HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC
AN TOÀN MẠNG

CHƯƠNG 1 – GIỚI THIỆU AN TOÀN MẠNG

Giảng viên: PGS.TS. Hoàng Xuân Dậu

E-mail: dauhx@ptit.edu.vn

Khoa: An toàn thông tin

TÀI LIỆU THAM KHẢO

1. Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg. Network Security: The Complete Reference, McGraw-Hill Osborne Media, 1st edition, 2003.
2. Mark Rhodes-Ousley. Information Security: The Complete Reference, McGraw-Hill Osborne Media, 2nd edition, 2013.
3. William Stallings. Cryptography and Network Security Principles And Practice, 7th edition, Pearson Education Limited, 2017.
4. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security, 7th edition, Cengage Learning, 2021.
5. Michael T. Simpson, Nicholas Antill. Hands-On Ethical Hacking and Network Defense, 3rd edition, Cengage Learning, 2016.

ĐÁNH GIÁ MÔN HỌC

- Các điểm thành phần:
  - Chuyên cần: 10%
  - Kiểm tra: 10%
  - Bài tập/thảo luận: 30%
  - Thi cuối kỳ: 50%

NỘI DUNG MÔN HỌC

1. Giới thiệu về an toàn mạng
2. Các nguy cơ và lỗ hổng trong bảo mật mạng
3. Các kỹ thuật tấn công mạng
4. Các giải pháp phòng ngừa và ngăn chặn tấn công.

NỘI DUNG CHƯƠNG 1

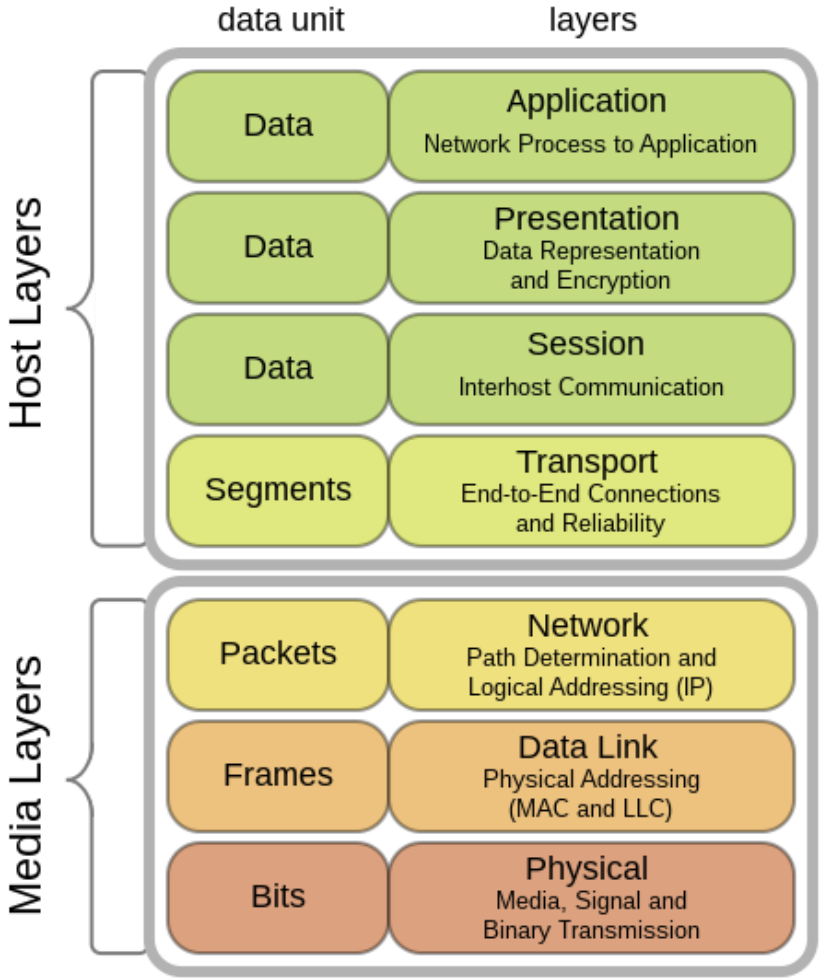
1. Ôn tập về mô hình OSI, bộ giao thức TCP/IP
2. Các yêu cầu và định hướng đảm bảo an toàn mạng
3. Phân tích rủi ro và các mô hình phòng thủ
4. Các thực tế tốt nhất về phòng thủ mạng
5. Tổ chức, quản lý bảo mật.

1.1 Ôn tập về OSI và TCP/IP

- Mô hình OSI
  - Các tầng của OSI
- Bộ giao thức TCP/IP
- Các giao thức thông dụng

Mô hình OSI

- OSI (Open Systems Interconnection Reference Model) là mô hình tham chiếu cho kết nối các hệ thống mở do tổ chức ISO và IUT-T khởi xướng;
  - Còn được gọi là mô hình 7 tầng.
  - Các tầng: Physical (Vật lý), Data Link (Liên kết dữ liệu), Network (Mạng), Transport (Giao vận), Session (Phiên), Presentation (Trình diễn), Application (Ứng dụng).



Mô hình OSI – 1. Tầng Vật lý

- Tầng vật lý định nghĩa tất cả các đặc tả về điện và vật lý cho các thiết bị;
- Chức năng và dịch vụ căn bản được thực hiện bởi tầng vật lý bao gồm:
  - Thiết lập hoặc ngắt mạch kết nối điện với một môi trường truyền dẫn phương tiện truyền thông;
  - Tham gia vào quy trình mà trong đó các tài nguyên truyền thông được chia sẻ hiệu quả giữa nhiều người dùng, như giải quyết tranh chấp tài nguyên và điều khiển lưu lượng;
  - Điều chế (modulation), hoặc biến đổi giữa biểu diễn dữ liệu số (digital data) của các thiết bị người dùng và các tín hiệu tương ứng được truyền qua kênh truyền thông.

Mô hình OSI – 2. Tầng liên kết dữ liệu

- Tầng liên kết dữ liệu cung cấp các phương tiện có tính chức năng và quy trình để truyền dữ liệu giữa các thực thể mạng;
  - Truy cập đường truyền, đưa dữ liệu vào mạng
  - Phát hiện và có thể sửa chữa các lỗi trong tầng vật lý nếu có.
- Sử dụng địa chỉ vật lý như MAC (Media Access Controller), LLC (Logical Link Control);
- Tầng liên kết dữ liệu chính là nơi các thiết bị chuyển mạch (switches) hoạt động;
  - Kết nối chỉ được cung cấp giữa các nút mạng được nối với nhau trong nội bộ mạng.

Mô hình OSI – 3. Tầng mạng

- Tầng mạng cung cấp các chức năng và quy trình cho việc truyền các gói tin có độ dài đa dạng, từ một nguồn tới một đích, thông qua một hoặc nhiều mạng, trong khi vẫn duy trì chất lượng dịch vụ (quality of service) mà tầng giao vận yêu cầu;
  - Tầng mạng thực hiện chức năng định tuyến;
  - Các thiết bị định tuyến (router) hoạt động tại tầng này - gửi dữ liệu ra khắp mạng mở rộng, làm cho liên mạng trở nên khả thi;
  - Sử dụng địa chỉ logic (VD địa chỉ IP).

Mô hình OSI – 4. Tầng giao vận

- Tầng giao vận cung cấp dịch vụ chuyên dụng chuyển dữ liệu giữa người dùng tại các thiết bị đầu cuối;
  - Các tầng trên không phải quan tâm đến việc cung cấp dịch vụ truyền dữ liệu đáng tin cậy và hiệu quả;
  - Tầng giao vận kiểm soát độ tin cậy của một kết nối được cho trước.

Mô hình OSI – 5. Tầng phiên

- Tầng phiên kiểm soát các (phiên) hội thoại giữa các máy tính:
  - Thiết lập, quản lý và kết thúc các kết nối giữa trình ứng dụng cục bộ và trình ứng dụng ở xa
  - Hỗ trợ hoạt động song công (duplex) hoặc bán song công (half-duplex) hoặc đơn công (simplex);
  - Thiết lập các quy trình đánh dấu điểm hoàn thành (checkpointing) - giúp việc phục hồi truyền thông nhanh hơn khi có lỗi xảy ra, vì điểm đã hoàn thành đã được đánh dấu - trì hoãn (adjournment), kết thúc (termination) và khởi động lại (restart).

Mô hình OSI – 6. Tầng trình diễn

- Tầng trình diễn là trung gian chuyển đổi định dạng dữ liệu giữa tầng ứng dụng và tầng phiên. Các chức năng cụ thể:
  - Dịch các mã ký tự từ ASCII sang EBCDIC;
  - Chuyển đổi dữ liệu, ví dụ từ số interger sang số dấu phảy động;
  - Nén dữ liệu để giảm lượng dữ liệu truyền trên mạng;
  - Mã hoá và giải mã dữ liệu để đảm bảo sự bảo mật trên mạng.

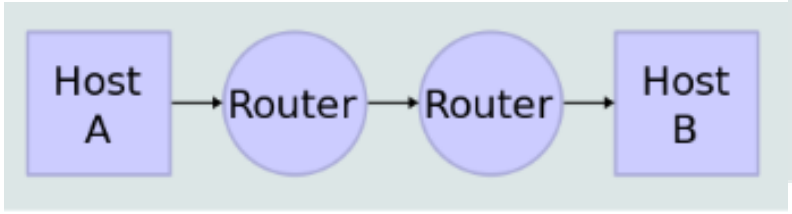
Mô hình OSI – 7. Tầng ứng dụng

- Tầng ứng dụng cung cấp phương tiện cho người dùng truy nhập các thông tin và dữ liệu trên mạng thông qua chương trình ứng dụng;
  - Tầng này là giao diện chính để người dùng tương tác với chương trình ứng dụng và qua đó với mạng;
  - Một số ví dụ về các ứng dụng trong tầng này bao gồm HTTP, Telnet, FTP, SMTP, IMAP.

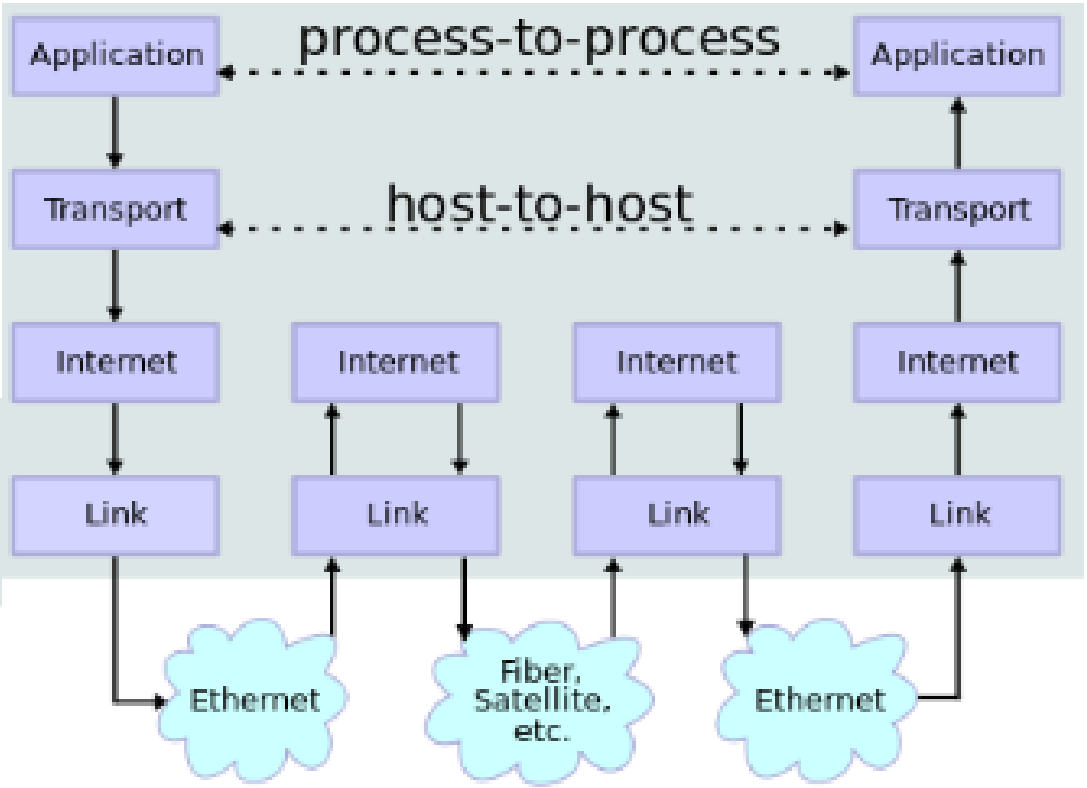
Bộ giao thức TCP/IP

- Bộ giao thức TCP/IP (TCP/IP protocol suite), hay còn gọi là bộ giao thức Internet là:
  - Một mô hình khái niệm và
  - Một tập hợp các giao thức truyền thông dùng trong mạng Internet và các hệ thống mạng máy tính tương tự.
- Tên gọi TCP/IP đến từ hai giao thức nền tảng của bộ giao thức là TCP (Transmission Control Protocol) và IP (Internet Protocol).

TCP/IP: mô hình mạng và luồng dữ liệu

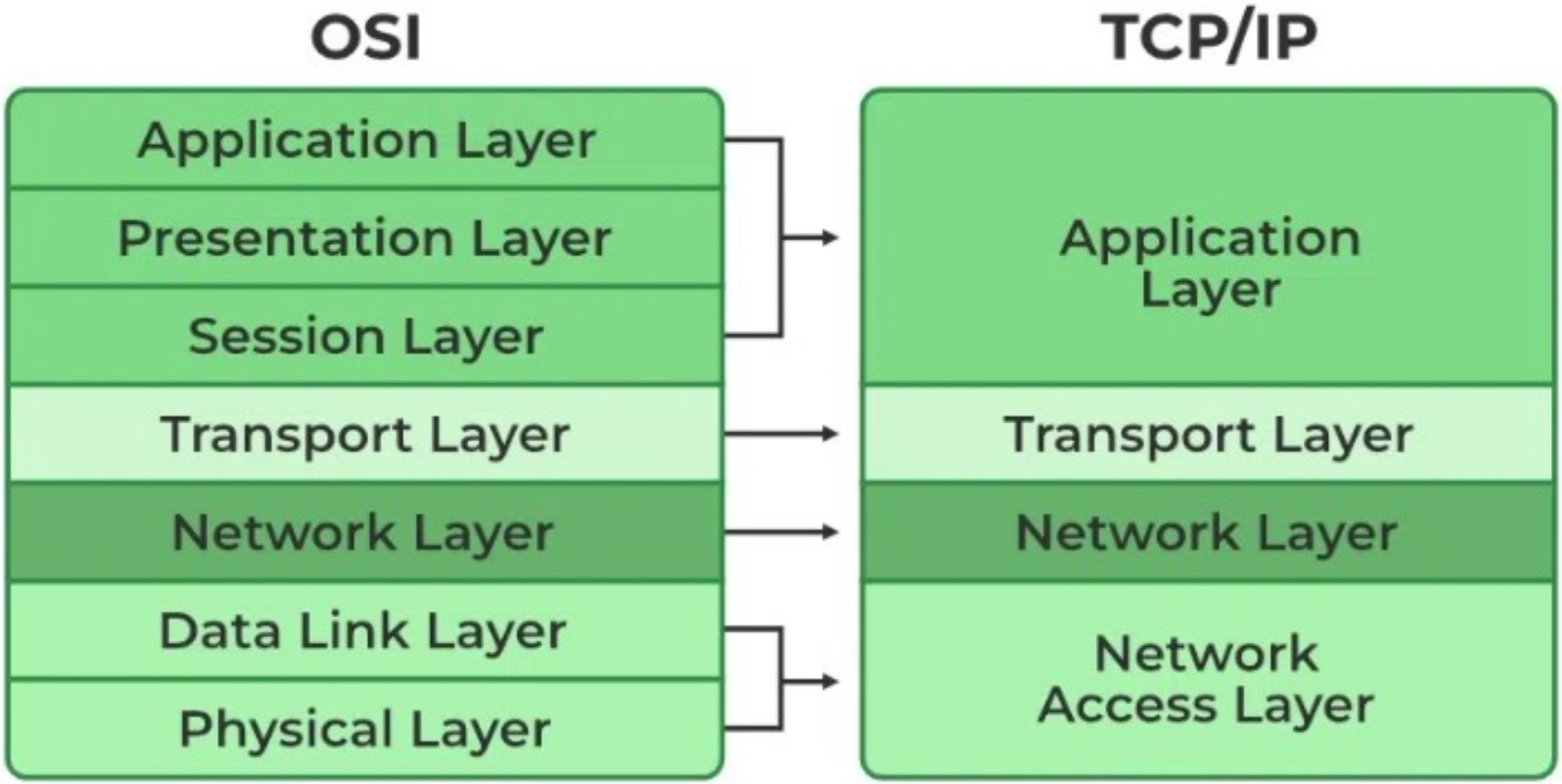


Mô hình mạng

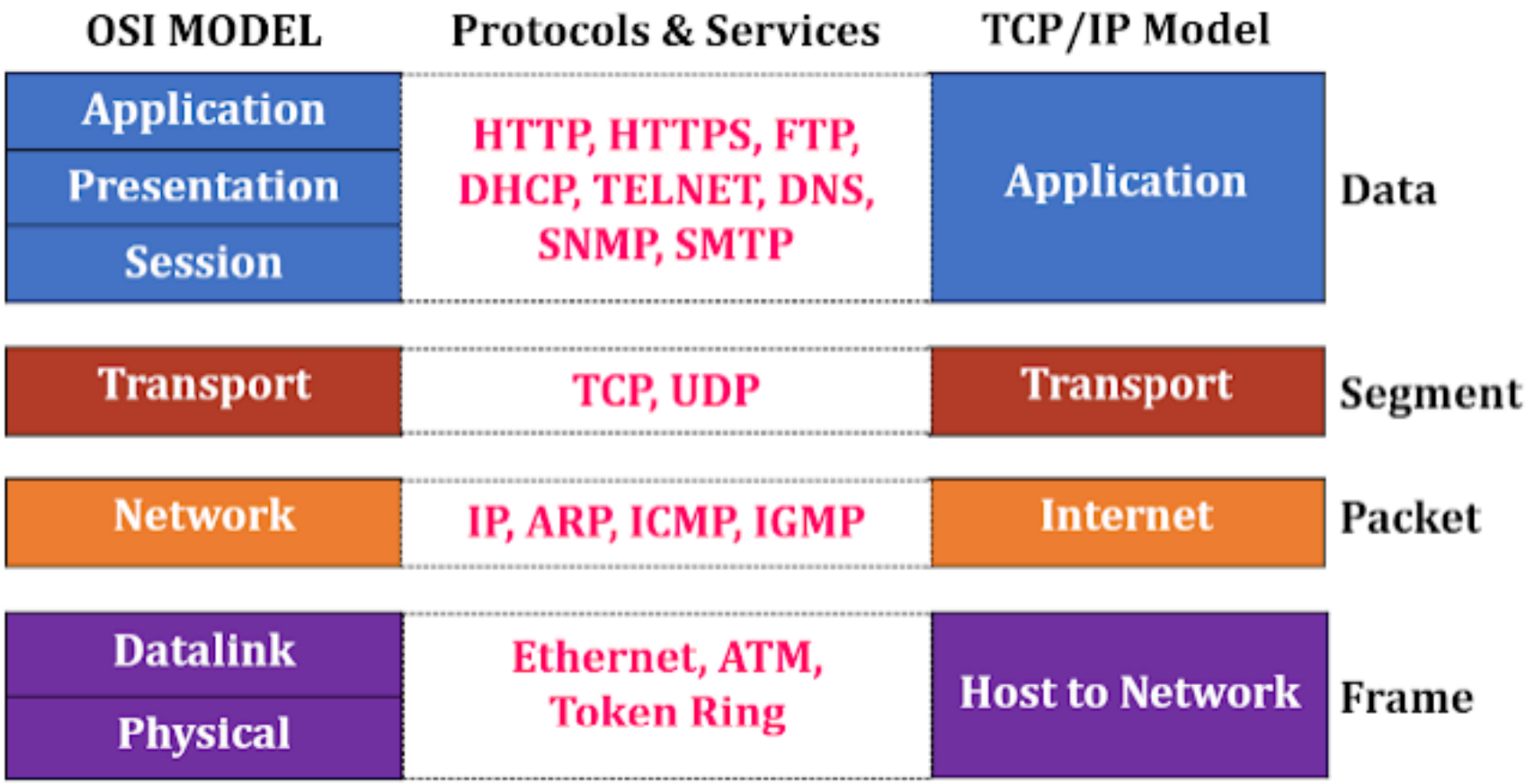


Luồng dữ liệu

So sánh giữa mô hình OSI và TCP/IP



So sánh giữa mô hình OSI và TCP/IP



Bộ giao thức TCP/IP – 1. Tầng liên kết dữ liệu

- Tầng liên kết dữ liệu (Link, Data Link, Network Access) có chức năng chuyển các gói tin từ tầng mạng đến các máy (host) khác;
  - Thường được thực hiện bởi các trình điều khiển thiết bị của các card giao tiếp mạng, hoặc bởi firmware của các chipset chuyên dụng;
  - Các giao thức thông dụng gồm:
    - Ethernet (mạng cục bộ), IEEE 802.11 (mạng WLAN)
    - PPP (cho modem quay số truy cập Internet qua mạng điện thoại)
    - PPPoE (cho modem truy cập Internet qua mạng bang rộng, như ADSL, cáp)...

Bộ giao thức TCP/IP – Tầng mạng

- Tầng mạng có nhiệm vụ chính là dẫn đường/định tuyến các gói tin từ mạng nguồn đến mạng đích;
- Các giao thức của tầng mạng:
  - IP là giao thức định tuyến chính thực hiện nhiệm vụ cơ bản dẫn đường dữ liệu từ nguồn tới đích;
    - IP có thể chuyển dữ liệu theo yêu cầu của nhiều giao thức tầng trên khác nhau.
  - ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol).

Bộ giao thức TCP/IP – Tầng giao vận

- Tầng giao vận có nhiệm vụ kết hợp các khả năng truyền thông điệp trực tiếp (end-to-end) không phụ thuộc vào mạng tầng dưới, kèm theo kiểm soát lỗi (error control), phân mảnh (fragmentation) và điều khiển lưu lượng;
- Việc truyền thông điệp trực tiếp hay kết nối các ứng dụng tại tầng giao vận có thể gồm:
  - Hướng kết nối (connection-oriented), như giao thức TCP
  - Không kết nối (connectionless), như giao thức UDP.
- Các giao thức:
  - TCP, UDP
  - SCTP (Stream Control Transmission Protocol).

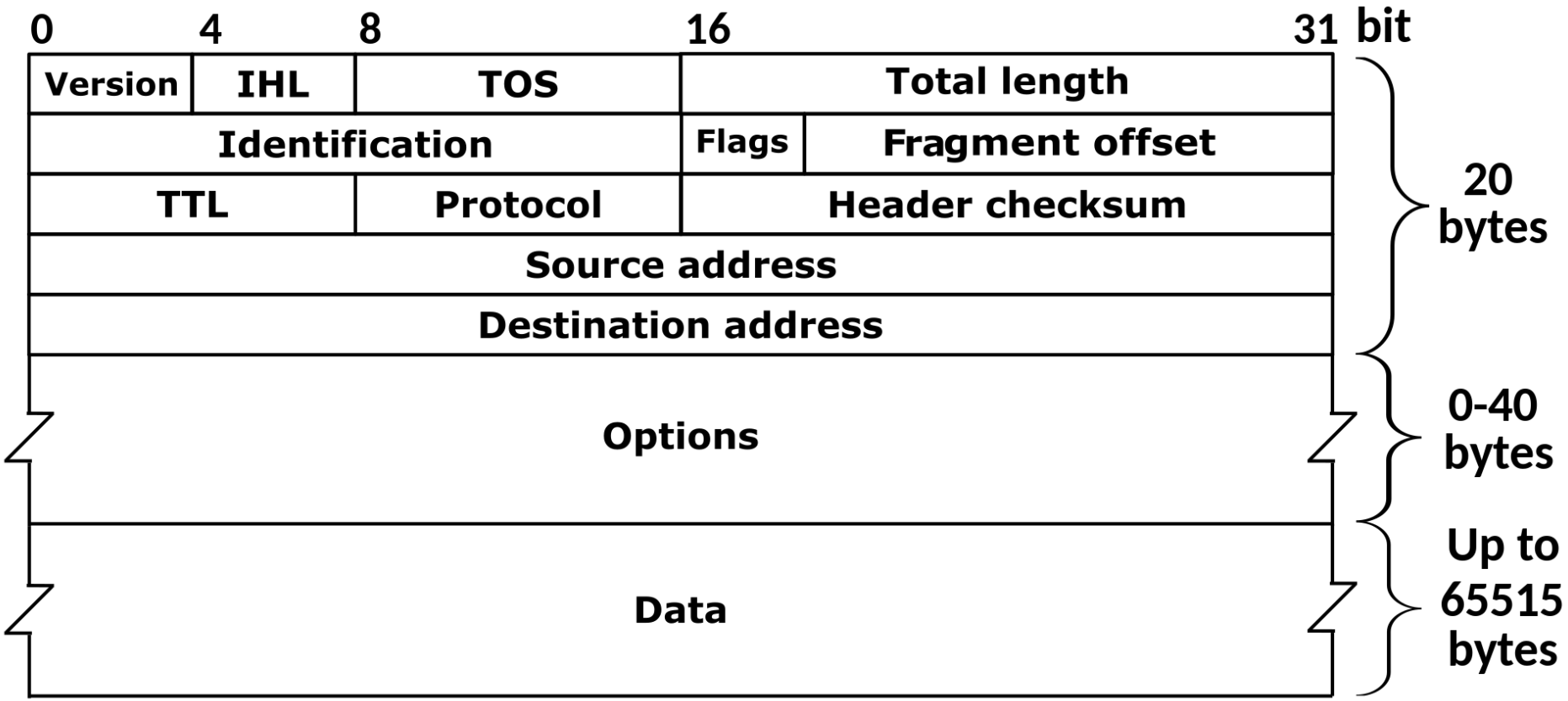
Bộ giao thức TCP/IP – Tầng ứng dụng

- Tầng ứng dụng bao gồm các giao thức sử dụng bởi các ứng dụng cung cấp dịch vụ cho người dùng, hoặc trao đổi dữ liệu qua mạng thông qua các tầng phía dưới;
- Các giao thức gồm:
  - HTTP, HTTPS, FTP
  - SMTP, POP, IMAP
  - DHCP, DNS
  - Telnet, SSH, Remote desktop...

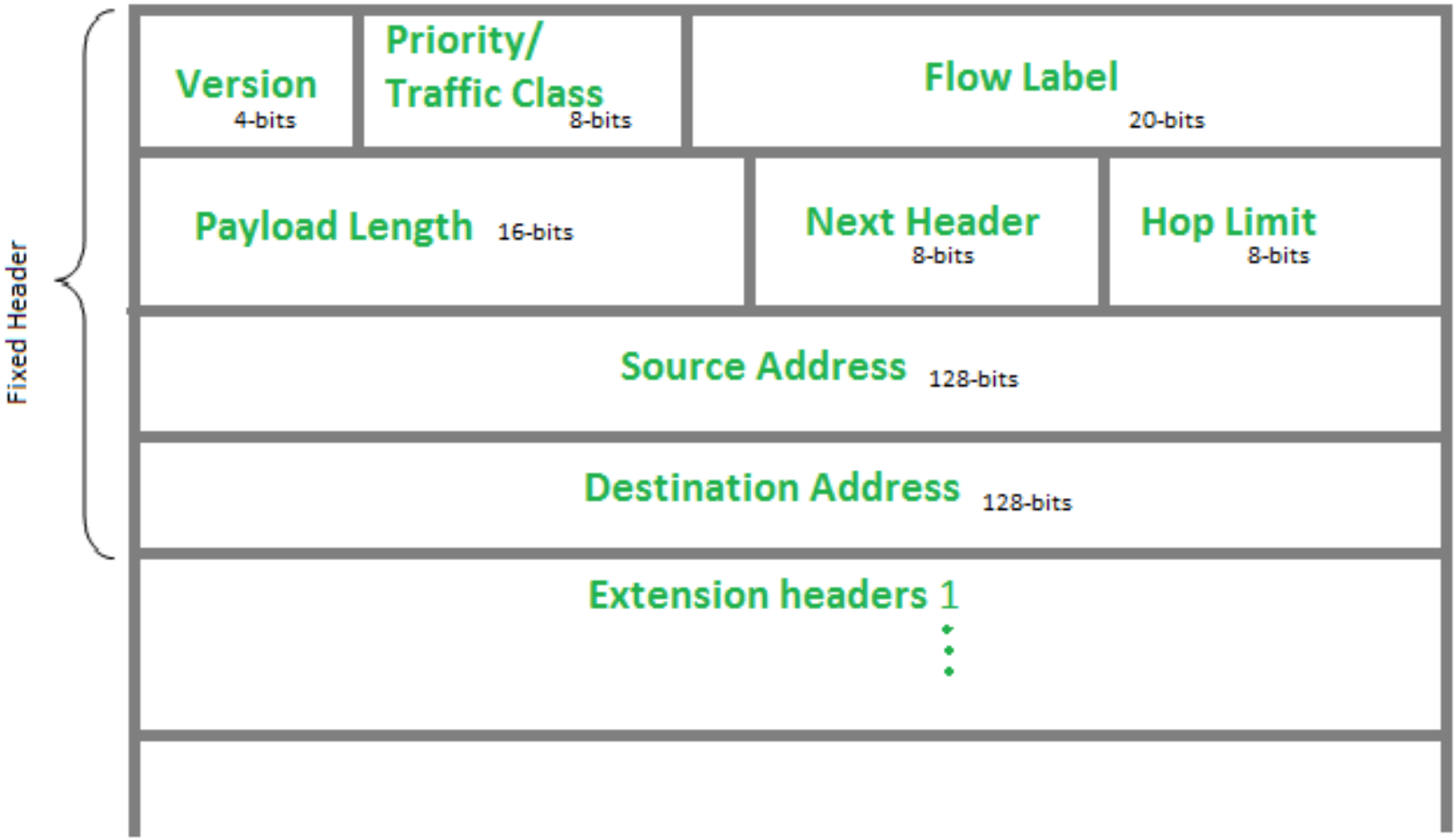
Các giao thức TCP/IP thông dụng

- Tìm hiểu về kiến trúc, hoạt động, định dạng gói/frame/message của các giao thức:
  - IP, ICMP, ARP, NAT
  - TCP, UDP
  - HTTP, HTTPS
  - FTP
  - SMTP
  - Telnet, SSH
  - DHCP
  - DNS.

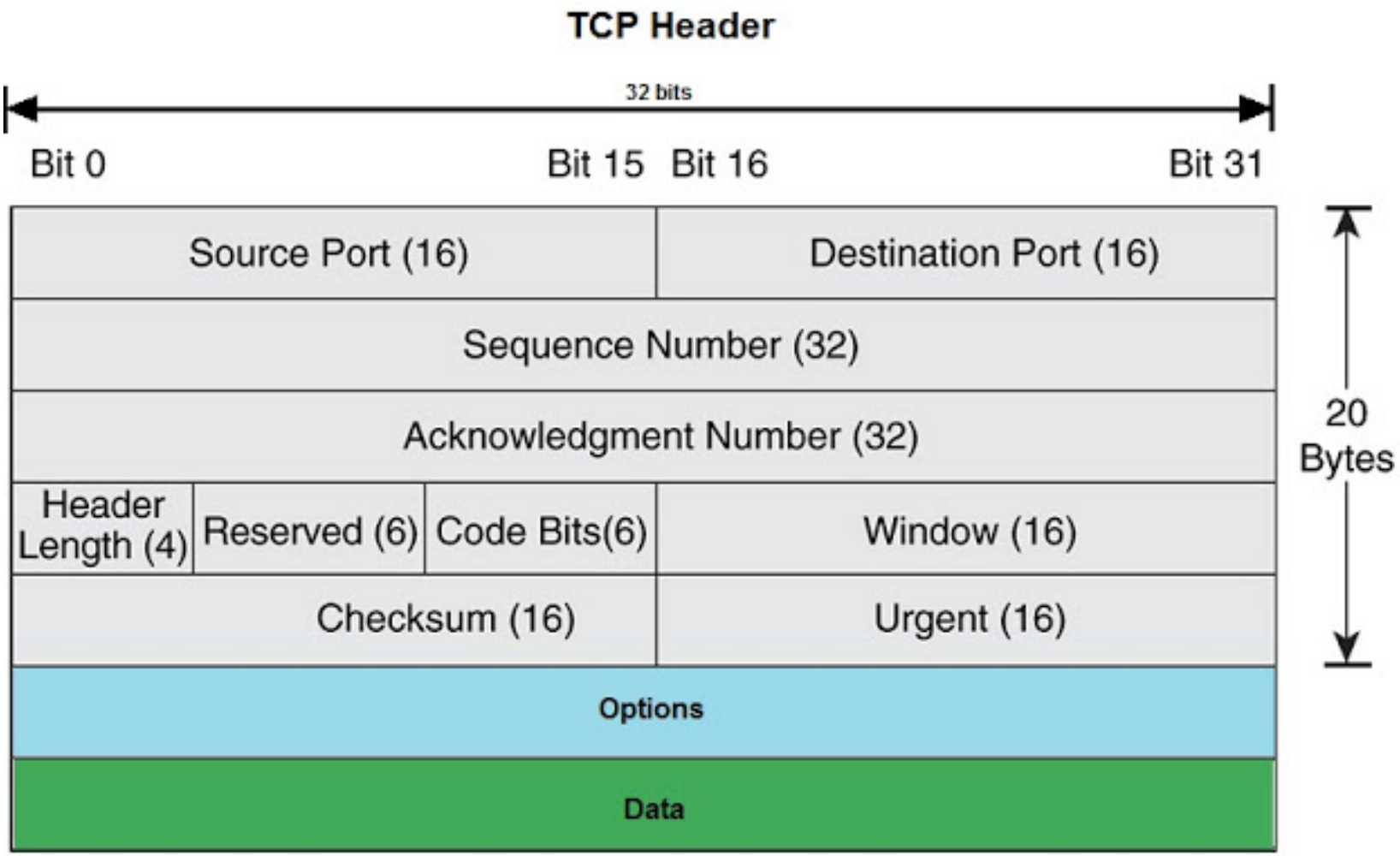
IP v4 packet format



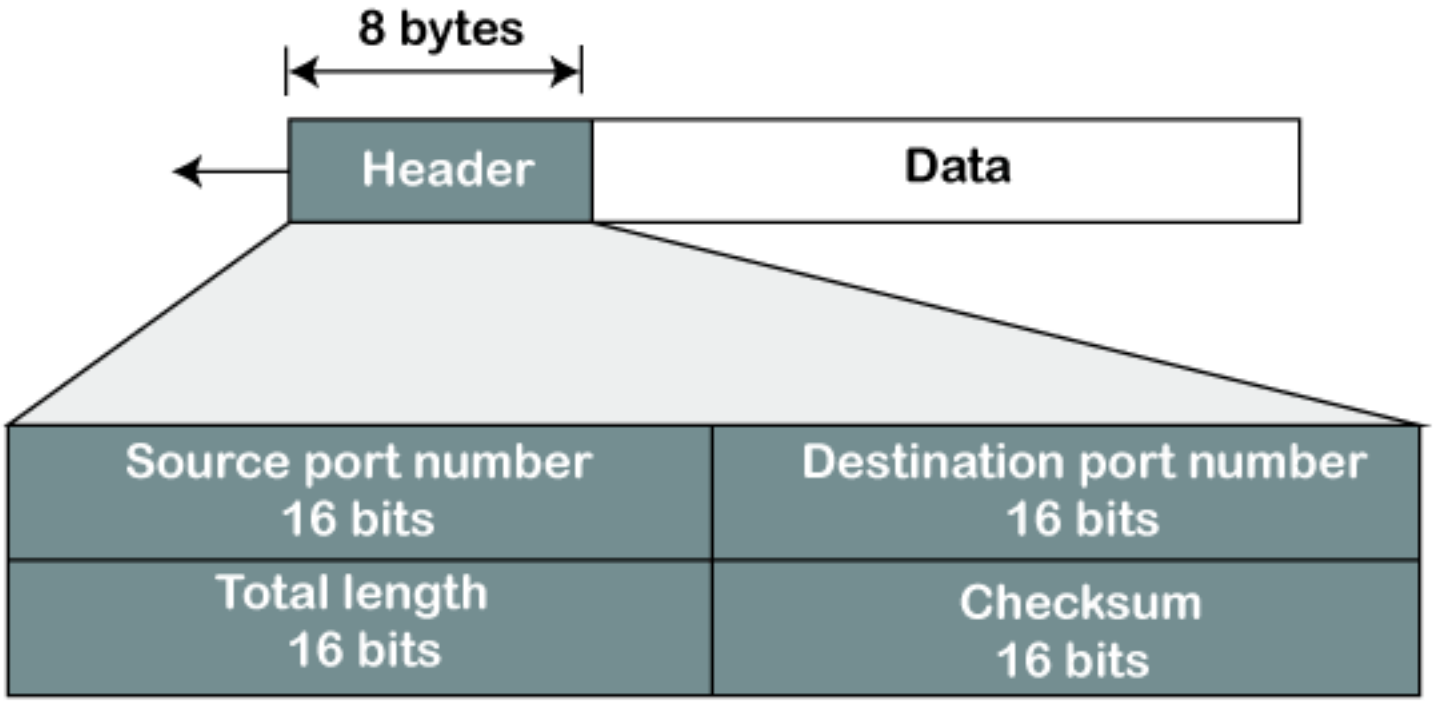
IP v6 packet format



TCP packet format



UDP message format



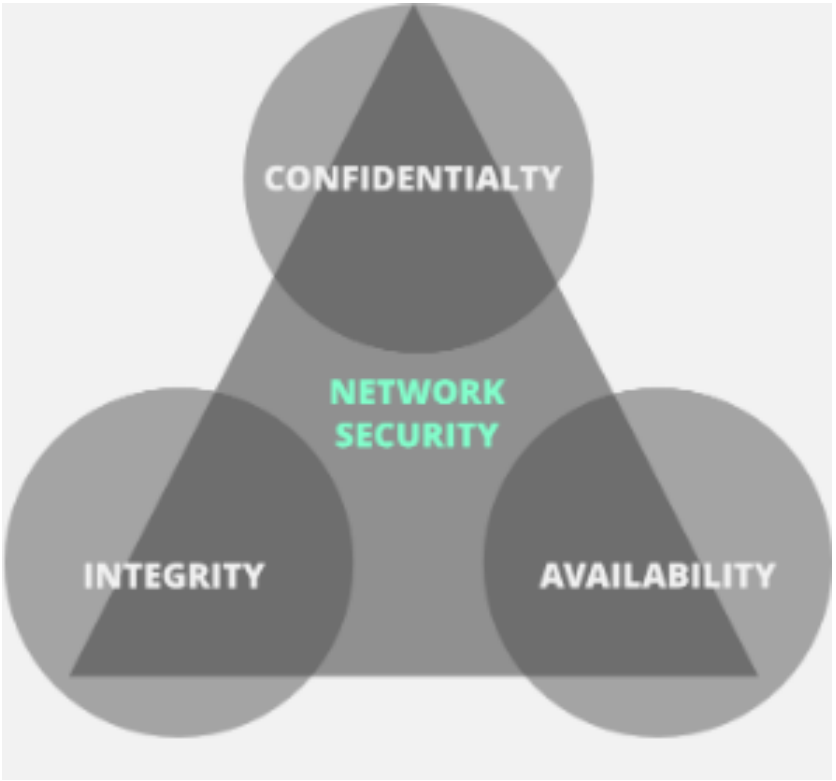
1.2 Các yêu cầu và định hướng đảm bảo ATM

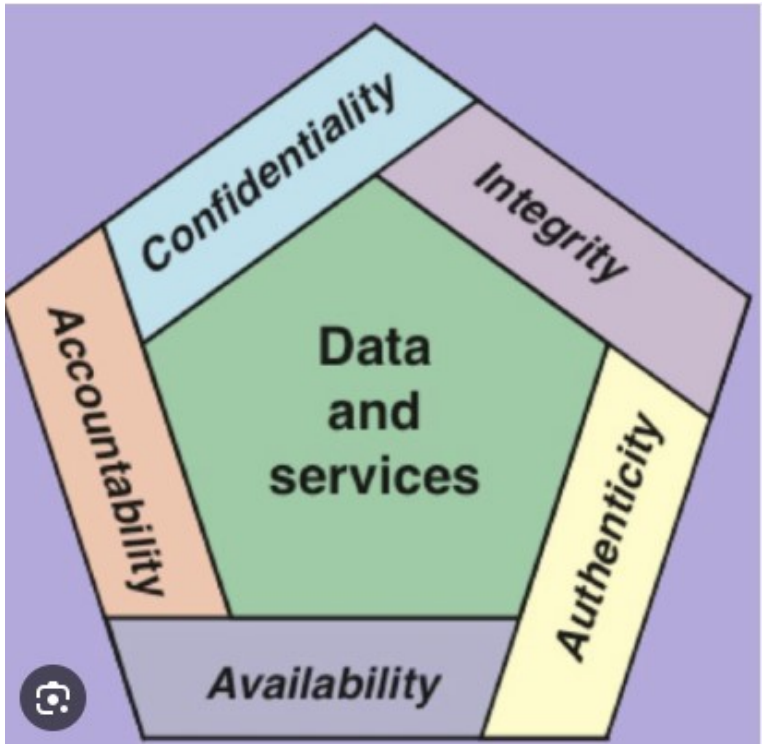
- Các yêu cầu đảm bảo an toàn mạng
- Các định hướng đảm bảo an toàn mạng

Các yêu cầu đảm bảo an toàn mạng

- An toàn mạng (Network security) liên quan đến bảo vệ dữ liệu, phần cứng, phần mềm trên mạng;
- Các yêu cầu cơ bản đảm bảo an toàn mạng gồm:
  - Tính bí mật (Confidentiality)
  - Tính toàn vẹn (Integrity)
  - Tính sẵn dùng (Availability)
  - Tính xác thực (Authenticity)
  - Tính truy vết được (Accountability).

Các yêu cầu đảm bảo an toàn mạng





Các yêu cầu đảm bảo an toàn mạng

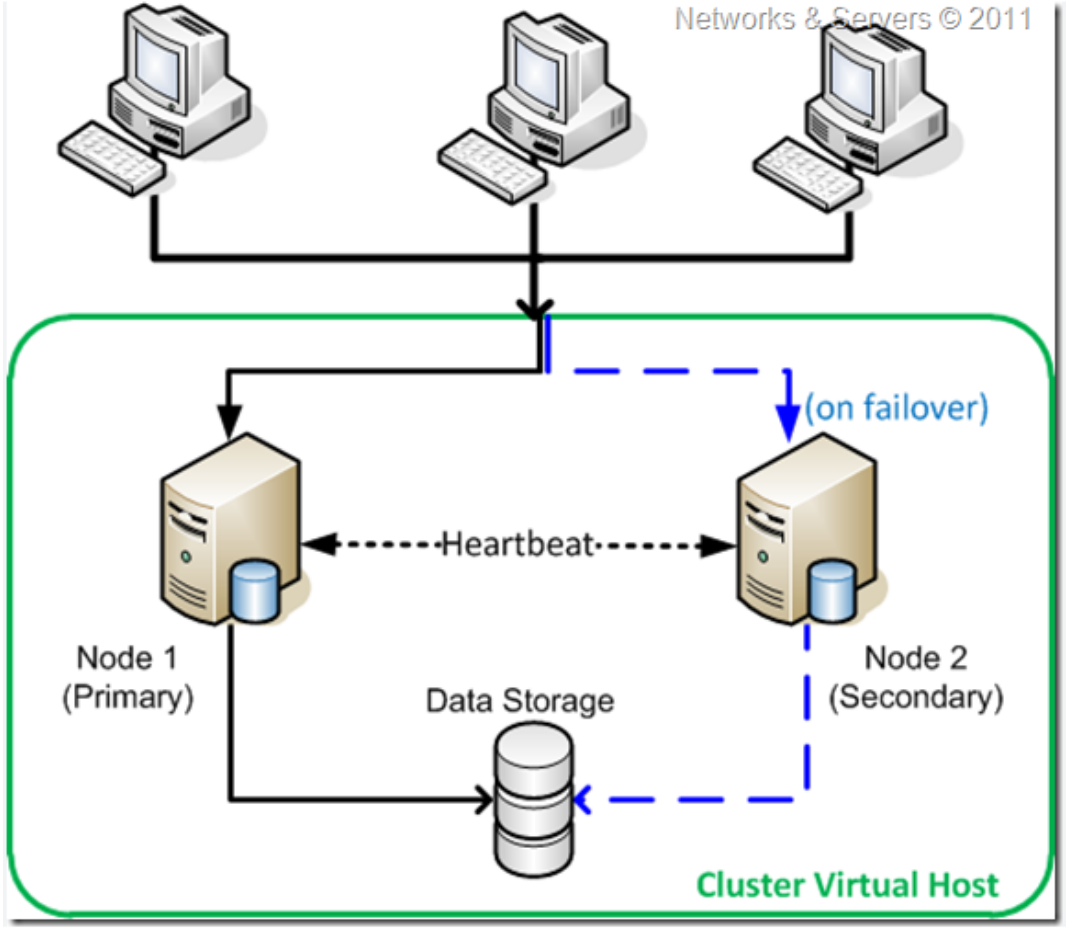
- Tính bí mật đảm bảo rằng dữ liệu / hệ thống / mạng chỉ có thể được truy cập bởi người dùng có thẩm quyền;
  - Sử dụng các phương pháp bảo vệ hệ thống về vật lý (tường bao, cửa, giám sát...)
  - Bảo vệ bằng mã hóa dữ liệu
  - Bảo vệ bằng các hệ thống lọc, xác thực (tường lửa, IDS/IPS...)

Các yêu cầu đảm bảo an toàn mạng

- Tính toàn vẹn đảm bảo rằng dữ liệu / hệ thống / mạng chỉ có thể được chỉnh sửa bởi người dùng có thẩm quyền.
  - Sử dụng hàm băm
  - Sử dụng chữ ký số
  - Sử dụng các ràng buộc.

Các yêu cầu đảm bảo an toàn mạng

- Tính sẵn dùng đảm bảo rằng dữ liệu / hệ thống / mạng luôn sẵn sàng cho người sử dụng hợp pháp bất cứ khi nào họ có nhu cầu;
  - Sử dụng máy chủ dự phòng, các chuỗi cân bằng tải.



Các yêu cầu đảm bảo an toàn mạng

- Tính xác thực đảm bảo rằng dữ liệu/ thông điệp / hệ thống / mạng có nguồn gốc tin cậy, có thể xác minh được;
- Tính truy vết được, hoặc giải trình được đảm bảo hệ thống / mạng cần quản lý lưu trữ các thông tin hoạt động để có thể điều tra, truy vết, qui trách nhiệm khi có sự cố.

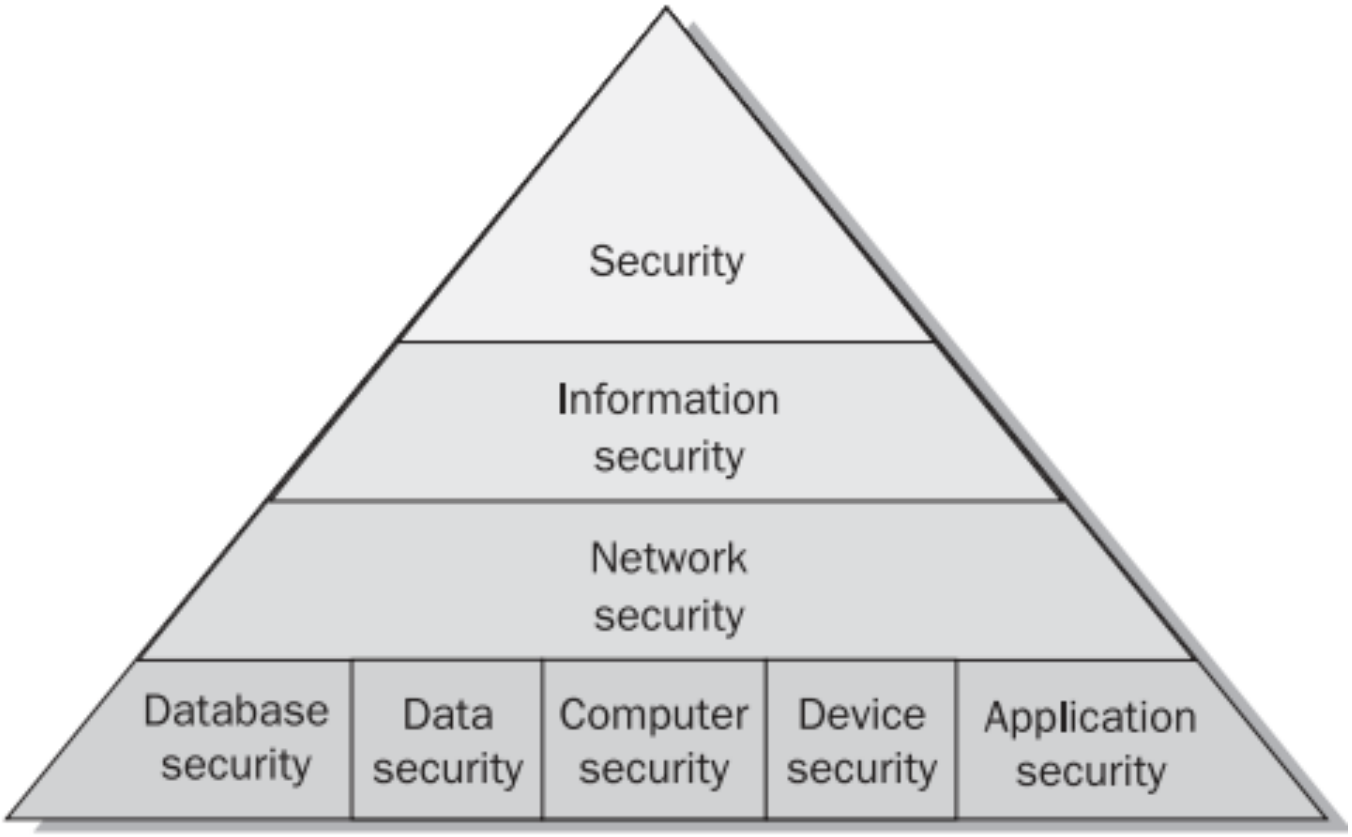
Các yêu cầu đảm bảo an toàn mạng

- Các yêu cầu bổ sung đảm bảo an toàn mạng gồm:
  - Accuracy
  - Awareness
  - Non-repudiation
  - Completeness
  - Response
  - Consistency
  - Utility.

Các định hướng đảm bảo an toàn mạng

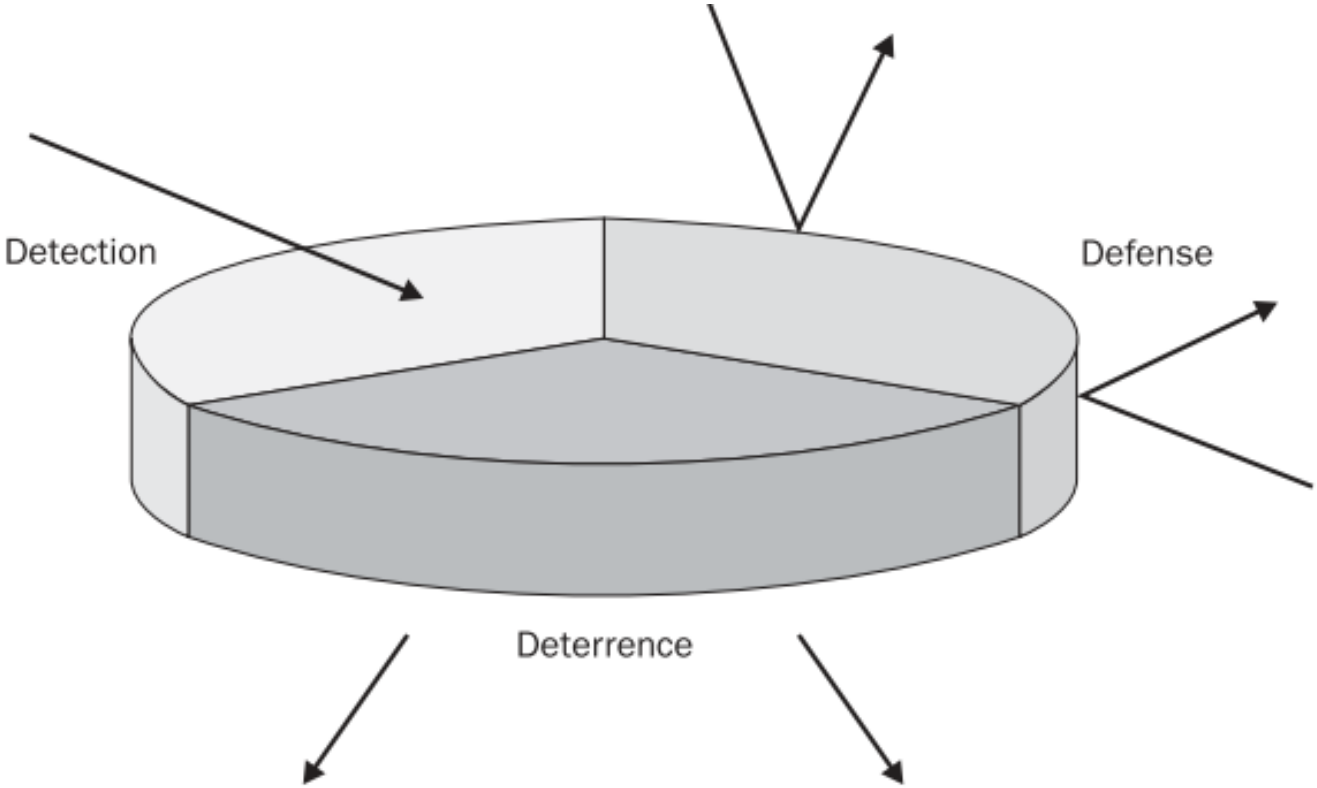
- Các lớp đảm bảo an toàn và An toàn mạng
- Mô hình bảo mật 3 chữ D
- 5 bước cho nâng cao an toàn
- Chiến lược và chiến thuật an toàn
- Liên kết yếu nhất
- Không có “viên đạn bạc”
- Qui trình nghiệp vụ với các kiểm soát kỹ thuật

Các lớp đảm bảo an toàn và An toàn mạng



Mô hình bảo mật 3 chữ D

- Sử dụng mô hình bảo mật 3 chữ D:
  - Defense (Phòng thủ)
  - Deterrence (Răn đe)
  - Detection (Phát hiện)



Mô hình 3D - Defense

- Defense (Phòng thủ) là phương thức đầu tiên của chiến lược an ninh và cần đi trước bất kỳ nỗ lực bảo vệ nào khác;
- Các biện pháp phòng thủ làm giảm khả năng xâm nhập thành công các tài sản có giá trị, do đó làm giảm rủi ro và có khả năng tiết kiệm chi phí cho các sự cố không tránh được;
- Tuy nhiên, phòng thủ chỉ nên là một phần của chiến lược an ninh hoàn chỉnh, không nên là thành phần duy nhất;
  - Nhiều công ty chỉ dựa vào tường lửa để bảo vệ tài sản thông tin của họ và những công ty này dễ bị tổn thương vì họ đang bỏ qua những điểm yếu có thể được bảo vệ bởi các phương thức bảo mật khác.

Mô hình 3D - Deterrence

- Deterrence (Răn đe) là phương thức bảo mật thứ hai sau Phòng thủ;
  - Ý tưởng của răn đe được chỉ rõ trong luật hình sự: các hành vi phạm pháp đều là bất hợp pháp và sẽ bị trừng phạt;
- Răn đe thường được coi là một phương pháp hiệu quả để giảm tần suất xâm phạm bảo mật và do đó giảm tổng thiệt hại do sự cố bảo mật;
  - Nhiều công ty đưa ra các Nội quy với qui định xử phạt nghiêm khắc với các hành vi vi phạm của nhân viên, như phát tiền, cảnh cáo hoặc sa thải.

Mô hình 3D – Detection

- Detection (Phát hiện) là phương thức bảo mật thứ ba, sau các phương thức Phòng thủ và Răn đe;
- Nếu chỉ dựa vào phòng thủ hoặc răn đe, chiến lược an ninh thường bỏ qua quá trình phát hiện tội phạm đang diễn ra.
  - Trên thực tế, nhiều người coi hệ thống báo động là đủ để cảnh báo những người có liên quan về hành vi cố gắng vi phạm vành đai an ninh (chẳng hạn như sử dụng chuông báo động cho nhà hoặc ô tô) và họ hiếm khi thuê nhân viên thực thi an ninh, những người được đào tạo để ứng phó với sự cố, để giám sát các hệ thống báo động này.
- Nếu không được phát hiện đầy đủ, vi phạm bảo mật có thể không được chú ý trong nhiều giờ, nhiều ngày hoặc thậm chí là mãi mãi.

Mô hình 3D – Ví dụ

- Áp dụng mô hình 3D cho bảo vệ 1 ngôi nhà có chứa tài sản lớn (như 1 nhẫn kim cương):
  - Phòng thủ: khóa tất cả cửa sử dụng khóa tốt nhất, chỉ những người có chìa chuẩn mới có thể mở;
  - Răn đe: có thể dùng luật pháp để cảnh báo, hoặc nuôi chó hoặc vật nuôi dữ tợn để trông nhà;
  - Phát hiện: lắp camera giám sát, cảm biến hồng ngoại và các thiết bị công nghệ khác để cảnh báo các nỗ lực xâm nhập.

Vai trò của mỗi phương thức trong mô hình 3D

- Mỗi phương thức trong mô hình bảo mật 3D có độ quan trọng ngang nhau và bổ sung cho nhau:
  - Một chiến lược phòng thủ ngăn chặn kẻ tấn công và giảm sự lạm dụng và tai nạn nội bộ;
  - Chiến lược răn đe không khuyến khích các nỗ lực làm suy yếu các mục tiêu và quy trình kinh doanh, đồng thời giữ cho hiệu quả của công ty tập trung vào các nỗ lực sản xuất;
  - Chiến lược phát hiện cảnh báo những người có trách nhiệm về những vi phạm chính sách.

Vai trò của mỗi phương thức trong mô hình 3D

- Không có nỗ lực bảo mật nào có thể hoàn toàn hiệu quả nếu không có tất cả 3 phương thức.
- Ngược lại, một nỗ lực bảo mật sử dụng cả ba phương thức sẽ mang lại sự bảo vệ mạnh mẽ.

Mô hình 3D – Các biện pháp phòng thủ

- Có thể gồm các thiết bị kiểm soát truy cập, như:
  - tường lửa
  - các danh sách truy cập router
  - các danh sách định tuyến tĩnh
  - các bộ lọc spam và mã độc
  - các kiểm soát thay đổi.
- Vai trò:
  - Cung cấp bảo vệ khỏi các lỗ hổng, lỗi phần mềm, các script tấn công, các vi phạm chính sách, các hư hỏng dữ liệu do tai nạn;
  - Ngăn chặn các hành động không mong muốn trên mạng và đưa các hành động mạng vào các kênh tuân thủ các yêu cầu của đơn vị.

Mô hình 3D – Các biện pháp răn đe

- Có thể gồm các biện pháp:
  - Emails gửi cho nhân viên nhắc nhở về các chính sách bảo mật và việc sử dụng tài nguyên công ty ở mức chấp nhận được;
  - Cung cấp danh sách các trang web nhân viên có thể truy cập từ máy tính của công ty trong giờ làm việc;
  - Các chương trình nâng cao ý thức và giao tiếp cho nhân viên về đạo đức, qui tắc ứng xử, việc sử dụng tài nguyên công ty ở mức chấp nhận được và các chế tài xử phạt nếu không tuân thủ;
  - Các biện pháp khuyến khích nhận viên tuân thủ các nội qui bảo mật, hạn chế việc vi phạm cố ý hoặc vô tình.

Mô hình 3D – Các biện pháp phát hiện

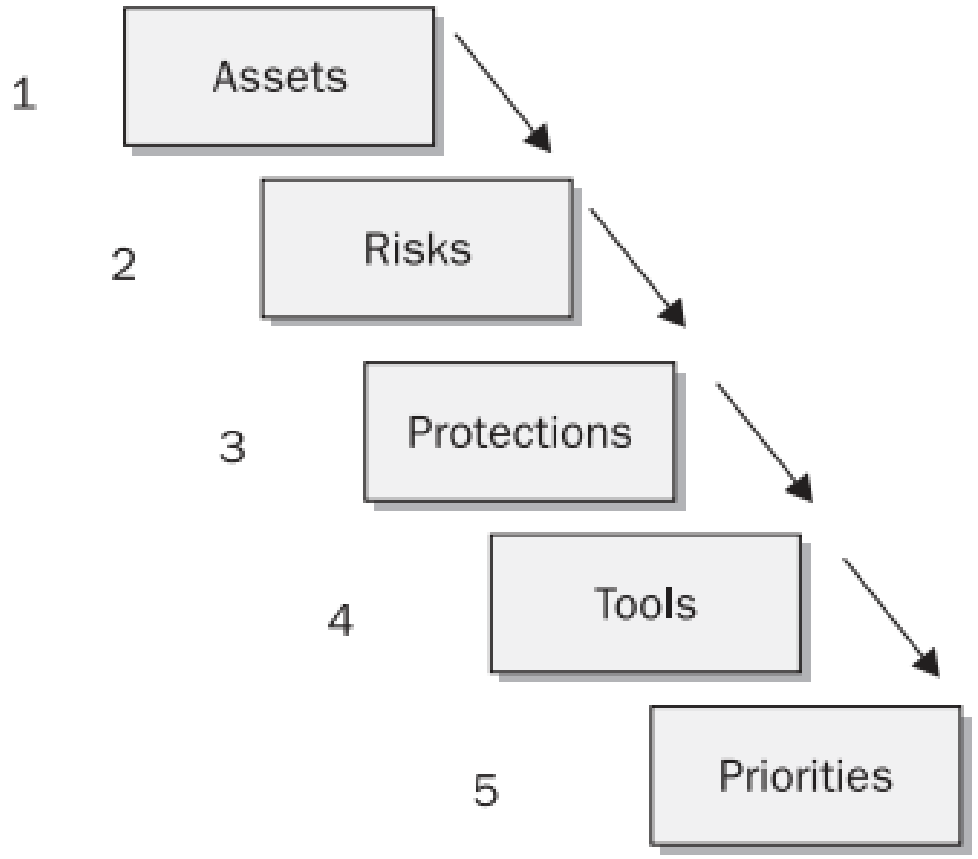
- Có thể gồm các biện pháp:
  - Ghi log các hoạt động trong các hệ thống;
  - Sử dụng HIDS/NIDS
  - Báo cáo tổng hợp được duyệt hàng ngày bởi nhân sự có chuyên môn về nhận dạng các website được thăm, các cuộc tấn công thành công và bị phong tỏa...
  - Trình bày với lãnh đạo quản lý cấp cao về tính hiệu quả của chương trình bảo mật, cũng như nhận dạng các thành công và thất bại.

Mô hình 3D – Lưu ý

- Nếu một đơn vị chỉ áp dụng 1 hoặc 2 trong 3 phương thức của mô hình 3D, hệ thống có thể gặp vấn đề:
  - Nếu chỉ áp dụng Phòng thủ và Phát hiện mà không sử dụng Răn đe, hệ thống mạng có thể bị tổn thương bởi các tấn công nội bộ, lạm dụng bởi các nhân viên không tuân thủ nội quy;
  - Một hệ thống mạng không áp dụng Phát hiện có thể phải đối mặt với tất cả các lỗi của các biện pháp kiểm soát phòng thủ và răn đe, đồng thời người quản lý có thể không bao giờ nhận thức được những lỗi này, điều đó có nghĩa là các hành vi lạm dụng có thể tiếp tục không được kiểm soát;
  - Việc không sử dụng các biện pháp Phòng thủ trên mạng sẽ khiến mạng đó gặp phải bất kỳ mối đe dọa nào có nguồn gốc bên trong hoặc bên ngoài mạng.

5 bước cho nâng cao an toàn

- Assets (Các tài sản)
- Risks (Các rủi ro)
- Protections (Các bảo vệ)
- Tools (Các công cụ)
- Priorities (Các ưu tiên)



5 bước cho nâng cao an toàn - Assets

- Bước Assets (Tài sản) cần trả lời được câu hỏi: Cái gì cần được bảo vệ?
  - Dữ liệu khách hang
  - Máy chủ
  - Hệ thống mạng...

5 bước cho nâng cao an toàn - Risks

- Bước Risks (Các rủi ro) cần giải đáp được câu hỏi các đe dọa, lỗ hổng và rủi ro là gì?
- Sau khi nhận dạng được tài sản cần bảo vệ, tiếp theo cần liệt kê được:
  - Các đe dọa có thể có với tài sản đó
  - Các lỗ hổng tồn tại trong tài sản đó
  - ➔ Các rủi ro là xác suất đe dọa thành hiện thực và chi phí khắc phục.
  - ➔ Sử dụng phân tích rủi ro.

5 bước cho nâng cao an toàn - Protections

- Bước Protections (Bảo vệ) xác định các chính sách, tiến trình và kỹ thuật để cung cấp mức bảo vệ phù hợp cho tài sản trên cơ sở xác định được mức rủi ro với tài sản đó;
- Các biện pháp bảo vệ có thể gồm:
  - Các chính sách, thủ tục, qui trình
  - Các giải pháp kỹ thuật, như tường lửa, thiết bị kiểm soát truy cập, xác thực, mã hóa...
  - Các công cụ giám sát tự động hoặc thủ công.

5 bước cho nâng cao an toàn - Tools

- Bước Tools (Công cụ) cần trả lời câu hỏi: Cái gì sẽ được thực hiện/triển khai để đảm bảo sự bảo vệ đó?
- Bước này tiếp theo Bước Protection để lựa chọn các công cụ cụ thể để thực hiện các yêu cầu đảm bảo an toàn;
- Kết quả của bước này là 1 danh sách các bước thực hiện bảo vệ được thực thi.

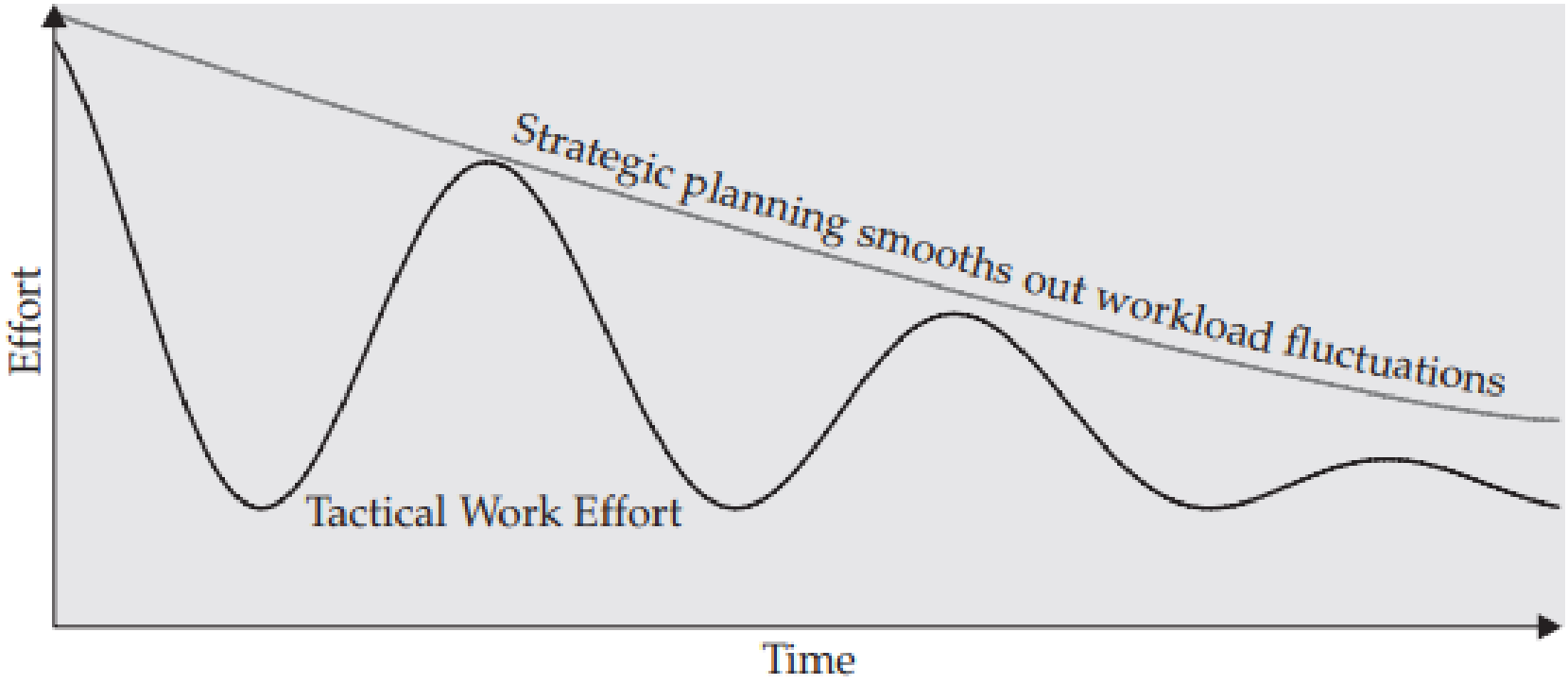
5 bước cho nâng cao an toàn - Priorities

- Bước Priorities (Ưu tiên) xác định thứ tự thực hiện các bước trong "danh sách các bước thực hiện bảo vệ được thực thi" trong bước Tools;
- Khi các công cụ và kỹ thuật để bảo vệ tài sản khỏi các mối đe dọa đã được xác định và tổ chức không có đủ nguồn lực để thực thi ngay toàn bộ thì việc xác định thứ tự thực hiện là cần thiết;
  - Chẳng hạn, thứ tự các việc cần thực hiện để bảo mật một hệ thống web là: đầu tiên cài đặt tường lửa, sau đó tăng cường an toàn cho máy chủ web bằng cấu hình, tiếp theo triển khai các biện pháp mã hóa, bảo mật CSDL...

Chiến lược và chiến thuật bảo mật

- Chiến lược bảo mật (Security strategy) bao gồm các thành phần kiến trúc và chính sách để tạo ra một kế hoạch hoàn chỉnh cho Phòng thủ, Răn đe và Phát hiện;
- Chiến thuật bảo mật (Security tactic) là các hoạt động hàng ngày của các cá nhân và công nghệ được sử dụng để đảm bảo an toàn cho các tài sản;
- Chiến lược thường có tính chủ động (proactive) và chiến thuật thường có tính phản ứng (reactive);
- Chiến lược bảo mật và Chiến thuật bảo mật đều quan trọng và không thể thiếu 1 trong 2.

Chiến lược và chiến thuật bảo mật



Liên kết yếu nhất

- Liên kết yếu nhất (The weakest link) là vị trí, điểm yếu nhất, dễ tổn thương nhất trong hệ thống mạng, thường bị kẻ tấn công khai thác;
- Chẳng hạn với 1 ngôi nhà, kẻ tấn công có thể tìm điểm yếu nhất để đột nhập theo thứ tự:
  - Cửa chính
  - Cửa sổ
  - Các lối ra vào khác
  - Xâm nhập qua mái (cắt mái), tường (khoét tường)...

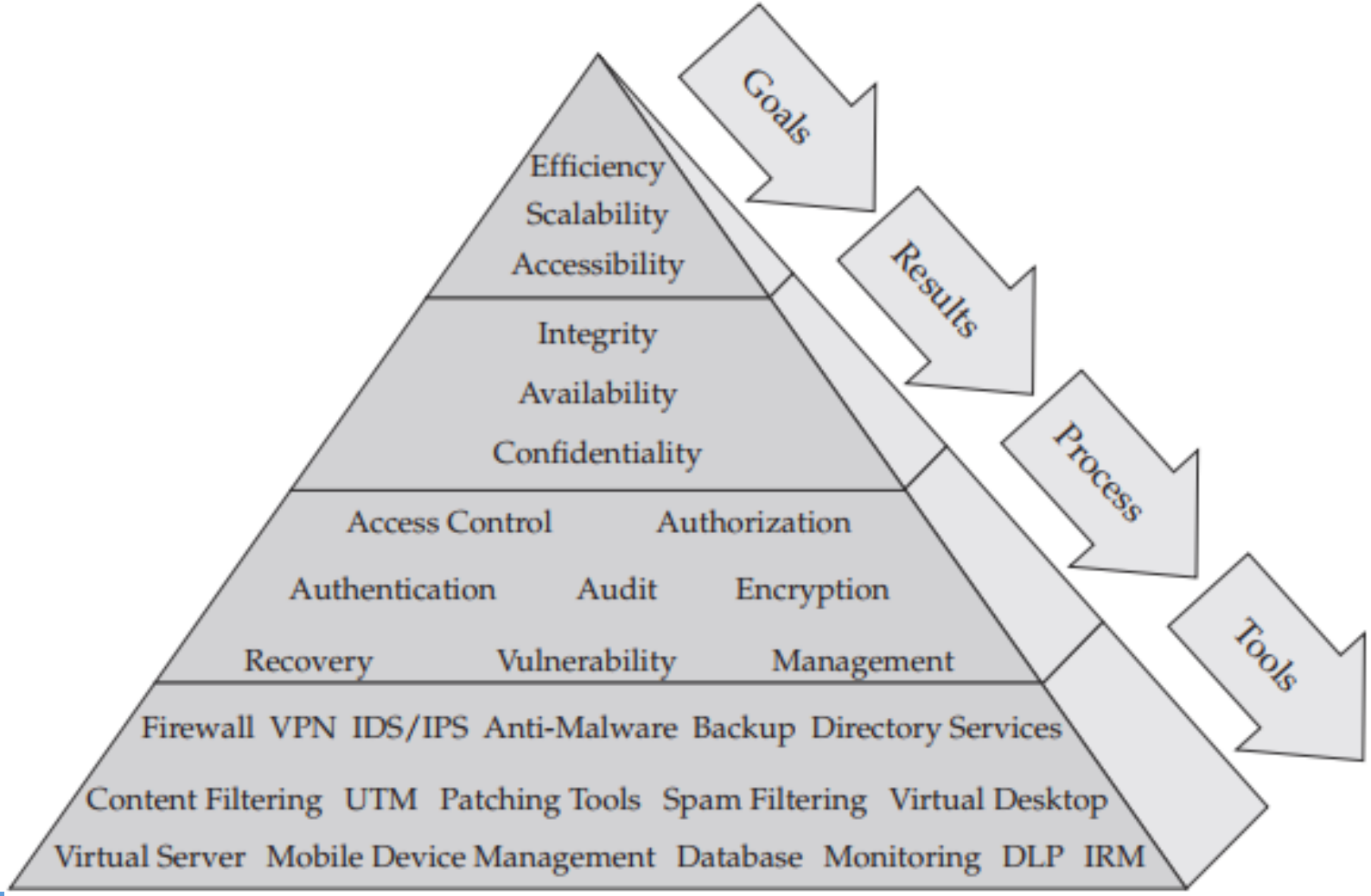
Không có "viên đạn bạc"

- Không có "viên đạn bạc" (No silver bullet) là một nguyên tắc quan trọng trong ATTT: không có 1 công cụ, 1 giải pháp đơn lẻ nào có thể đảm bảo an toàn tuyệt đối cho hệ thống mạng;
- Một số giải pháp bảo mật được quảng cáo quá mức là "all in one/total solution" có khả năng giải quyết mọi vấn đề bảo mật, nhưng không thực sự hiệu quả trên thực tế;
- ➔ cần một hệ thống các giải pháp bảo mật.

Qui trình nghiệp vụ với các kiểm soát kỹ thuật

- Các kiểm soát kỹ thuật bảo mật cần gắn liền với qui trình nghiệp vụ của tổ chức → đảm bảo hiệu quả bảo vệ;
- Từ qui trình nghiệp vụ (như luồng xử lý dữ liệu/luồng hoạt động) → lựa chọn các kỹ thuật, công cụ bảo mật;
- Không thể đạt được 100% an toàn, nhưng có thể "quản lý được rủi ro" đối với tài sản.

Qui trình nghiệp vụ định hướng lựa chọn công cụ bảo mật



1.3 Phân tích rủi ro và các mô hình phòng thủ

- Định nghĩa đe dọa, lỗ hổng và rủi ro
- Phân tích rủi ro
- Các mô hình phòng thủ

Các định nghĩa

- Đe dọa (threat) là điều gì đó có thể xảy ra sai sót và gây thiệt hại cho các tài sản có giá trị;
- Lỗ hổng (vulnerability) là 1 điểm yếu tồn tại trong hệ thống mạng cho phép kẻ tấn công khai thác gây tổn hại đến các thuộc tính an ninh, an toàn của hệ thống mạng;
- Rủi ro (Risk) là chi phí khắc phục khi một đe dọa khai thác thành công một lỗ hổng tồn tại trong hệ thống mạng:
  - Mỗi rủi ro là sự kết hợp của đe dọa, khai thác lỗ hổng và chi phí khắc phục hậu quả sự cố.

Các khía cạnh liên quan đến Đe dọa (Threat)

- Để xây dựng mô hình bảo mật phù hợp, cần phải xem xét tất cả các loại đe dọa. Các khía cạnh liên quan đến Đe dọa cần lưu ý:
  - Threat vectors
  - Threat sources and targets
  - Types of attacks
  - Malicious mobile code
  - Advanced Persistent Threats (APTs)
  - Manual attacks.

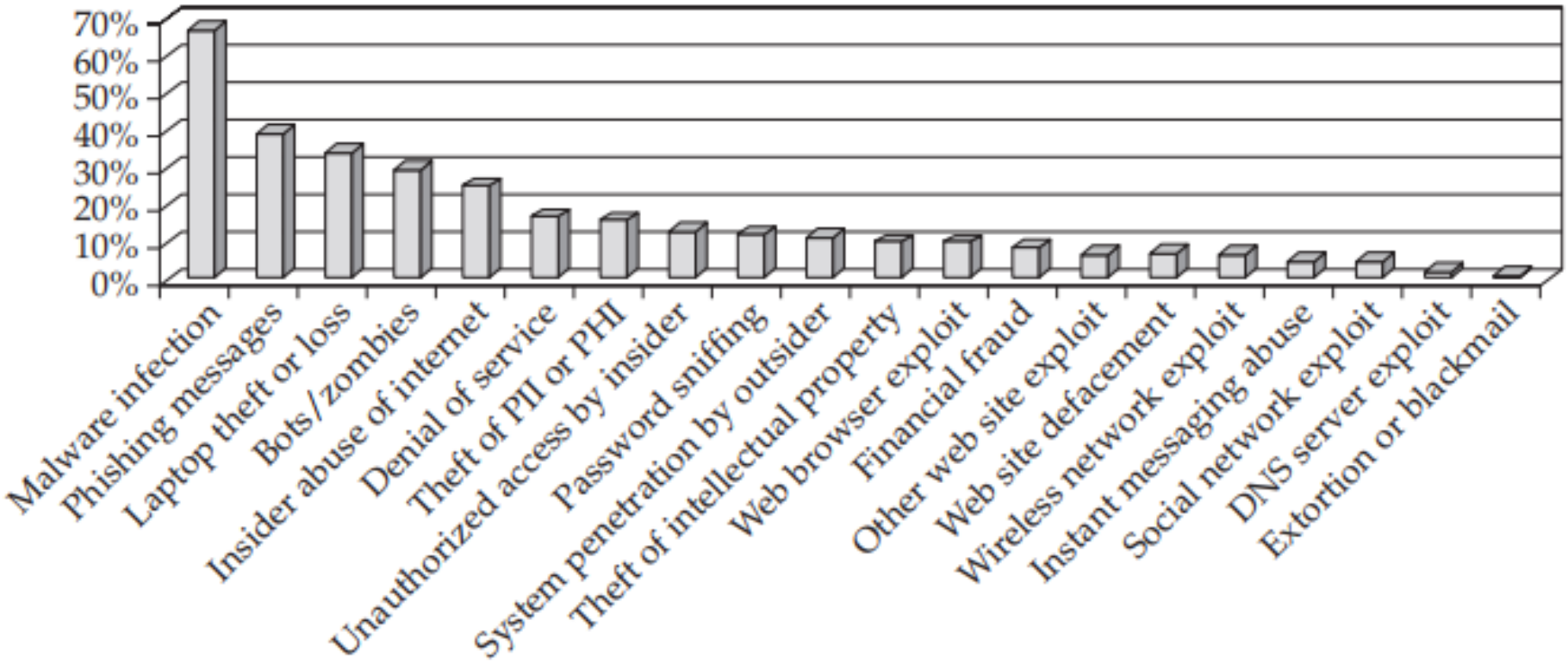
Threat vectors

- Threat vector (véc tơ đe dọa) là 1 thuật ngữ mô tả một đe dọa là gì và nó đến từ đâu;
- Ví dụ về véc tơ đe dọa:
  - Một email gửi từ bên ngoài đến 1 nhân viên trong 1 tổ chức với dòng đề mục (Subject) rất hấp dẫn, đính kèm 1 file thực hiện – thực tế là 1 file mã độc trojan sẽ thỏa hiệp máy tính của người dùng nếu được mở ra và thực hiện.

Một số mẫu Threat vectors

Sources	Threats	Targets
Employee	Theft	Intellectual property
Contractor	Loss	Trade secret
Consultant	Exposure	Personally identifiable information (PII)
System integrator	Unauthorized change	Protected health information (PHI)
Service provider	Deletion (complete)	Financial data
Reseller	Deletion (partial)	Credit card number
Vendor	Unauthorized addition	Social Security number
Cleaning staff	Fraud	Document
Third-party support	Impersonation	Computer
Competitor	Harassment	Peripheral
Insider	Espionage	Storage
Terrorist	Denial of service	Network
Internet attacker	Malfunction	Operating system
Software	Corruption	E-mail
Malware	Misuse	Voice communication
Software bug	Error	Application
Accident	Outage	Privacy
Weather	Physical hazard	Productivity
Natural cause	Injury	Health and safety

Mức độ phổ biến của các đe dọa



Phân tích rủi ro

- Phân tích rủi ro (Risk analysis) là một phần quan trọng của mọi nỗ lực an ninh;
  - Căn cứ vào kết quả phân tích rủi ro, các kiểm soát phòng thủ, răn đe và phát hiện được lựa chọn và triển khai theo các lớp để đạt được hiệu quả bảo vệ cao nhất.
- Phân tích rủi ro cần thực hiện:
  - Phân tích và phân loại các tài sản cần được bảo vệ
  - Các rủi ro cần tránh
  - Lựa chọn và xếp trật tự thực thi các biện pháp bảo vệ
  - Cung cấp phương tiện đo lường hiệu quả của kiến trúc bảo mật tổng thể bằng cách theo dõi các rủi ro đó và biện pháp giảm thiểu rủi ro có liên quan.

Phương pháp tiếp cận đánh giá rủi ro

- Các phương pháp tiếp cận đánh giá rủi ro đã học trong môn Cơ sở ATTT:
  - Phương pháp đường cơ sở (Baseline approach)
  - Phương pháp không chính thức (Informal approach)
  - Phương pháp phân tích chi tiết rủi ro (Detailed risk analysis)
  - Phương pháp kết hợp (Combined approach).

Ước lượng rủi ro

- Định nghĩa đầy đủ của rủi ro: Rủi ro (risk) là xác suất xuất hiện 1 sự kiện không mong muốn (một đe dọa) khai thác 1 lỗ hổng để gây ra 1 hậu quả không mong muốn cho 1 tài sản;
- Công thức chung tính rủi ro:

Rủi ro = Xác xuất xuất hiện(Đe dọa + Khai thác lỗ hổng) x Chi phí khắc phục tài sản hư hại.

Ước lượng rủi ro

- Cách tiếp cận định lượng để phân tích rủi ro sẽ tính đến các giá trị thực tế:
  - Xác suất ước tính hoặc khả năng xảy ra sự cố cùng với chi phí tổn thất hoặc thiệt hại thực tế của tài sản được đề cập;
  - Một cách tiếp cận thường được sử dụng để gán chi phí cho rủi ro là kỳ vọng tổn thất hàng năm (ALE-Annualized Loss Expectancy): Đây là chi phí của một sự kiện không mong muốn - kỳ vọng tổn thất đơn (SLE-Single Loss Expectancy) nhân với số lần bạn dự kiến sự kiện đó xảy ra trong một năm - tỷ lệ xảy ra hàng năm (ARO-Annualized Rate of Occurrence);

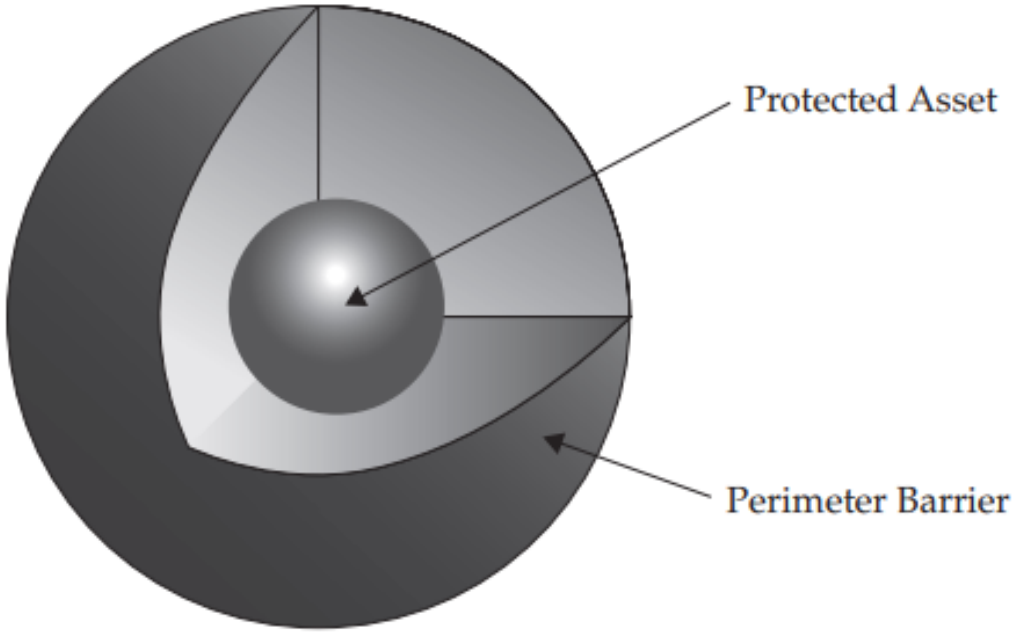
Kỳ vọng tổn thất hàng năm (ALE) = Kỳ vọng tổn thất đơn (SLE) x Tỷ lệ xảy ra hàng năm (ARO)

Các mô hình phòng thủ

- Mô hình Lollipop (kẹo mút)
- Mô hình Onion (củ hành)

Mô hình Lollipop

- Mô hình Lollipop là mô hình phòng thủ được sử dụng rộng rãi nhất trong an ninh mạng, được biết như là *an toàn ngoại vi* (perimeter security);



Mô hình Lollipop

- An toàn ngoại vi liên quan đến việc xây dựng 1 bức tường thực (hoặc ảo) để bảo vệ đối tượng có giá trị;
- An toàn ngoại vi giống như cái kẹo mút (Lollipop) có lớp vỏ cứng và giòn bao quanh nhân mềm và dai;
  - Tường, cửa nhà (thực – vật lý) để bảo vệ tài sản bên trong → mô hình Lollipop;
  - Tưởng lửa (tường ảo) để bảo vệ mạng nội bộ → ngăn chặn tin tặc xâm nhập.
    - Tường lửa không thể ngăn chặn tất cả tin tặc.

Mô hình Lollipop

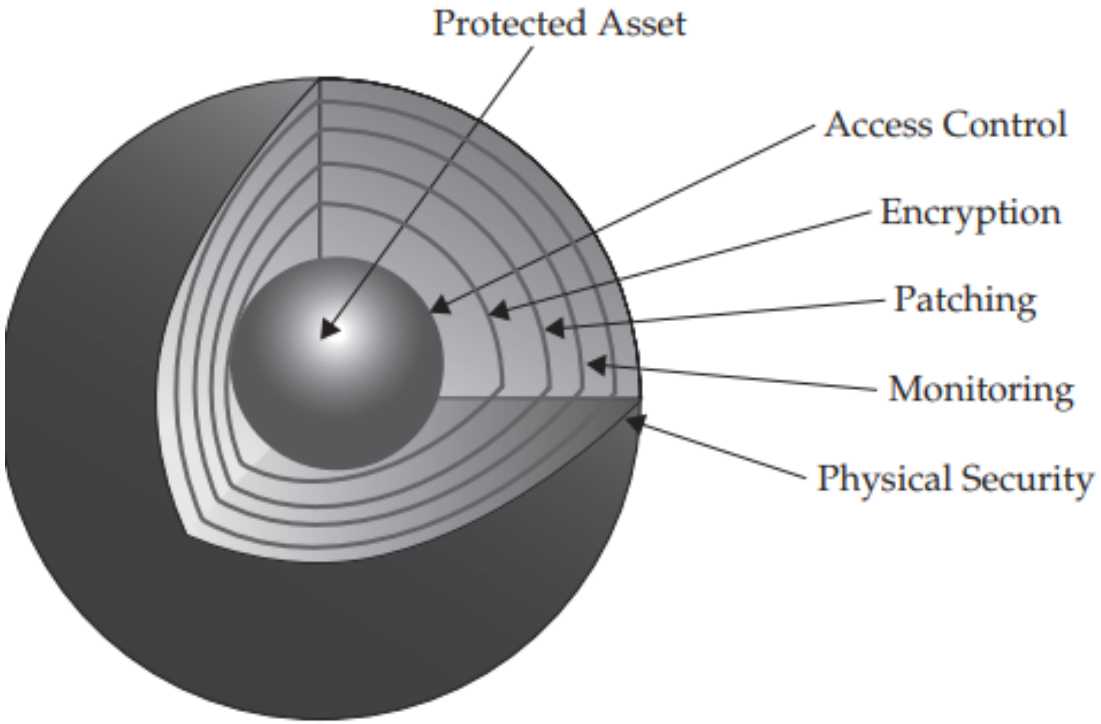
- Hạn chế của mô hình Lollipop:
  - Khi tin tặc vượt qua được lớp an ninh ngoại vi → hắn có thể truy cập tất cả thông tin, tài nguyên được bảo vệ;
    - Lollipop không phải là mô hình tốt nhất.
  - Không cung cấp nhiều mức bảo mật cho các loại tài sản thông tin khác nhau;
    - Trong mạng máy tính, tường lửa cũng có những hạn chế, nên nó ko nên được sử dụng là lớp bảo vệ duy nhất.

Mô hình Lollipop

- Kết luận về mô hình Lollipop:
  - Mô hình phòng thủ Lollipop không đảm bảo an toàn đầy đủ cho hệ thống mạng;
  - Mô hình này không phòng chống được các đe dọa từ bên trong và không cung cấp bảo vệ khi lớp bảo vệ ngoại vi bị xuyên thủng;
- Tường lửa trong mô hình Lollipop:
  - Là thành phần rất quan trọng trong chiến lược an toàn mạng;
  - Nhưng tường lửa chỉ là 1 thàng phần đảm bảo an toàn;
  - Tiếp cần phòng thủ nhiều lớp là tốt nhất.

Mô hình Onion

- Mô hình Onion là mô hình phòng thủ nhiều lớp, còn được gọi là *Phòng thủ theo chiều sâu* (Defense in depth);



Mô hình Onion

- Mô hình Onion khắc phục được vấn đề bảo vệ dự phòng khi lớp bảo mật ngoại vi bị phá vỡ;
- Các lớp bảo mật được xây dựng kế tiếp nhau, như các lớp vỏ của củ hành:
  - Lớp ngoại vi
  - Các lớp trung gian
  - Trong cùng là tài sản cần bảo vệ.
- Tin tặc cần vượt qua tất cả các lớp bảo vệ để xâm nhập được vào tài sản cần bảo vệ.

1.4 Các thực tế tốt nhất về phòng thủ mạng

- Các thực tế tốt nhất về phòng thủ mạng (Best Practices for Network Defense) gồm:
  - Bảo mật môi trường vật lý
  - Tăng cường an toàn cho hệ điều hành
  - Cập nhật các bản vá
  - Sử dụng các phần mềm chống virus
  - Sử dụng phần mềm tường lửa
  - Thiết lập quyền truy cập thư mục chia sẻ an toàn
  - Sử dụng mã hóa
  - Bảo mật ứng dụng
  - Sao lưu hệ thống
  - Cài đặt kỹ thuật phòng chống tấn công đầu độc ARP
  - Xây dựng kế hoạch bảo mật hệ thống.

Bảo mật môi trường vật lý

- Bảo mật môi trường vật lý là khâu quan trọng đầu tiên trong bảo mật hệ thống mạng:
  - Tùy theo mức độ quan trọng, các máy tính, máy chủ cần được đặt trong phòng riêng có khóa, chỉ người có trách nhiệm mới được ra/vào;
  - Bổ sung camera giám sát và các biện pháp xác thực mạnh cho cửa ra vào.
- Xem xét các biện pháp bổ sung:
  - Bảo vệ bằng mật khẩu khởi động
  - Bảo vệ CMOS bằng mật khẩu
  - Cấm khởi động hệ thống sử dụng các thiết bị nhớ ngoài, như USB, CD...

Tăng cường an toàn cho hệ điều hành

- Hệ điều hành là phần mềm nền tảng quản lý truy cập mạng trên hầu hết các thiết bị. HĐH cần được tăng cường an toàn sử dụng các biện pháp:
  - Tắt/vô hiệu quá tất cả các dịch vụ không cần thiết để giảm thiểu bề mặt tấn công hệ thống
  - Cài đặt các phần mềm an toàn
  - Thiết lập cấu hình an toàn cho các phần mềm
  - Định kỳ và kịp thời cập nhật các bản vá cho hệ thống
  - Phân đoạn mạng thành các vùng tin cậy và đặt các hệ thống vào các vùng đó dựa trên nhu cầu liên lạc và mức độ tiếp xúc với Internet của chúng;
  - Tăng cường an toàn cho khâu xác thực
  - Hạn chế số lượng và quyền hạn của các quản trị viên hệ thống.

Cập nhật các bản vá

- Cần có chế độ cập nhật định kỳ các bản vá cho hệ thống
  - Cập nhật ngay với các bản vá có lỗ hổng có độ nghiêm trọng cao.
- Cần thiết lập hệ thống cập nhật tự động để tránh bỏ sót các lỗ hổng không được vá trong thời gian dài.
  - Trên thực tế, rất nhiều lỗ hổng nghiêm trọng đã biết vẫn tồn tại trên nhiều hệ thống, đặc biệt là các dịch vụ, nền tảng cũ mà không được cài đặt các bản vá, mặc dù các bản vá đã được nhà cung cấp phát hành từ lâu.

Sử dụng các phần mềm chống virus

- Các phần mềm chống virus/malware (Anti-virus/ Anti-malware) với khả năng rà quét theo thời gian thực là rất cần thiết với hầu hết các hệ thống;
  - Đặc biệt là với các hệ thống máy của người dùng (PC, desktop, laptop...);
  - Xem xét triển khai các hệ thống Anti-virus/ Anti-malware trên các máy chủ, các cổng kết nối (như cổng email) một cách phù hợp;
  - Cần cập nhật CSDL mẫu malware thường xuyên cho các hệ thống Anti-virus/ Anti-malware để đảm bảo hiệu quả rà quét.

Sử dụng phần mềm tường lửa

- Phần mềm tường lửa cũng rất quan trọng trong hệ thống bảo vệ, đặc biệt đối các hệ thống máy của người dùng (PC, desktop, laptop...);
- Với các máy chủ, mạng, nên sử dụng tường lửa cứng để đảm bảo tốc độ lọc.

Thiết lập quyền truy cập thư mục chia sẻ an toàn

- Các thư mục chia sẻ trên mạng (Network shared folders) cần được thiết lập quyền truy cập phù hợp, hạn chế các truy cập trái phép:
  - Hạn chế các truy cập của người dùng Everyone
  - Hạn chế truy cập ngầm định không cần mật khẩu
  - Hạn chế các truy cập toàn quyền (full control).

Sử dụng mã hóa

- Nên sử dụng các phần mềm, hoặc các kênh truyền thông có mã hóa để làm việc với các hệ thống:
  - SSH, Remote desktop thay cho Telnet cho làm việc từ xa
  - FTPS thay cho FTP cho truyền file
  - HTTPS thay cho HTTP
- Sử dụng VPN (dựa trên IPSec, SSL/TLS) nếu phù hợp
- Sử dụng hệ thống file có mã hóa để bảo vệ dữ liệu file khỏi bị đánh cắp (sao chép, copy...).

Bảo mật ứng dụng

- Nhiệm vụ hàng đầu của các quản trị viên là quản lý các ứng dụng và vấn đề bảo mật của chúng. Bảo mật ứng dụng có thể được thực hiện thông qua:
  - Cấu hình bảo mật ứng dụng (đặc biệt là các ứng dụng mạng, như trình email Outlook, trình duyệt web, cấm các dạng file nguy hiểm – các file mã, file script..., lọc file đính kèm...)
  - Cài đặt ứng dụng mạng trên các cổng và thư mục không chuẩn
  - Khóa các ứng dụng khi cần thiết (cần người quản trị cấp phép việc cài đặt và chạy các ứng dụng cho người dùng thông thường)
  - Tăng cường bảo mật cho các dịch vụ P2P (nhất là dịch vụ chia sẻ file)
  - Đảm bảo các lập trình viên tuân thủ các nguyên tắc lập trình an toàn.

Sao lưu hệ thống

- Sao lưu (backup) là phương pháp chủ động để chống lại việc mất mát dữ liệu cố tình hoặc ngẫu nhiên:
  - Dữ liệu mất do hỏng hóc các thiết bị lưu trữ
  - Dữ liệu mất do tấn công phá hoại, chỉnh sửa, xóa các file trái phép (tin tặc, malware...)
- Sao lưu cần được thực hiện định kỳ tự động:
  - Có thể sao lưu file dữ liệu ra các các thiết bị nhớ ngoài
  - Hoặc sao lưu lên đám mây.

Cài đặt kỹ thuật phòng chống tấn công đầu độc ARP

- Tấn công đầu độc ARP là dạng tấn công thường gặp và một đe dọa chính đối với hạ tầng mạng, nhất là các hệ thống mạng không dây;
  - Một trong các dạng tấn công đầu độc ARP là tấn công man-in-the-middle (MITM) cho phép tin tặc âm thầm chặn bắt và chỉnh sửa lưu lượng mạng.
- Các biện pháp phòng chống tấn công đầu độc ARP gồm:
  - Sử dụng bảng ánh xạ ARP tĩnh
  - Cấu hình giới hạn tốc độ cổng
  - Sử dụng DHCP snooping với kiểm tra ARP động.

Xây dựng kế hoạch bảo mật hệ thống

- Xây dựng kế hoạch bảo mật hệ thống là một trong các phần việc quan trọng của một chiến lược bảo mật. Các bước cần thiết để xây dựng kế hoạch bảo mật gồm:
  1. Kiểm kê các tài sản phải bảo vệ;
  2. Xác định giá trị từng tài sản và khả năng chúng bị khai thác để tính toán mức rủi ro;
  3. Xây dựng một kế hoạch cụ thể để tăng cường an toàn cho các tài sản cần bảo vệ:
     - Tài sản có mức rủi ro cao nhất cần các biện pháp bảo vệ tốt nhất;
     - Đảm bảo tất cả các tài sản được bảo vệ với mức an toàn cơ sở (baseline).

Xây dựng kế hoạch bảo mật hệ thống

4. Phát triển các công cụ và phương pháp bảo mật cơ sở, như:
   - Phát triển một mẫu bảo mật có thể chấp nhận được cho các máy trạm của người dùng cuối
   - Ghi lại phương pháp áp dụng các mẫu bảo mật cho các máy trạm đó, và
   - Áp dụng các chính sách và quy trình để đảm bảo mỗi máy trạm được cấu hình với một mẫu bảo mật.
5. Sử dụng các công cụ rà quét lỗ hổng để đảm bảo các tài sản được cấu hình phù hợp;
6. Thực hiện kiểm tra định kỳ để bảo đảm các cài đặt bảo mật luôn được triển khai;
7. Thay đổi và cập nhật kế hoạch khi xuất hiện các sự cố bảo mật và rủi ro mới.

1.5 Tổ chức, quản lý bảo mật

- Mỗi tổ chức cần có một đơn vị quản lý bảo mật. Tuỳ vào qui mô tổ chức, đơn vị quản lý bảo mật có cơ cấu khác nhau;
- Các vấn đề có liên quan đến tổ chức, quản lý bảo mật:
  - Vai trò và trách nhiệm
  - Phân tách nhiệm vụ
  - Quản lý vận hành bảo mật
  - Quản lý vòng đời bảo mật
  - Vấn đề nhận thức bảo mật
  - Bắt buộc thực thi
  - Phân loại thông tin
  - Xây dựng tài liệu
  - Kiểm toán bảo mật.

Vai trò và trách nhiệm

- Đơn vị quản lý bảo mật của các tổ chức khác nhau sẽ có qui mô và trách nhiệm khác nhau:
  - Các công ty, tổ chức lớn thường có đơn vị bảo mật chuyên trách;
  - Các công ty, tổ chức vừa và nhỏ thường sử dụng lực lượng kiêm nhiệm thực thi các tác vụ có liên quan đến bảo mật.
- Các vấn đề liên quan đến đơn vị bảo mật trong các công ty, tổ chức gồm:
  - Các vị trí công việc bảo mật
  - Đội phản ứng sự cố ATTT

Các vị trí công việc bảo mật

- Các vị trí công việc bảo mật gồm:
  - Nhân viên bảo mật (Security officer):
    - Giao tiếp với nhóm điều hành
    - Quản lý chung đơn vị bảo mật, quyết định nhân sự, giải quyết xung đột và ngân sách
  - Trưởng phòng bảo mật (Chief security officer):
    - Tương tự như Nhân viên bảo mật, là thành viên của nhóm điều hành.
  - Giám đốc bảo mật (Security manager):
    - Điều phối các nỗ lực của nhân viên kỹ thuậtvà đảm bảo rằng các nỗ lực bảo mật phù hợp với yêu cầu kinh doanh;
    - Đưa ra quyết định trong khi xuất hiện một cuộc tấn công hoặc lỗi bảo mật.

Các vị trí công việc bảo mật

- Các vị trí công việc bảo mật gồm:
  - Kiến trúc sư bảo mật (Security architect)
    - Xác định và lập kế hoạch cho hạ tầng an ninh, bao gồm kiến trúc bảo mật kỹ thuật, chính sách bảo mật, tiêu chuẩn, hướng dẫn và thủ tục.
  - Nhân viên bảo mật cơ sở (Facility security officer)
    - Chịu trách nhiệm về những gì diễn ra tại khu vực họ phụ trách
    - Theo dõi các hoạt động, đảm bảo rằng các chính sách và thủ tục được tuân thủ và là phản hồi đầu tiên trong trường hợp xảy ra sự cố bảo mật.
  - Quản trị viên bảo mật (Security administrator)
    - Quản lý và giám sát các thiết bị và hệ thống liên quan đến bảo mật, chẳng hạn như tường lửa, ACL của bộ định tuyến, hệ thống chống vi-rút và máy chủ lọc thư rác.

Đội phản ứng sự cố ATTT

- Đội phản ứng sự cố ATTT (Security Incident Response Team) là một nhóm gồm nhiều nhân viên từ các bộ phận của cơ quan, tổ chức để xử lý các trường hợp khẩn cấp.
- Đội phản ứng sự cố ATTT có thể được gọi với các tên:
  - Đội phản ứng bảo mật (SRT - Security Response Team)
  - Đội phản ứng sự cố máy tính (CIRT - Computer Incident Response Team)
  - Đội phản ứng sự cố (IRT - Incident Response Team)

Đội phản ứng sự cố ATTT

- Một số dạng sự cố mà Đội phản ứng sự cố có thể xử lý:
  - Xâm nhập thù địch vào mạng bởi những người không được ủy quyền
  - Phần mềm gây hại hoặc thù địch hoạt động trên hệ thống hoặc trên mạng
  - Điều tra nhân sự về truy cập trái phép hoặc vi phạm qui định sử dụng
  - Hoạt động của virus/mã độc
  - Lỗi phần mềm, sự cố hệ thống và mất mạng
  - Hợp tác với điều tra quốc tế
  - Điều tra, thu thập bằng chứng theo lệnh của tòa án
  - Các hoạt động bất hợp pháp như vi phạm bản quyền phần mềm.

Phân tách nhiệm vụ

- Phân tách nhiệm vụ trong CNTT
  - Phân tách vai trò và trách nhiệm trong hoạt động CNTT để tránh tình trạng 1 người quyết định tất cả → lạm dụng;
  - VD:
    - Người nhập dữ liệu khác biệt với người kiểm tra dữ liệu
    - Người viết mã chương trình khác người test chương trình.
- Phân tách nhiệm vụ trong quản trị hệ thống
  - Phân tách nhiệm vụ trong quản trị hệ thống để tránh tình trạng "siêu quản trị viên" có thể dẫn đến lạm dụng, gây hại cho cả hệ thống;
  - Cần giảm số lượng "siêu quản trị viên", tách nhiệm vụ để mỗi người quản trị một mảng trong hệ thống.

Quản lý vận hành bảo mật

- Các trách nhiệm vận hành bảo mật
  - Việc phân công trách nhiệm quản lý thực hiện, vận hành bảo mật cần được thực hiện rõ ràng (như sử dụng ma trận trách nhiệm).
- Quản lý dự án
  - Các vấn đề bảo mật cần được quan tâm, xem xét tại mỗi giai đoạn của vòng đời dự án (Khởi động, Thiết kế, Thực thi và Kiểm thử)
- Ủy ban bảo mật
  - Nhằm phối hợp hoạt động của các bộ phận trong tổ chức phục vụ hoạt động đảm bảo ATTT.

Các trách nhiệm vận hành bảo mật

ategory	Function	Description	Owner[1]	Admin[2]	O/S[3]	Application[4]	Level 1[5]	Level 2[6]	Level 3[7]
thentication:									
	Network Authentication	Provides basic network device-to-device authentication as well as RADIUS authentication for end users using the legacy dial-up system	Security Dept.	Network Dept.	Network Dept.	Security Dept.	Help Desk	Network Dept.	Security Dept.
	Token Authentication	Authentication mechanism for end users using VPN for remote access, via dial-up, broadband, and wireless; provides the user database for accounts and hand-held tokens for authentication	Security Dept.	Help Desk	Network Dept.	Security Dept.	Help Desk	Network Dept.	Security Dept.
stem Protection:									
	Virus Management Console	Pushes virus signatures to the desktop clients; provides a central repository for virus data files	Security Dept.	Network Dept.	Network Dept.	Security Dept.	Help Desk	Network Dept.	Security Dept.
	Virus Desktop Client	Provides virus management on the end-user desktop systems and laptops	Security Dept.	Network Dept.	Network Dept.	Security Dept.	Help Desk	Desktop	Security Dept.
	E-Mail Screening Server	Screens e-mail inbound to the company for viruses and spam, blocks messages according to rules	Security Dept.	Network Dept.	Network Dept.	Security Dept.	Help Desk	Network Dept.	Security Dept.
	Desktop Firewall Console Server	Provides the policy rules for desktop clients on the network and laptops that connect remotely	Security Dept.	Security Dept.	Network Dept.	Security Dept.	Security Dept.	Security Dept.	Security Dept.
	Desktop Firewall Client	Blocks directed attacks on the network from penetrating the end-user systems; also provides reporting of attack attempts to console server	Security Dept.	Desktop	Network Dept.	Security Dept.	Help Desk	Desktop	Security Dept.

Các trách nhiệm vận hành bảo mật

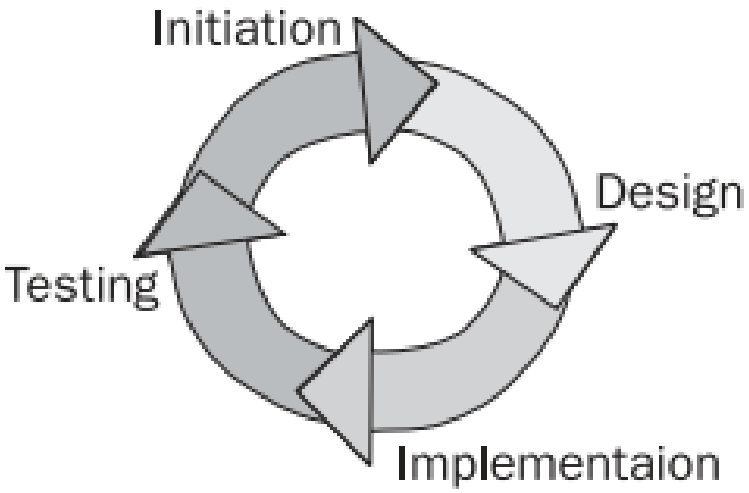
1. Owner: Responsible for decisions about system and app, versions, architecture
2. Admin: Enters data into application
3. O/S: Decides on O/S version and patch level, manages O/S patches, installs O/S
4. Application: Decides on app version and patch level, manages app patches and versions, installs app
5. Level 1: Gets first call, attempts basic troubleshooting
6. Level 2: Checks system, O/S, and services running
7. Level 3: Contacts vendor; performs advanced troubleshooting

Quản lý vòng đời bảo mật

- Nhiệm vụ đảm bảo an toàn có tính vòng đời, trong đó môi trường thay đổi dẫn đến nhiệm vụ đảm bảo an toàn phải thay đổi theo;
- Một số vấn đề liên quan đến Quản lý vòng đời bảo mật:
  - Qui trình bảo mật
  - Vòng đời bảo mật

Qui trình bảo mật

- Vòng đời bảo mật được quản lý bởi qui trình bảo mật, gồm 4 giai đoạn:
  - Khởi động (Initiation)
  - Thiết kế (Design)
  - Cài đặt (Implementation)
  - Kiểm thử (Testing)



Vòng đời bảo mật

- Vòng đời bảo mật gồm 4 giai đoạn chính:
  - Đánh giá (Assessment): kiểm kê tài sản cần bảo vệ, đánh giá rủi ro
  - Chính sách (Policies): xây dựng chính sách, kế hoạch triển khai
  - Gia cố (Hardening): lựa chọn và triển khai các biện pháp bảo mật, tăng cường an toàn
  - Kiểm toán (Audit): kiểm tra, đánh giá kết quả thực hiện bảo mật.

Vấn đề nhận thức bảo mật

- Nâng cao nhận thức bảo mật cho nhân viên là một trong các phương pháp hiệu quả để giảm thiểu các dạng tấn công khai thác yếu tố "người dùng" – những người có quyền truy cập các tài nguyên hệ thống;
- Các chương trình đào tạo, nâng cao nhận thức bảo mật cho nhân viên có thể gồm nhiều mức:
  - Mức cơ bản: Bồi dưỡng, nâng cao nhận thức bảo mật cho nhân viên và người quản lý.
  - Mức chuyên sâu: Bồi dưỡng, nâng cao kỹ năng chuyên môn cho nhân viên bảo mật.

Bắt buộc thực thi

- Bắt buộc thực thi (Enforcement) là một thành phần rất quan trọng của chiến lược bảo mật;
  - Các chính sách, thủ tục và công nghệ bảo mật có thể bị bỏ qua, hoặc lạm dụng nếu không có cơ chế bắt buộc thực thi có hiệu lực.
- Các dạng bắt buộc thực thi:
  - Chính sách bắt buộc thực thi cho nhà cung cấp
  - Chính sách bắt buộc thực thi cho nhân viên
  - Bắt buộc thực thi dựa trên phần mềm
    - Định kỳ đổi mật khẩu bắt buộc.

Phân loại thông tin

- Các thông tin, dữ liệu trong tổ chức cần được phân loại để có cơ chế quản lý bảo mật phù hợp, hạn chế rò rỉ thông tin nhạy cảm.
- Các loại thông tin:
  - Cá nhân (Personal)
  - Công cộng (Public)
  - Confidential (Bí mật)
  - Proprietary (Độc quyền)
  - Secret (Tối mật).

Xây dựng tài liệu

- Xây dựng tài liệu là 1 phần việc quan trọng trong mọi qui trình bảo mật, nhưng thường bị bỏ qua;
  - Một hệ thống bảo mật có tài liệu kèm theo đầy đủ sẽ thuận lợi cho quá trình vận hành, bảo trì, hoặc nâng cấp;
  - Không có hoặc thiếu tài liệu sẽ gây khó khan rất lớn cho quá trình vận hành, bảo trì, hoặc nâng cấp, đặc biệt là khi có sự cố.

Xây dựng tài liệu

- Các tài liệu bảo mật nên gồm các thành phần:
  - Phạm vi
  - Người đọc
  - Các yêu cầu nghiệp vụ
  - Mục đích
  - Các giả thiết
  - Chi tiết về hệ thống bảo mật.

Kiểm toán bảo mật

- Kiểm toán bảo mật (Security audit) là kiểm tra việc tuân thủ các chính sách, qui định bảo mật trong tổ chức;
  - Xác minh các kết quả mong đợi có khớp với các kết quả thực tế, cùng với tính hiệu quả của các biện pháp bảo mật đã được triển khai thực hiện.
  - Có thể được thực hiện định kỳ hoặc không định kỳ theo yêu cầu của tổ chức.
  - Kết quả của kiểm toán bảo mật có thể sử dụng để đưa ra các khuyến nghị cần thực hiện để tăng cường hiệu quả cho các biện pháp bảo mật đã hoặc sẽ triển khai.

Kiểm toán bảo mật

- Kiểm toán bảo mật toàn diện cần kiểm tra các vấn đề:
  - Tính dư thừa: Hệ thống mạng cần đảm bảo có dự phòng về đường truyền và thiết bị để nó vẫn có thể hoạt động nếu có một số thành phần trung tâm gặp trục trặc;
  - Phòng thủ nhiều lớp:
    - Có lớp bảo vệ ngoại vi chống lại các tấn công từ bên ngoài, như tường lửa;
    - Có lớp bảo vệ thứ hai chống lại các hành vi tấn công, lạm dụng, như các hệ thống IDS/IPS.
  - Bảo mật vật lý:
    - Hệ thống mạng cần được đảm bảo an toàn về mặt vật lý: các thiết bị mạng và máy chủ trọng yếu cần được đặt trong phòng riêng có khóa và truy cập vật lý đến các thiết bị này cần được kiểm soát chặt chẽ.

Kiểm toán bảo mật

- Kiểm toán bảo mật toàn diện cần kiểm tra các vấn đề:
  - Truy cập từ xa:
    - Kết nối VPN nên được sử dụng thay cho các kết nối quay số hoặc kết nối đến văn phòng từ xa do độ ổn định và bảo mật cao hơn;
    - Các kết nối qua VPN cũng cho phép người dùng ở xa có kênh an toàn có thể bảo vệ mật khẩu và quyền truy cập.
  - Chính sách bảo mật của tổ chức:
    - Chính sách bảo mật của tổ chức cần được thiết lập theo mục tiêu kinh doanh của đơn vị;
    - Chính sách bảo mật cần được cập nhật theo sự thay đổi của tổ chức.