Chương 3

Gia cố hệ thống

- Khái niệm
- Gia cố hệ điều hành và hệ điều hành mạng
- Gia cố ứng dụng mạng
- Chính sách an ninh
- Các bước điều tra xâm nhập

Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan các kỹ thuật sử dụng trong gia cố hệ thống nhằm ngăn chặn các cuộc tấn công.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Hiểu được thế nào là gia cố hệ thống.
  - Phân loại được gia cố hệ điều hành và hệ điều hành mạng.
  - Trình bày được các kỹ thuật gia cố ứng dụng và dịch vụ mạng.
  - Hiểu được cách tổ chức chính sách an ninh mạng.
  - Mô tả được các bước điều tra xâm nhập.

Khái niệm về gia cố hệ thống

- Gia cố hệ thống (system hardening)

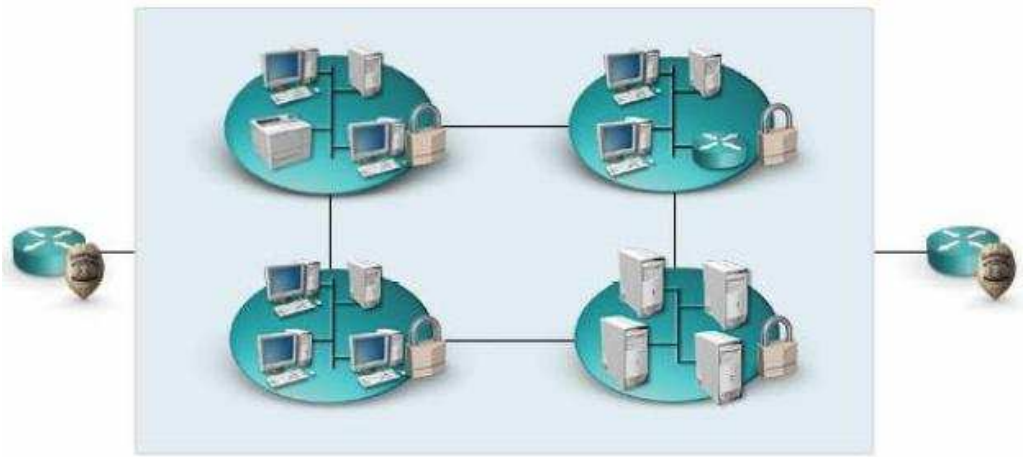
Gia cố hệ thống là quá trình làm cho hệ thống máy tính và hệ thống mạng vững chắc hơn, khó bị tấn công hơn.

Làm cho kẻ xâm nhập bỏ ý định tấn công để chuyển qua 1 mục tiêu khác dễ dàng hơn

Các đối tượng cần phải gia cố bao gồm:
- Hệ điều hành
- Hệ điều hành mạng
- Ứng dụng mạng

Gia cố hệ điều hành và HĐH mạng

- Khái niệm



Quá trình gia cố cơ sở hạ tầng mạng và cài đặt các chính sách bảo mật sẽ **cung cấp các tầng bảo vệ** để chống lại các tội phạm tin học cùng với các hệ thống phát hiện xâm nhập giúp **bảo đảm những thiệt hại khi bị tấn công xuống mức thấp nhất**.

Các vấn đề cần quan tâm trong gia cố HĐH:

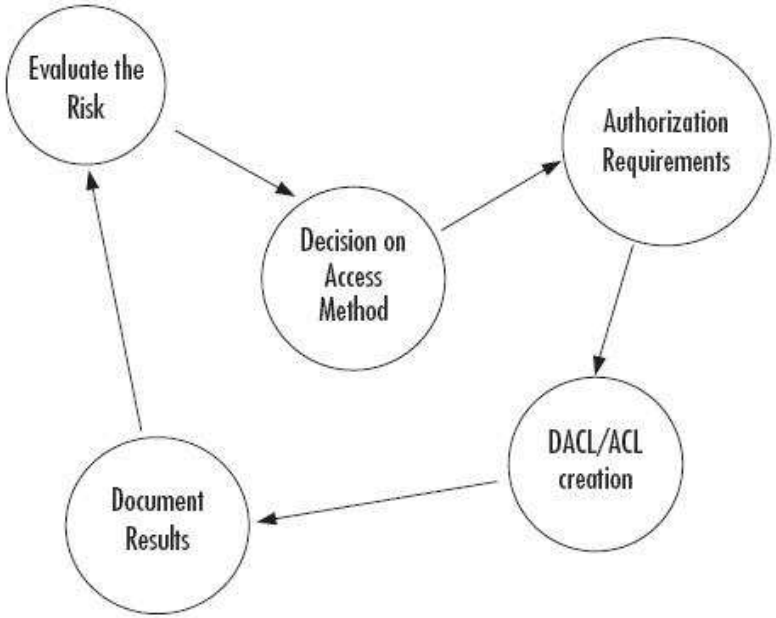
- Hệ thống tập tin
- Update
- Hotfix
- Service pack
- Patch

Gia cố hệ điều hành và HĐH mạng

- Hệ thống tập tin

Người dùng chỉ được **cấp các quyền ít nhất** sao cho **vừa đủ** có thể hoàn thành được công việc của họ

- Nhóm các người dùng có cùng các yêu cầu truy cập vào cùng 1 nhóm.
- Định quyền cho nhóm.
- Hiệu chỉnh các quyền riêng cho cá nhân



Sau khi xác định được những rủi ro từ các phương thức truy cập nào đó, người quản trị sẽ **thiết lập các chính sách điều khiển truy cập** và những loại **chứng thực** nào cho hệ thống để truy cập được các tài nguyên được bảo vệ đó.

Gia cố hệ điều hành và HĐH mạng

- Bản cập nhật (Update)

• Cung cấp bởi chính **những nhà sản xuất ra hệ điều hành.**
• Truy cập từ Website của nhà sản xuất
• Chứa những nâng cấp hệ điều hành hay các thành phần trong hệ điều hành.

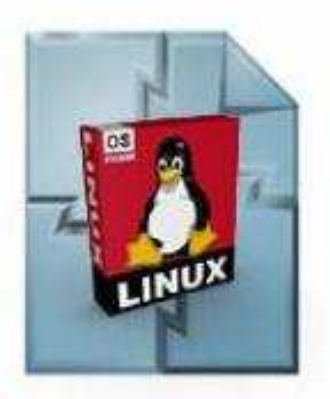
• Nâng cao khả năng hoạt động
• Bổ sung thêm một tính năng mới của hệ điều hành

• Trước tiên, phải kiểm tra ảnh hưởng của nó đến hệ thống.
• Kiểm tra toàn diện trở lại sau khi cài đặt xem có ẩn chứa những vấn đề bảo mật mới không.

Phân biệt với Upgrade
• Update: sửa đổi, thay thế, … => miễn phí
• Upgrade: bổ sung, thêm mới => tính phí

Gia cố hệ điều hành và HĐH mạng

- Bản sửa lỗi (Hotfixes)



• Thường được dùng để **chỉnh sửa 1 số các vấn đề** xảy ra trên 1 số lượng ít các máy trạm hay server.
• Thường được cung cấp từ **những nhà sản xuất phần cứng** để điều chỉnh 1 số không tương thích.

• Có thể được cài đặt mà không cần phải làm gián đoạn quá trình hoạt động của hệ thống.
• Chỉ được kiểm thử trên 1 số ít thiết bị nên có khả năng không hoạt động tốt trên các thiết bị khác.

Khi thật cần thiết, mới nên cài đặt Hotfix vào hệ thống

Gia cố hệ điều hành và HĐH mạng

- Bản vá lỗi (patches)

• Các bản vá lỗi được tạo ra đa số có **liên quan đến vấn đề an toàn** cho hệ thống.
• Chúng thường được nhóm lại với nhau để vá lỗi cho một nhóm các vấn đề cùng 1 lúc.

• Dùng để chỉnh sửa tạm thời
• Bỏ qua 1 số phần lỗi của 1 ứng dụng
• Giải quyết nhanh các vấn đề cụ thể trong hệ điều hành.

Không được kiểm thử kéo dài và triển khai trên nhiều hệ thống

Service Pack: tập hợp của nhiều patch, hotfix, update, …

• Không an toàn như cài đặt các bản cập nhật
• Nên backup lại các file gốc trước khi cài đặt bản vá

Gia cố ứng dụng mạng

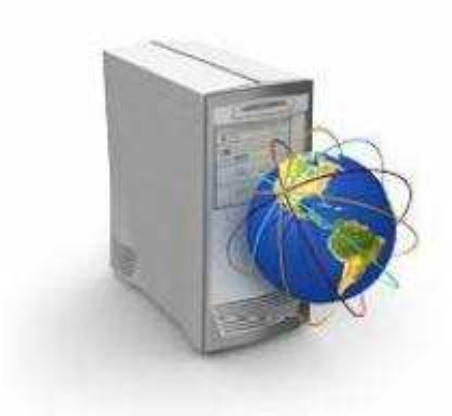
- Khái niệm

Rất nhiều hệ điều hành rất an toàn nhưng khi kết hợp với các dịch vụ mạng phải đối mặt với các vấn đề bảo mật

Ứng dụng mạng là các mục tiêu được hacker quan tâm nhiều nhất tùy thuộc vào các điểm yếu được công bố và tính thông dụng của ứng dụng đó

Gia cố ứng dụng mạng

- Web Server



• Hacker rất quan tâm đến sự hiện diện của các website và hiểu rất rõ cách thức hoạt động của các webserver.
• Đôi khi đây là điểm duy nhất mà hacker có thể tấn công vào mạng.

Các bước gia cố cho WebServer:

• Gia cố cho **hệ điều hành** trước: cài đặt các bản cập nhật, vá lỗi, gỡ bỏ các dịch vụ và giao thức không cần thiết.
• Đặt Website phía sau một hàng rào chắn bảo vệ như **tường lửa hay proxy**
• Gia cố cho chính **WebServer** và **Website** đó
  o Kiểm tra các quyền của tài khoản anonymous nối kết đến Web Server.
  o Nên tạo các tài khoản riêng dùng cho các thao tác quan trọng trên web.
  o Chuyển qua chứng thực bằng SSL (nếu cần).

Gia cố ứng dụng mạng

- Mail Server

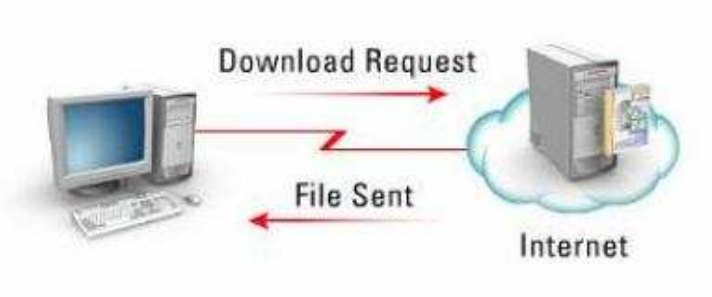
Mail Server có thể bị các dạng tấn công như: DoS, virus, tấn công giả mạo và tấn công relay.

Các bước để gia cố cho Mail Server:

- Cài đặt chương trình diệt virus dành riêng cho Server
- Không cài đặt các dịch vụ và ứng dụng mạng nào khác trên Server.
- Kiểm soát chặt chẽ các quyền admin và quyền truy xuất hệ thống
- **Relay Server** cấu hình chỉ cho phép các người dùng hợp lệ gửi mail
- Cài đặt bộ **lọc spam** và chống DoS
- Cấu hình cơ chế chống **Bomb-mail** : số lượng, kích thước, khoảng thời gian để gửi email, …
- Đảm bảo webserver hỗ trợ webmail phải an toàn (được gia cố).

Gia cố ứng dụng mạng

- FTP Server



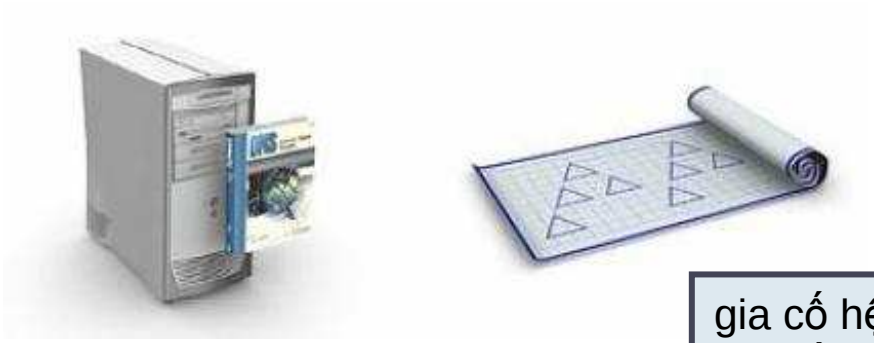
FTP là 1 giao thức không an toàn vì nó gửi tất cả thông tin chứng thực trên mạng là dạng plain-text.

Các bước để gia cố cho FTP Server:

- Cấu hình cẩn thận tài khoản vô danh (anonymous)
- Tài khoản FTP và tài khoản người dùng (trên HĐH) nên tách biệt.
- Cô lập đĩa phục vụ FTP riêng với đĩa chứa hệ thống file hệ thống và các dữ liệu quan trọng khác.
- FTP Server hoạt động tại vùng DMZ:
    - Có khả năng bị tấn công từ chính người dùng bên trong mạng.
    - Nên có cơ chế kiểm soát và phòng ngừa việc tấn công trở lại mạng cục bộ khi FTP Server bị thâm nhập.
- Kiểm tra thường xuyên log file và vùng đĩa cho phép Upload.

Gia cố ứng dụng mạng

- DNS Server



Một trong những cách tấn công là tấn công DNS Server để đánh lừa người dùng truy cập qua 1 địa chỉ giả mạo khác

gia cố hệ điều hành mạng trước rồi sau đó mới đến gia cố chính bản thân của dịch vụ DNS

Các bước để gia cố cho DNS Server:

- Tách biệt hệ thống tên miền Internet và hệ thống miền cục bộ phục vụ cho mạng LAN.
- Bảo đảm các cập nhật giữa những DNS Server phải nằm trong vùng (zone) được kiểm soát.
- Người dùng gửi các yêu cầu DNS cũng phải giới hạn trong vùng cho phép thông qua ACL.
- Yêu cầu các DNS Server chứng thực lẫn nhau trước khi chấp nhận các thông tin cập nhật.

Gia cố ứng dụng mạng

- Server phục vụ chia sẻ file và máy in

Đôi khi người dùng không quản lý được việc chia sẻ của mình và tạo cho người khác có thể xâm nhập và lợi dụng việc truy xuất đó

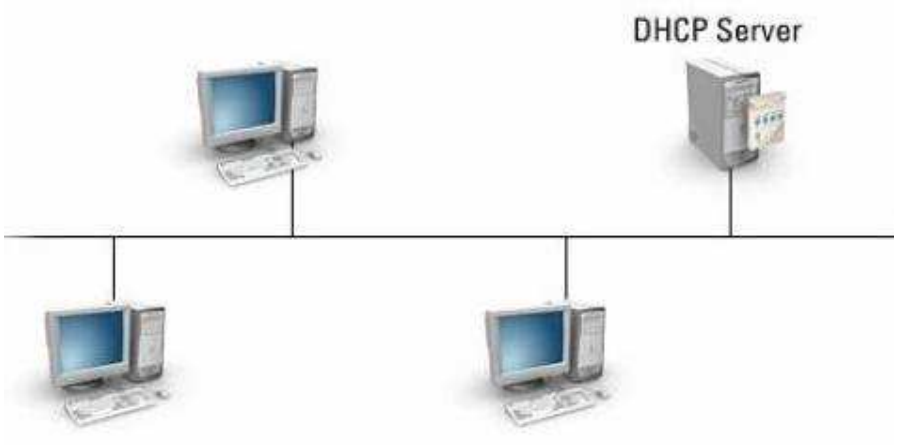
Khi chia sẻ, dịch vụ sẽ tự động thực hiện trên tất cả các card mạng của Server => người dùng ở ngoài sẽ "thấy" các tài nguyên đó như người dùng cục bộ bên trong mạng.

Các đề nghị việc gia cố :
- Tạo ra Server chuyên dụng để phục vụ
- Thực hiện chia sẻ tài nguyên chính xác.
- Bảo mật địa chỉ của Server

Nên tắt dịch vụ này trên Server và máy trạm nếu không sử dụng.

Gia cố ứng dụng mạng

- DHCP Server



Thực hiện việc dành chổ sẵn (reservation) và tạo bộ lọc dựa theo địa chỉ MAC của các Client.

Hạn chế được các máy tính trái phép thâm nhập vào mạng (nhất là trong mạng WLAN).

Gia cố ứng dụng mạng

- Database Server

Mỗi loại database chạy trên các nền hệ điều hành khác nhau, sử dụng các port khác nhau và có những nguy cơ bảo mật khác nhau

- Cấu hình đúng dịch vụ
- Mật khẩu phải đủ khó
- Bản vá, bản cập nhật phải luôn được quan tâm.

- Backup lại dữ liệu định kỳ
- Đường truyền trong giao tiếp với Webserver, Application Server phải được xem xét cẩn thận

Chính sách an ninh mạng

- Khái niệm

Chính sách an ninh mạng (**network security policies**) quy định những thao tác nào trên mạng được xem là đúng.

Chính sách an ninh mạng bao gồm tập các quy tắc những thao tác cho phép và không cho phép.
Được chuẩn hóa trong các RFC như 2504, 2196, …

Việc xây dựng chính sách an ninh của một tổ chức (công ty) nên dựa theo những chính sách an ninh chuẩn như sau:
- Chính sách giới hạn truy cập
- Chính sách an ninh cho máy trạm
- Chính sách an ninh vật lý
- và các chính sách an ninh khác …

Chính sách an ninh mạng

- Chính sách giới hạn truy cập (restricted access)

Mỗi nhân viên chỉ có thể thực hiện được các **truy cập tối thiểu** theo yêu cầu công việc của mình. Khi có quyền hơn thế sẽ tạo ra các rủi ro về bảo mật.

Các chính sách an ninh giới hạn truy cập có thể bao gồm các vấn đề như:
•Hạn chế truy cập vào hệ thống file hay dữ liệu trên Server cục bộ.
• Hạn chế truy cập Internet: yêu cầu tài khoản và mật khẩu.
• Giới hạn truy cập vào hệ thống VPN: đòi hỏi username, số PIN, số của token được cung cấp, ...
• Thường sử dụng đến các **điều khiển truy cập**.
• Giới hạn truy cập không chỉ về dữ liệu mà áp dụng cho cả về con người.

Chính sách an ninh mạng

- Chính sách an ninh cho máy trạm (workstation security policies)

Máy trạm là 1 máy tính nối kết đến mạng và sử dụng các tài nguyên của mạng.

Các chính sách an ninh cho máy trạm có thể bao gồm các vấn đề như:

- Lưu trữ file trên máy tính và copy dữ liệu ra thiết bị lưu trữ ngoài.
- Thay đổi cấu hình, giao thức mạng, cài đặt phần mềm, …
- Tài khoản người dùng cục bộ và quyền của người dùng.
- Việc sử dụng các thiết bị di động và cầm tay mang vào cơ quan.

Chính sách an ninh mạng

- Chính sách an ninh vật lý (physical security)

Giới hạn các truy cập vật lý trực tiếp, hạn chế những nguy cơ xảy ra.

Các chính sách an ninh vật lý có thể bao gồm các thành phần như:

- Địa điểm: phòng Server, phòng thí nghiệm, ...
- Tài sản: phần cứng, phần mềm, dữ liệu, thiết bị, …
- Mức độ an toàn: tủ bảo vệ, khóa, loại chứng thực, …
- Thủ tục chứng thực: ai cần chứng thực, chứng thực như thế nào , …
- Giám sát và ghi nhận: ai ở địa điểm này vào thời gian nào.

Chính sách an ninh mạng

- Các bước để xây dựng các chính sách an ninh

Risk analysis
1. Inventory assets
2. Determine threats
3. Investigate vulnerabilities
4. Decide actions on risks

Phân tích rủi ro là bước đầu tiên phải thực hiện trong việc xây dựng các chính sách an ninh mạng.

Compliance monitoring and evaluation

Security policy
1. Due care
2. Separation of duties
3. Need to know

Các thành phần trong chính sách an ninh mạng

Incident response policy
Ethics policy

Acceptable use policy (AUP)
Human resource policy
Password management policy
Privacy policy
Disposal and destruction policy
Service-level agreement (SLA) policy

Một số chính sách an ninh mạng thông dụng

Chính sách an ninh mạng

- Các thành phần trong chính sách an ninh mạng

Quan tâm xứng đáng (due care)
Người chủ và người quản lý tài sản phải có nghĩa vụ quan tâm đến tài sản đó và có những biện pháp phòng ngừa để bảo vệ chúng.

• Sử dụng cẩn thận thiết bị, dữ liệu, phần mềm, … tránh gây ra hư hỏng hay tạo các lỗ hổng để bị xâm nhập.
• Bảo dưỡng thiết bị định kỳ, sao lưu dữ liệu thường xuyên

• Giám sát và ghi nhận các sự kiện xảy ra trên hệ thống để có thể dự đoán, phân tích và phát hiện các tấn công hay xâm nhập.
• Không để **hacker chiếm quyền điều khiển hệ thống và dùng nó tấn công một hệ thống khác** trên mạng vì như vậy cũng **xem như mình vi phạm**.

Chính sách an ninh mạng

- Các thành phần trong chính sách an ninh mạng

Sự riêng tư (privacy)

Người quản trị và đội ngũ quản lý có quyền sử dụng các phần mềm để giám sát trên hệ thống mạng bao gồm cả những thông tin riêng tư (như nội dung email, các địa chỉ Web đã truy cập) mà người dùng sử dụng trên mạng của công ty, tổ chức.

Chính sách an ninh mạng

- Các thành phần trong chính sách an ninh mạng

Tách biệt phận sự (separation of duties)

• Các quyền được cấp sẽ phụ thuộc vào vai trò và phận sự của người và nhóm người đó.
• Mỗi người sẽ chịu trách nhiệm cho phần việc của mình.

Win2000 và Win2003 sử dụng Active Directory để cho phép phân chia phận sự cho những người quản trị mạng.

Nếu có vấn đề xảy ra, có thể dễ phát hiện và khoanh vùng để xử lý

Chính sách an ninh mạng

- Các thành phần trong chính sách an ninh mạng

Cần biết (need to know)

Dữ liệu được phân loại và cung cấp vừa đủ cho đối tượng cần phải biết để thực hiện được công việc của mình.

Win2003 khi cài đặt là 1 hệ thống "đóng". Người quản trị sẽ được yêu cầu xác định các nhu cầu của người dùng và sau đó mới cho phép truy cập.

Chính sách an ninh mạng

- Một số loại chính sách an ninh thông dụng

Name of Security Policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Analog line policy	Defines standards for use of analog dial-up lines for sending and receiving faxes and for connection to computers
Antivirus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments and investigate incidents to ensure conformance to security policies or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded t an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Dial-in access policy	Outlines appropriate dial-in access and its use by authorized personnel

Có nhiều chính sách an ninh mạng có thể được thiết lập tùy thuộc vào yêu cầu của tổ chức.

Chính sách an ninh mạng

- Một số loại chính sách an ninh thông dụng (tt)

Name of Security Policy	Description
Demilitarized zone (DMZ) security policy	Defines standards for all networks and equipment located in the DMZ
E-mail policy	Creates standards for using corporate e-mail
E-mail retention policy	Helps employees determine what information sent or received by e-mail should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations t access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organ tion's information in a manner appropriate to its level o security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security c servers
Virtual private network (VPN) security policy	Establishes requirements for Remote Access IP security (IPSec) or Layer 2 Tunneling Protocol (L2TP) VPN connections to the organization's network
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

Một số chính sách an ninh mạng đã được chuẩn hóa và cho phép download mẫu (template) về hiệu chỉnh.

Có thể truy cập một số chính sách an ninh mẫu tại: www.sans.org/resources/policies

Chính sách an ninh mạng

- Chính sách những việc sử dụng được chấp nhận (acceptable use policies)

Đề ra các hoạt động nào được phép thực hiện khi sử dụng máy tính và mạng.

Các chính sách cụ thể được soạn thảo giống như hợp đồng được ký kết giữa công ty và nhân viên.

Chính sách AUP quy định một số vấn đề cụ thể như:

- Không dùng tài nguyên mạng của tổ chức để đe dọa hay tấn công người khác.
- Giới hạn các loại website và email được sử dụng.
- Các thao tác online nào được được phép và cấm sử dụng (chẳng hạn: game).
- Không dùng mạng cơ quan cho việc riêng.
- Các loại thông tin nào không được lan truyền, email, …

Chính sách an ninh mạng

- Chính sách quản lý mật khẩu và chứng chỉ số (Password and certificate management policy)

Chính sách này quy định mật khẩu như sau:

- Mật khẩu đặt phải đủ mạnh: bao gồm ký tự chữ thường và chữ HOA, số, ký tự đặc biệt, …
- Mật khẩu phải thay đổi trong 1 thời gian quy định trước (45-90 ngày).
- Không sử dụng lại các mật khẩu cũ.
- Dùng kèm với các ký thuật chứng thực khác.

Tài khoản administrator (hoặc root) thường không nên sử dụng và mật khẩu phải được bảo quản cẩn thận.

- Chứng chỉ số được sử dụng khi muốn thông tin truyền đi trên mạng được đi từ đúng người gửi và đến đúng người nhận.
- Thường dùng khi mua bán trên mạng với thanh toán thông qua thẻ tín dụng.

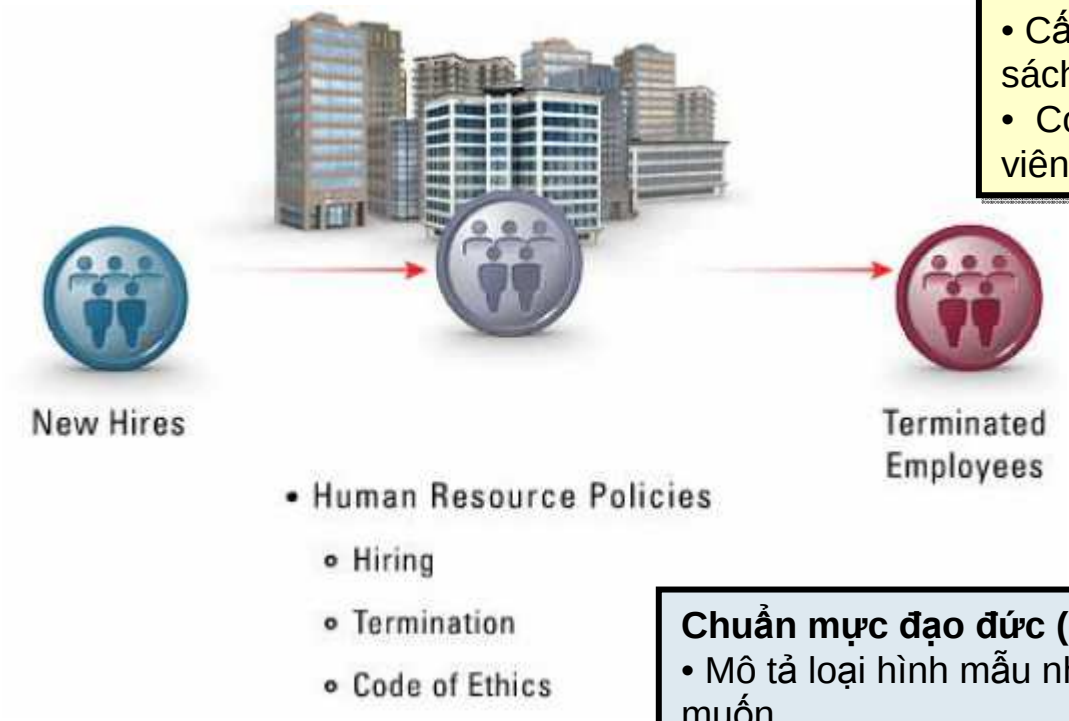
Chính sách an ninh mạng

- Chính sách bỏ và hủy (disposal & destruction)

• Khi bỏ các thiết bị máy tính như đĩa cứng, đĩa mềm, CD, … phải có giải pháp xóa vĩnh viễn các dữ liệu bên trong bằng các phần mềm chuyên dụng.
• Các tài liệu khi bỏ đi cũng phải hủy cẩn thận.

Chính sách an ninh mạng

- Chính sách của phòng nhân sự (Human Resource policy – HR policy)



Hiring (thuê)
• Cấp thẻ, tạo tài khoản (mật khẩu) và chính sách an ninh cho nhân viên mới được thuê.
• Có các hướng dẫn và quy định cho nhân viên mới thuê này.

Termination (kết thúc)
• Thu lại thẻ, khóa (không xóa) tài khoản cho nhân viên kết thúc hợp đồng.
• Các dữ liệu có liên quan đến nhân viên này phải được backup lại.

Chuẩn mực đạo đức (code of ethics)
• Mô tả loại hình mẫu nhân viên mà công ty, tổ chức mong muốn.
• Các quy định liên quan đến đạo đức nghề nghiệp, xã hội.

Các bước điều tra xâm nhập

- Giới thiệu

Hacking Tools and Implements

Pháp y máy tính (computer forensics) bao gồm 1 quá trình thu thập các chứng cứ để có thể phát hiện ra tội phạm.

- Không chỉ đơn thuần là phục hồi lại dữ liệu hay làm cho hệ thống hoạt động trở lại.
- Phải tuân theo các bước tiến hành hợp pháp, các thủ tục phù hợp để giữ nguyên được các chứng cứ phục vụ cho điều tra.

Nên thuê đội ngũ chuyên nghiệp có đủ năng lực và kinh nghiệm để có thể phân tích và điều tra chính xác .

Các bước điều tra xâm nhập

- Nhận thức (Awareness)

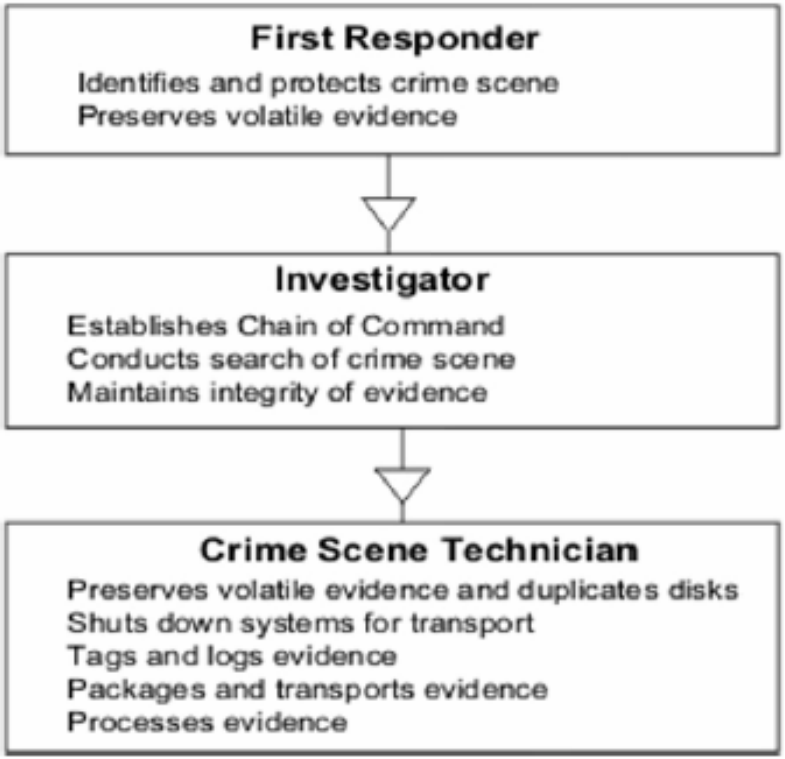
Việc nhận thức về an ninh mạng trong mỗi người dùng là rất quan trọng vì thông thường người dùng là người phát hiện ra các vấn đề xuất hiện trong hệ thống trước nhất.

Nên thành lập 1 **đội phản ứng nhanh** để có thể xử lý kịp thời: xác định được việc gì xảy ra, khôi phục tạm thời các hoạt động chính, cô lập và giữ nguyên hiện trường phục vụ cho điều tra.

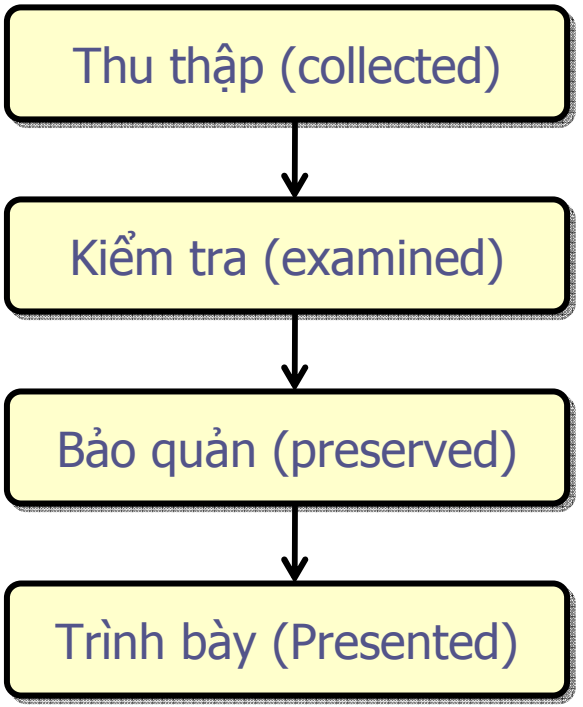
Người dùng phải có nhận thức:
• Thông báo với người quản lý những sự cố hay sự kiện đặc biệt xảy ra.
• Trình bày lại những gì mà mình quan sát và ghi nhận được về sự kiện trước, trong và sau khi diễn ra.

Các bước điều tra xâm nhập

- Phân biệt vai trò của những người điều tra



Các vai trò trong điều tra



4 thành phần chính trong điều tra

Các bước điều tra xâm nhập

- Chuỗi hành trình (chain of custody)

Là lịch sử về quãng đời của chứng cứ : ai điều khiển và khi nào thì thực hiện nó.

Log file luôn được sử dụng vì nó ghi nhận lại tất cả "Ai" làm việc gì và "khi nào" làm việc đó trong hệ thống.

Log file luôn phải được cài đặt trong hệ thống và lưu trữ cẩn thận.

Các bước điều tra xâm nhập

- Thu thập và bảo quản chứng cứ

• Có thể thu thập các chứng cứ thông qua log file của hệ điều hành, của ứng dụng.
• Nên copy lại chứng cứ bằng các phần mềm chuyên dụng như copy đĩa cứng theo từng bit.
• Một số các công cụ hỗ trợ: Safeback, Encase, ProDiscover

• Khi thu thập chứng cứ, không được phá hỏng hay làm thay đổi chứng cứ như: ghi đè lên file cấu hình, khôi phục lại các file đã bị xóa, shutdown hệ thống, format lại ổ cứng, …
• Không cho các nhân viên can thiệp hay làm xáo trộn chứng cứ.
• Nếu được, để khôi phục tạm thời lại hoạt động, nên thay thế bằng 1 hệ thống khác (Server, WebServer, Router khác, …) để giữ nguyên chứng cứ cho điều tra.