNTT, cũng như qua việc nghiên cứu khảo sát thực trạng về bảo mật và an toàn của hệ thống TTGDCK HCM và hệ thống đang hoàn thiện tại TTGDCK HN, đề tài đã đề xuất một số giải pháp nhằm nâng cao tính an toàn và bảo mật thông tin cho hệ thống máy tính tại TTGDCK .

Chúng tôi mong rằng, các giải pháp mà đề tài đã nêu ở trên cùng với những giải pháp tổng thể khác sẽ góp phần nâng cao khả năng quản lý và điều hành hoạt động của thị trường chứng khoán tạo, nhằm hướng đến một hệ thống ổn định, hiệu quả và công bằng cho các thành viên tham gia thị trường. Mặt khác, sẽ tạo đà phát triển và mở rộng thị trường chứng khoán ở Việt Nam trong xu thế hội nhập với sự phát triển của nền kinh tế thế giới.

TÀI LIỆU THAM KHẢO

Tiếng Anh

1. The Impact of recent technological advances on the securities markets-Report to the Congress. U.S. Securities and Exchange Commission.
2. The State Securities Commission of the SRV & Korea Stock Exchange Korea International Cooperation Agency:

   Final Report on the Technical Assistance for the establishment of a Stock Exchange in Vietnam. April 1998.
3. American Power Convesion (APC): Non-stop Networking. APC Legendary Reliability. 30/10/2001.
4. Cisco Systems: Cisco Secure Manager 2.2
5. Cisco Systems: Cisco Firewall Quick Look
6. Cisco Systems: CCNA

6. COSCOM-KOREA: IT course for Vietnamese Traineees, 3/6/2002

Tiếng Việt

7. Các giáo trình của đề án 112 Chính phủ-Chương trình tổng thể cải cách hành chính của Chính Phủ giai đoạn 2001-2010
8. Uỷ ban Chứng khoán Nhà nước(SSC) & Sở giao dịch chứng khoán Hàn Quốc (KSE): Báo cáo đợt 1 Dự án trợ giúp thành lập Sở giao dịch chứng khoán Việt Nam. Hà Nội, 7.1997.
9. Uỷ ban Chứng khoán Nhà nước. Trung tâm Giao dịch chứng khoán TP.HCM: Báo cáo kết quả làm việc với chuyên gia Hàn Quốc (30/8-

10/9/1999) Hệ thống giao dịch - Công bố thông tin - Hệ thống giám sát.