KỸ NĂNG BẢO ĐẢM AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

Nội dung chính

1. Tổng quan về các nguy cơ và rủi ro mất an toàn thông tin đối với người dùng
2. Nguy cơ rò rỉ và hình thức tấn công đánh cắp dữ liệu và thông tin cá nhân
3. Bảo đảm an toàn cho tài khoản đăng nhập
4. Bảo đảm an toàn thông tin cho máy tính cá nhân
5. Bảo đảm an toàn thông tin cho thiết bị thông minh
6. Bảo đảm an toàn hệ thống thông tin theo cấp độ

Nội dung phần I

1

- Tổng quan về các nguy cơ và rủi ro mất an toàn thông tin đối với người dùng

2

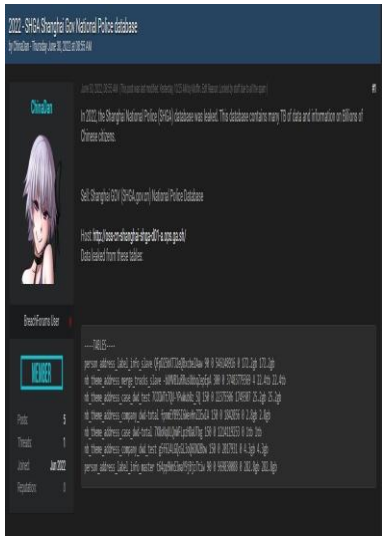
- Nguy cơ rò rỉ và hình thức tấn công đánh cắp dữ liệu và thông tin cá nhân

1. Tổng quan về các nguy cơ và rủi ro mất an toàn thông tin đối với người dùng

Nhiều sự cố lộ lọt dữ liệu cá nhân nghiêm trọng

Thế giới: Năm 2022, Hacker "ChinaDan" rao bán dữ liệu được cho là rò rỉ từ Sở Cảnh sát Quốc gia Thượng Hải trên một diễn đàn dành cho hacker:

- Dữ liệu được rao bán có dung lượng khoảng 23TB, bao gồm 1 tỷ bản ghi thông tin của người dân Trung Quốc, gồm các trường dữ liệu: Họ tên, Địa chỉ, Nơi sinh, Số định danh quốc gia và CSDL khác bao gồm: CSDL tội phạm, thông tin liên kết số điện thoại di động.



- Hacker yêu cầu 10 BTC (giá lúc đăng khoảng 200 nghìn USD) cho lượng dữ liệu khổng lồ này. Vụ việc được cho là vụ rò rỉ dữ liệu lớn nhất của Trung Quốc, đã gây chấn động mạnh tới giới bảo mật trong nước.

Việt Nam: Ngày 08/7/2022: Hacker "meli0das" rao bán dữ liệu được cho là rò rỉ từ một CSDL giáo dục tại Việt Nam với hơn 30 triệu dữ liệu học sinh, sinh viên, giáo viên… (khoảng 1/3 dân số Việt Nam) với giá 3.500 USD.

Nhiều vụ việc tấn công gây mất an toàn thông tin

Việt Nam:

Trong 9 tháng đầu năm 2022, tại Việt Nam, Trung tâm Giám sát an toàn không gian mạng – Cục An toàn thông tin cũng đã ghi nhận:

- Có **9.519** cuộc tấn công mạng, gây ra sự cố vào các hệ thống thông tin, trong đó riêng trong tháng 9/2022 là 988 cuộc; ngăn chặn 926 website lừa đảo, trong đó có nhiều trang giả mạo các ngân hàng, tổ chức tài chính;
- Gần **4.000** phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông tin tới hệ thống cảnh báo, qua kiểm tra, có rất nhiều trường hợp lừa đảo giả mạo website của ngân hàng, công ty tài chính…

Trong tháng 10/2022, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận:

- **517.627 địa chỉ IP** của Việt Nam nằm trong mạng botnet (giảm 2.49% so với tháng 9/2022), trong đó có **224 địa chỉ IP** của cơ quan, tổ chức nhà nước (20 địa chỉ IP Bộ/Ngành, 204 địa chỉ IP Tỉnh/Thành);
- **1.768 điểm yếu, lỗ hổng** an toàn thông tin tại các hệ thống thông tin của các cơ quan tổ chức nhà nước. Số lượng điểm yếu, lỗ hổng nêu trên là rất lớn.

Nguy cơ và Rủi ro

- **Nguy cơ (Threat):** là những **sự kiện** có khả năng ảnh hưởng đến an toàn của hệ thống.
- **Rủi ro (risk):** là xác suất xảy ra **thiệt hại** đối với hệ thống.

Các nguy cơ với người dùng

- Nguy cơ mất an toàn thông tin đối với người dùng (User)

- **Sử dụng Máy Tính**
- **Sử dụng Mạng Xã hội**
- **Sử dụng thiết bị di động**
- **Sử dụng mạng công cộng**
- **Bảo mật tài khoản**

=> USER cần trang bị kiến thức ATTT

Rủi ro mất an toàn thông tin đối với người dùng

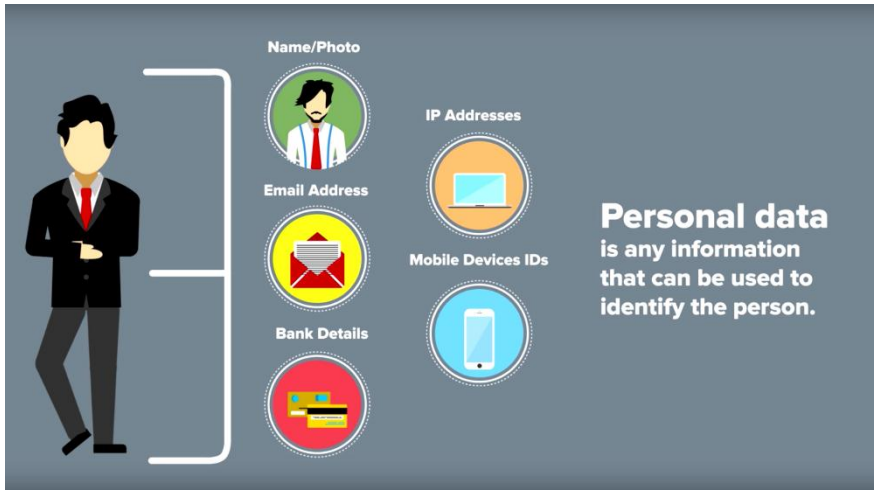
- **Mất dữ liệu (Mất tiền)**
- **Máy tính hoạt động không ổn định**
- **Làm bàn đạp để tấn công các máy tính khác trong mạng**
- **Tham gia vào mạng Botnet**

2. Nguy cơ rò rỉ và hình thức tấn công đánh cắp dữ liệu và thông tin cá nhân

Dữ liệu cá nhân

Dữ liệu cá nhân: Là bất kỳ thông tin nào để xác định được hay có thể xác định được danh tính của một cá nhân cụ thể

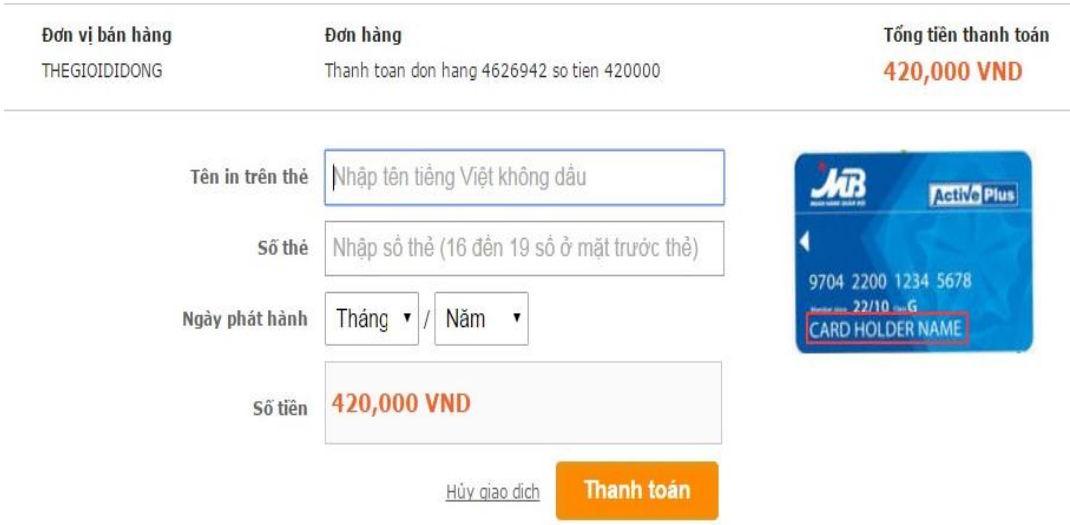
- Ví dụ: Họ tên, số điện thoại, địa chỉ email và địa chỉ cư trú/địa chỉ thư tín, thông tin thẻ tín dụng của cá nhân, ..



Sử dụng dữ liệu cá nhân

Dữ liệu cá nhân thường được dùng trong các ứng dụng:

- Email
- Thương mại điện tử.
- Để đăng ký sử dụng các dịch vụ trên internet (Facebook, youtube, …).



Quản lý thông tin cá nhân

Nhà quản lý thông tin cá nhân là người hoặc tổ chức quản lý việc thu thập, lưu trữ, xử lý hoặc sử dụng thông tin cá nhân.

- Cơ quan nhà nước
- Các tổ chức khác cơ quan nhà nước (khu vực tư nhân)

Nguyên nhân lộ lọt thông tin

- **Người dùng:** Thống kê cho thấy có tới 80% nguyên nhân lộ lọt thông tin cá nhân là xuất phát từ chính sự bất cẩn của người sử dụng.
- **Nhà quản lý thông tin:** hệ thống bị tấn công, bán thông tin cá nhân.

Hậu quả của lộ lọt thông tin

- Gặp rắc rối vì tin nhắn rác, tin nhắn quảng cáo...
- Lừa đảo trên mạng: sử dụng ảnh thật của người dùng mạng xã hội để tạo nên những tài khoản giả mạo, lừa chính bạn bè, người thân của họ.
- Tội phạm mạng: có thể sử dụng chính những thông tin do chính chủ tự nguyện cung cấp để đe dọa tống tiền, bắt cóc, hoặc lừa người sử dụng chuyển tiền vào tài khoản của tội phạm.

Điều gì xảy ra khi thông tin cá nhân bị lộ lọt?

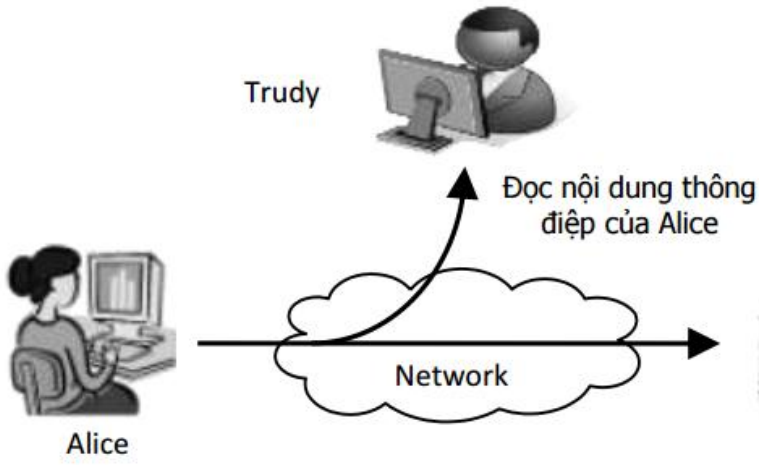
Tầm quan trọng của việc bảo vệ dữ liệu và bảo mật thông tin cá nhân

Bảo vệ dữ liệu cá nhân:

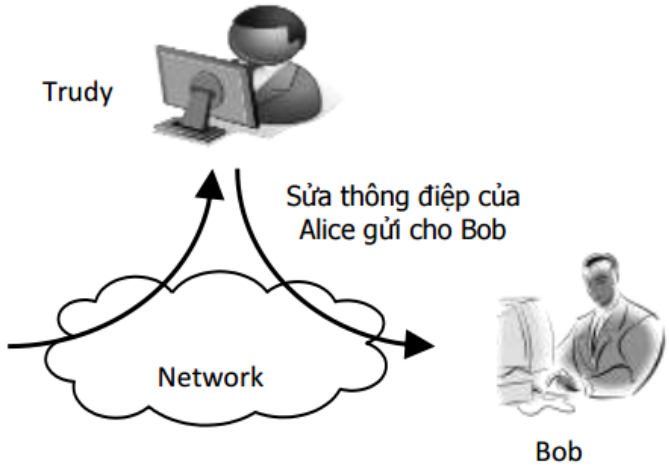
- Dùng để chỉ việc bảo vệ dữ liệu có liên quan đến cá nhân trước sự lạm dụng.
- Bảo vệ từng cá nhân không bị thiệt thòi trong quyền tự quyết định về thông tin của chính mình thông qua việc sử dụng dữ liệu liên quan đến cá nhân của họ.
- Để tránh những thiệt hại do thông tin cá nhân bị xâm nhập bất hợp pháp và bị lạm dụng

Các loại hình tấn công

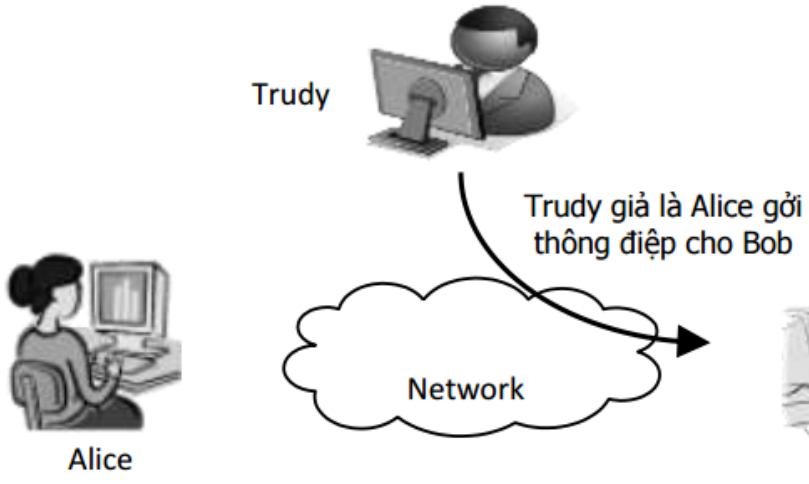
- **Xem trộm thông tin**



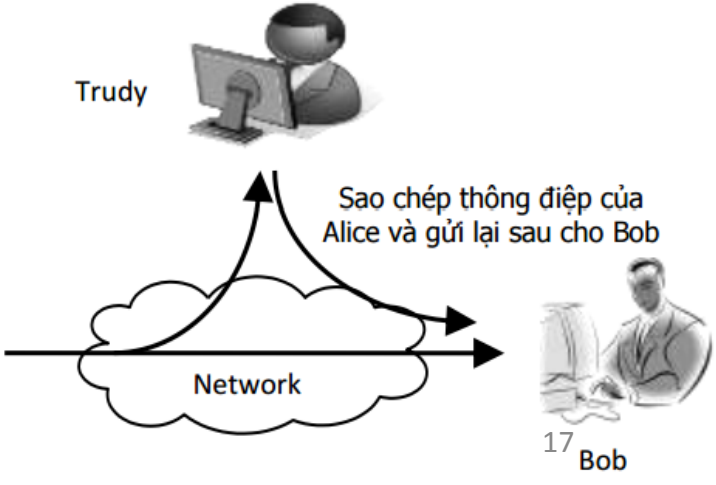
- **Thay đổi thông tin**



- **Mạo danh**



- **Phát lại thông tin**



Xem trộm thông tin

Xem thông tin mà không được sự cho phép của người sở hữu thông tin

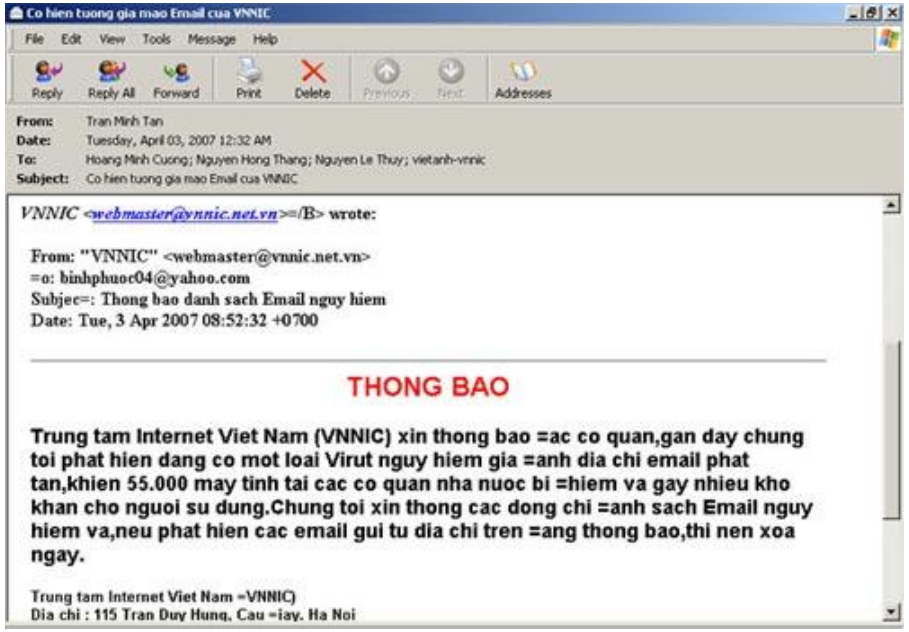
Thay đổi thông tin

Thay đổi trái phép thông tin gốc

Mạo danh

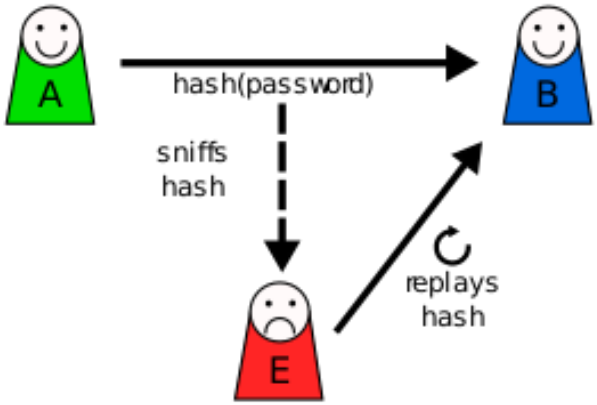
- Kẻ tấn công đóng giả là một tổ chức hoặc công ty uy tín để lừa đảo người dùng và thu thập thông tin nhạy cảm của họ – chẳng hạn thông tin thẻ tín dụng, tên đăng nhập, mật khẩu v.v.
- Gửi email
- Gọi điện thoại

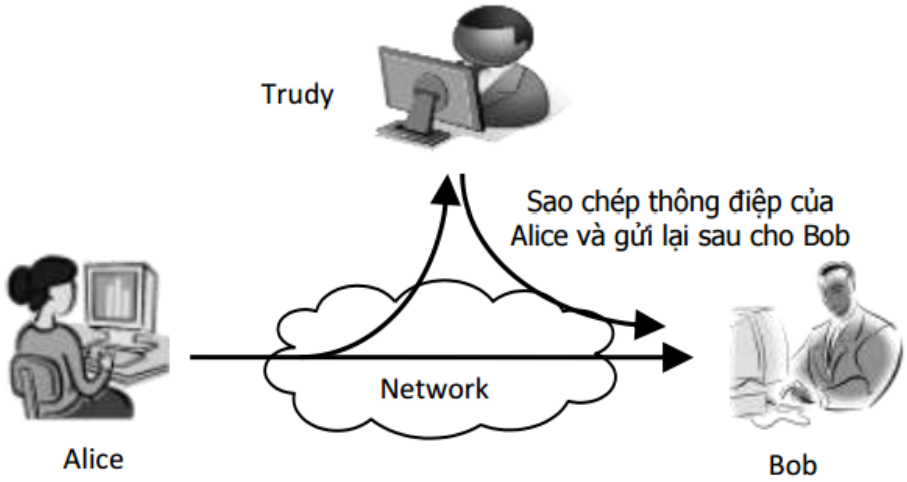
Social engineering



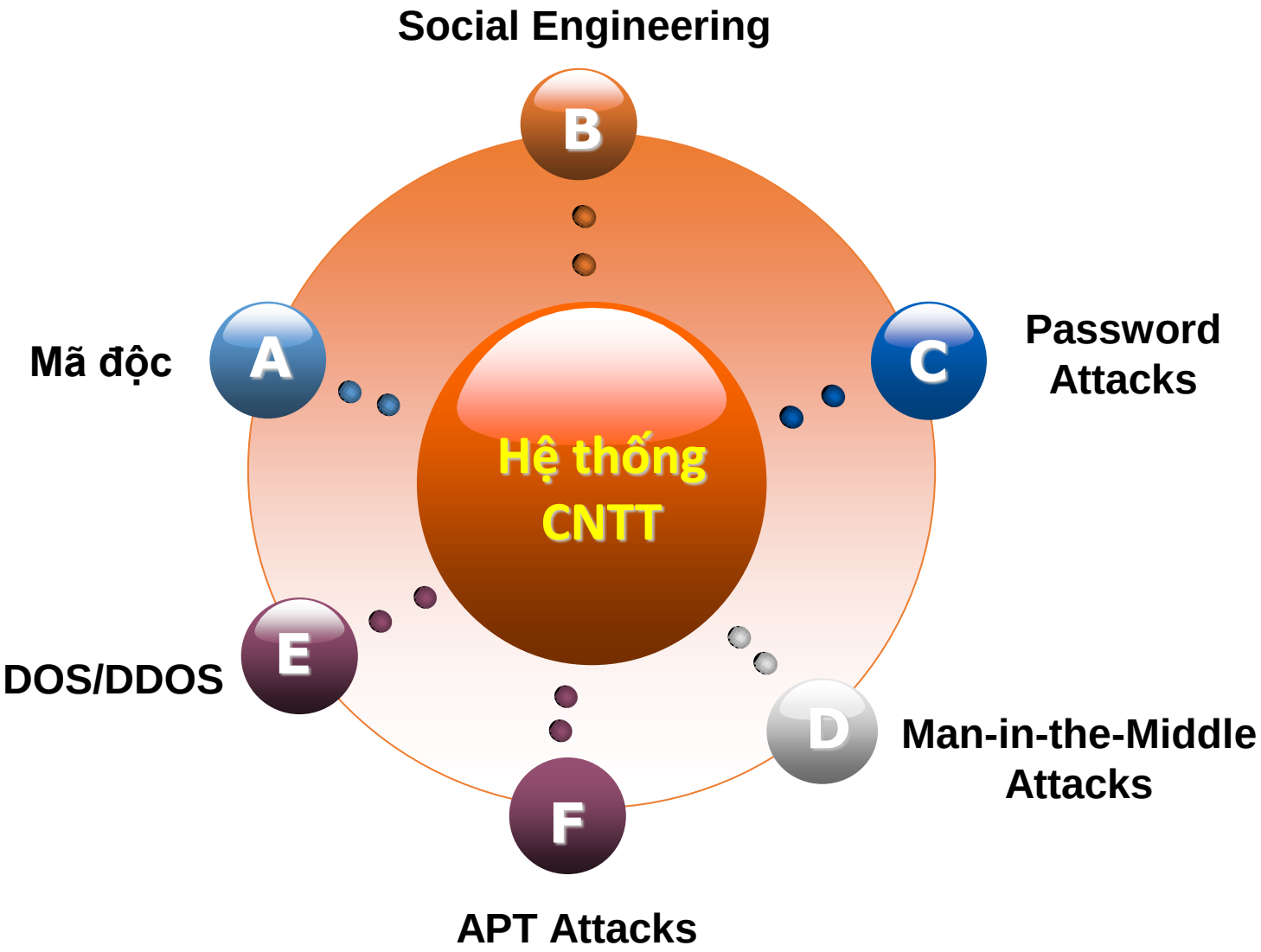
Phát lại thông tin

- Lặp lại việc truyền tải một dữ liệu hợp lệ đi vào trong mạng.
- Kẻ tấn công không thay đổi nội dung dữ liệu.





Các hình thức tấn công đánh cắp thông tin



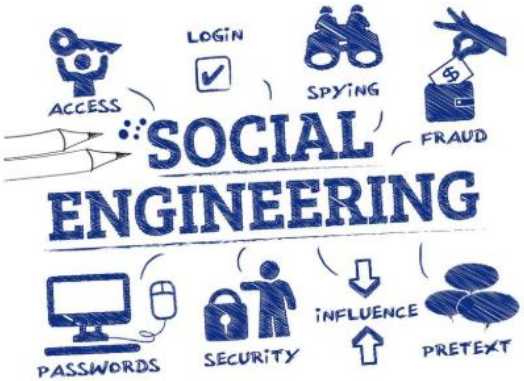
Social Engineering

Đánh lừa hoặc thuyết phục người dùng cung cấp thông tin nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó

Có 2 loại Social Engineering:

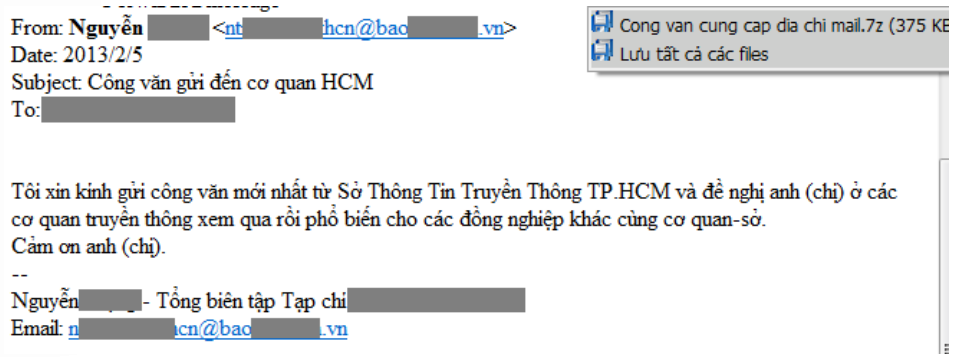
- Dựa trên con người: tương tác giữa con người với nhau
- Dựa trên máy tính: sử dụng các phần mềm để thu thập thông tin

Đánh lừa người dùng, nhằm lấy cắp dữ liệu hoặc tống tiền.

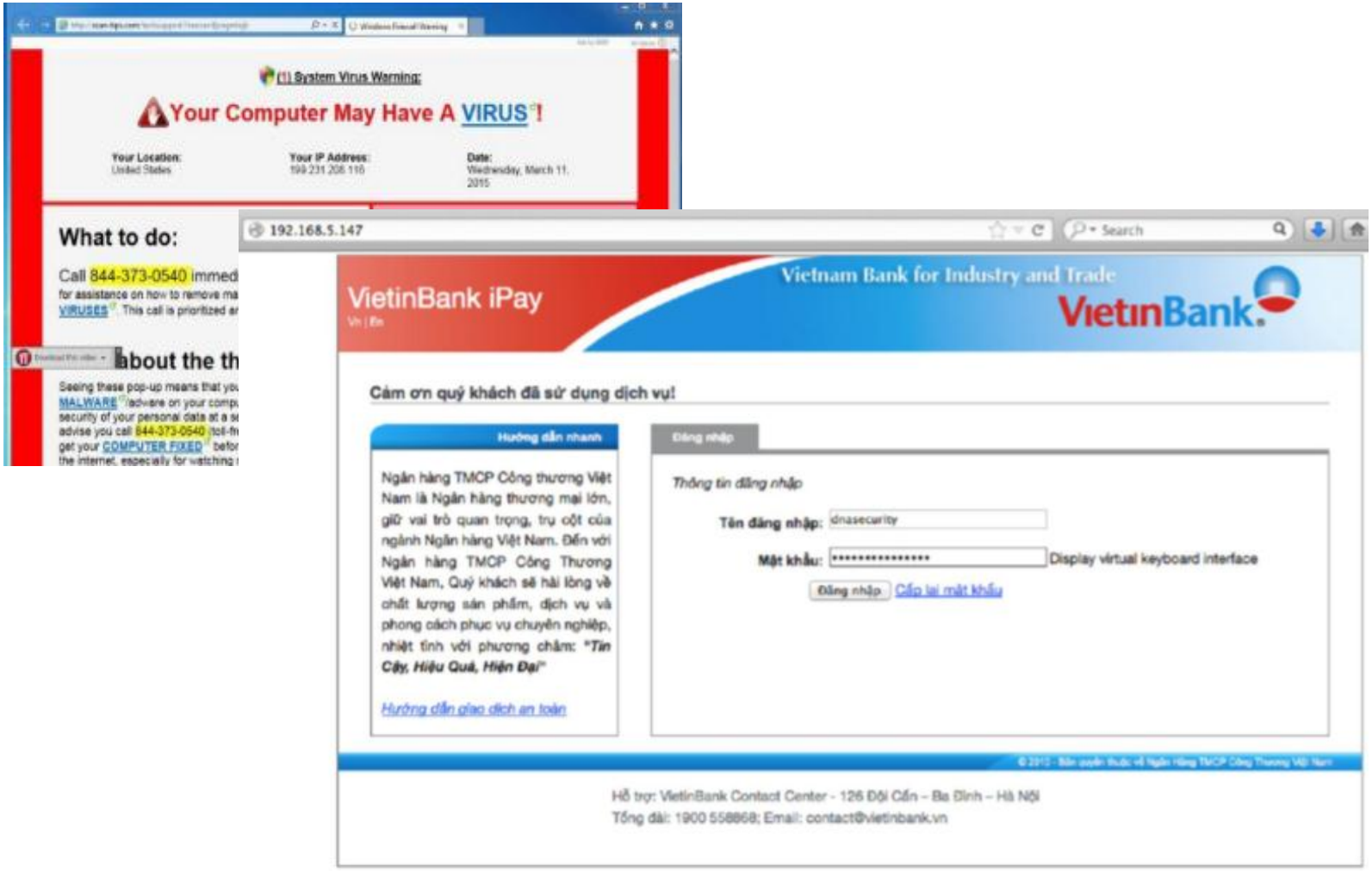


Giải pháp phòng chống: đào tạo

Social Engineering



Social Engineering



Mã độc (Malicious software)

Loại phần mềm được **tạo ra và chèn** vào hệ thống một cách **bí mật**.

Mục đích: thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin

Hậu quả: làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân.

Phân loại: tùy theo chức năng, cách thức lây nhiễm, phá hoại: virus, worm, trojan, rootkit …

Các loại mã độc phổ biến

Boot virus

Macro virus

Virus Hoax

Scripting virus

Biến thể

File Virus

Botnet

Trojan horse

Rootkit

BackDoor

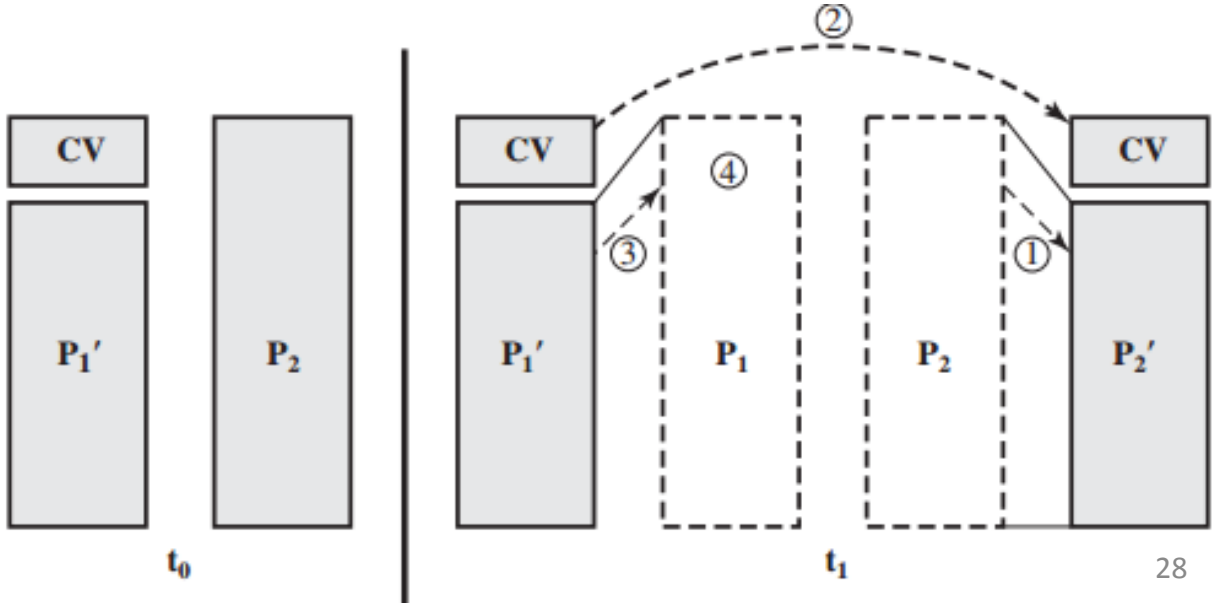
Worm

Adware và Spyware

Virus

- Sao chép chính nó từ đối tượng bị nhiễm sang đối tượng khác (File, Folder, Máy tính, ..).
- Hình thức lây lan:
  - USB, Email
  - File Download

Fred Cohen 1983



WORM

- Lây lan trên hệ thống mạng. Worm là network virus.
- Worm: Tự động lây lan mà không cần chờ sự kiện

Các hình thức lây lan

- Thông qua email, chat
- Chia sẻ file

Tấn công bằng mã độc

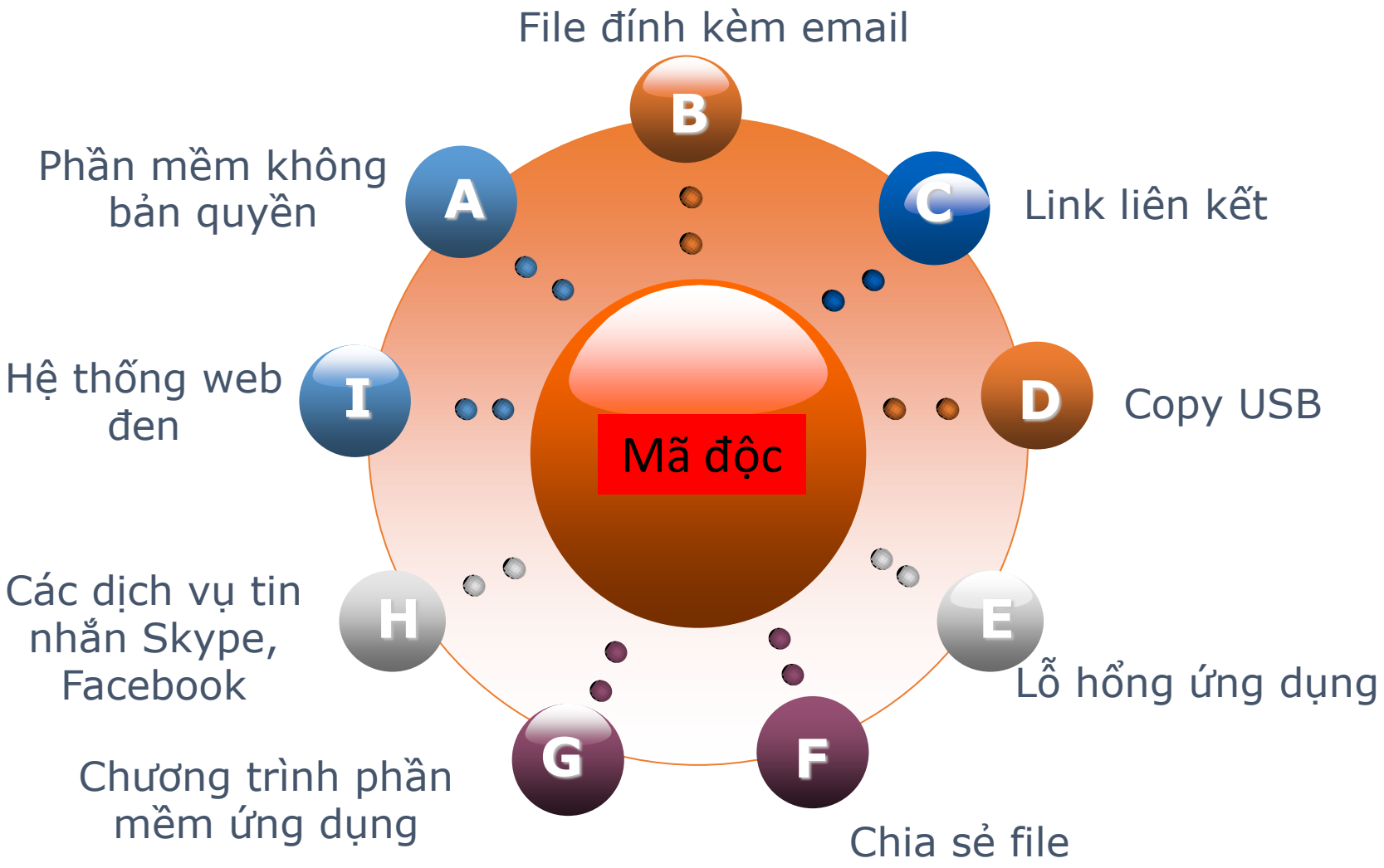
- Mã độc tống tiền WannaCry

EternalBlue MS17-010

Đính kèm mã độc trong Email

Đính kèm trong file Crack, data

Cơ chế lây lan của Mã độc

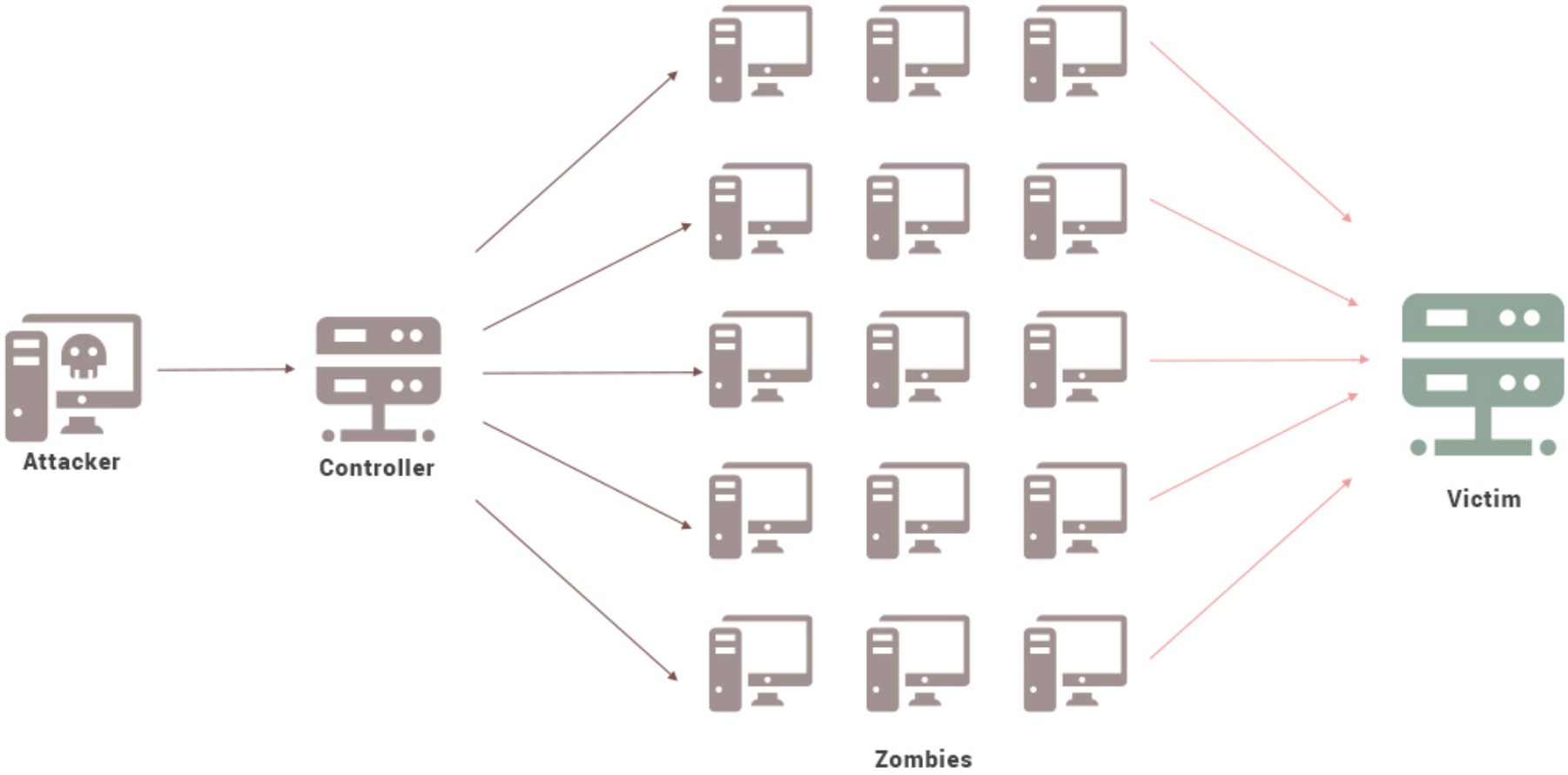


Password Attacks

- **Brute Force attack**: đoán mật khẩu (ngày sinh, CMND, mã số nhân viên, ..)
- **Dictionary attack**: dùng một file (dictionary) chứa tất cả các password có thể có. Thử từng password cho đến khi tìm được mật khẩu.

Tấn công DOS/DDOS

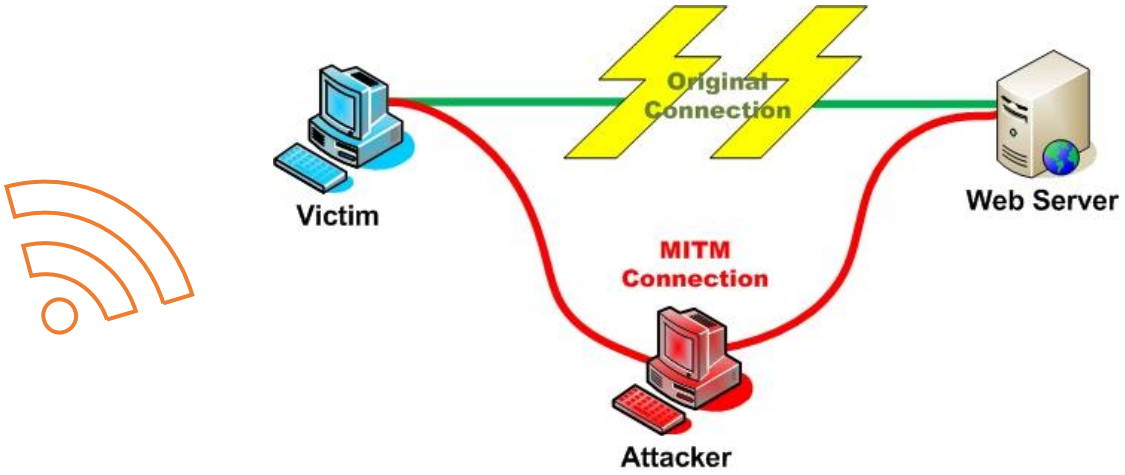
- **Tấn công từ chối dịch vụ/từ chối dịch vụ phân tán**

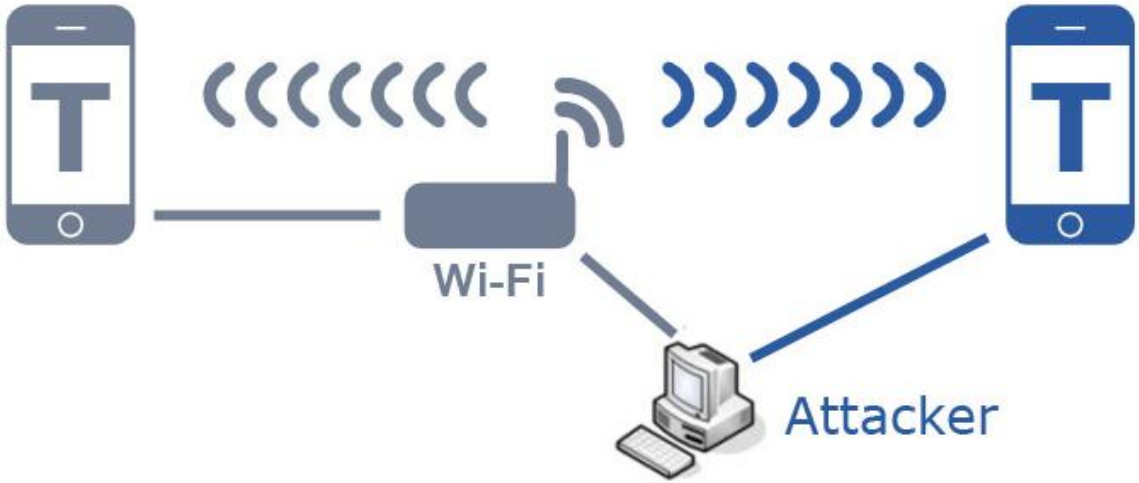


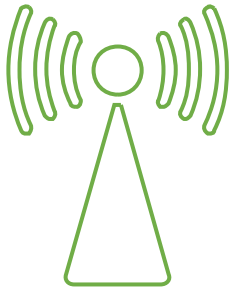
Man-in-the-Middle Attacks

- **Dữ liệu sẽ được truyền qua Attacker trước khi đến đích.**

Cần thận trọng khi sử dụng các mạng công cộng!!!







Tấn công có chủ đích APT

- Advanced Persistent Threat

Phương thức cơ bản bảo vệ dữ liệu cá nhân

- Sử dụng mạng xã hội.
- Sử dụng máy tính.
- Sử dụng điện thoại di động
- Sử dụng mạng công cộng.
- Bảo mật tài khoản đăng nhập.

Cung cấp thông tin càng ít càng tốt.

Nhận diện lừa đảo trên mạng

Sử dụng từ nguồn tin cậy

Phương thức cơ bản bảo vệ dữ liệu cá nhân

Sử dụng mạng xã hội: Mạng xã hội có những tính năng như trò chuyện, gửi thư điện tử, chia sẻ phim ảnh, tệp tin, đăng bài viết cá nhân, bình luận....

Không tiết lộ, địa chỉ thực tế, lịch công tác, thông tin liên quan tới công việc của mình tại cơ quan

Mật khẩu mạnh (Strong Password)

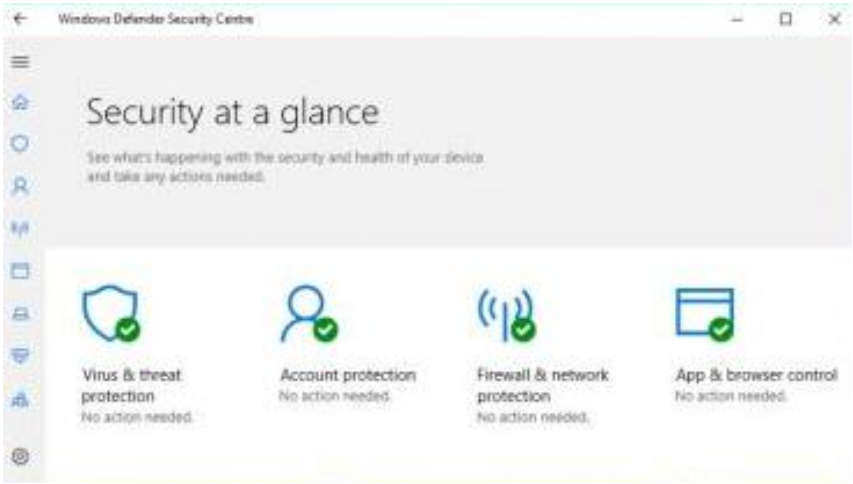
Suy nghĩ và cân nhắc kỹ về những gì viết và đăng trên mạng

Xin phép trước khi đăng tải những bức ảnh và các câu chuyện của họ

Phương thức cơ bản bảo vệ dữ liệu cá nhân

Sử dụng máy tính:

- Sử dụng hệ điều hành và các ứng dụng có bản quyền (license).
- Thường xuyên update hệ điều hành.
- Luôn sử dụng các chương trình bảo mật cho hê điều hành (Windows defender, antivirus)



Phương thức cơ bản bảo vệ dữ liệu cá nhân

Sử dụng máy tính:

- Chính sách password cho máy tính
- Backup dữ liệu
- Disable các User không sử dụng

- Chú ý khi sử dụng USB
- Sử dụng Email an toàn (Backup, chính sách password)

Phương thức cơ bản bảo vệ dữ liệu cá nhân

Sử dụng điện thoại di động

- Thiết lập password khóa màn hình
- Update hệ điều hành
- Cài các ứng dụng tin cậy

Phương thức cơ bản bảo vệ dữ liệu cá nhân

Sử dụng mạng công cộng.

- Tắt Network Sharing
- Dùng VPN (Virtual Private Network) nếu muốn truy cập vào các trang đăng nhập.
- Dùng các trang HTTPS

Phương thức cơ bản bảo vệ dữ liệu cá nhân

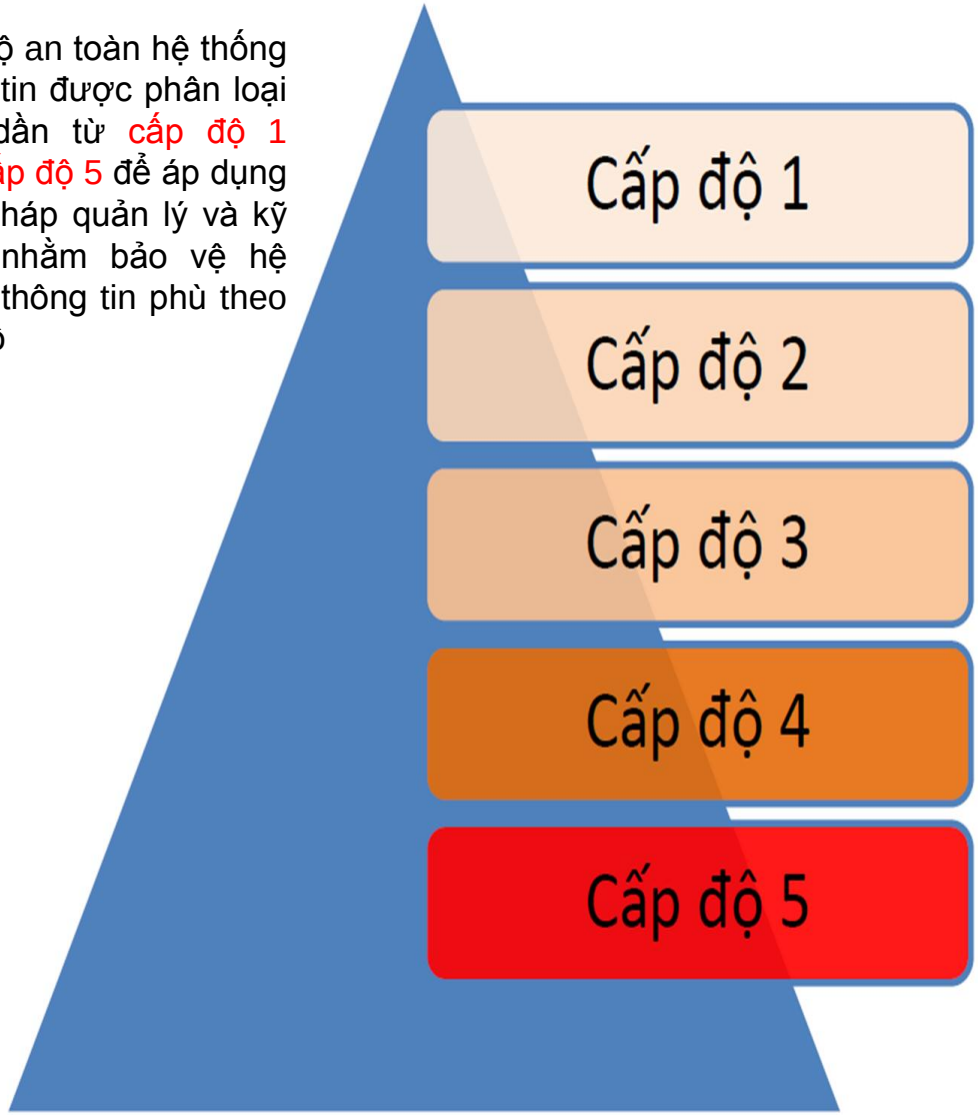
Bảo mật tài khoản đăng nhập

- Cấu hình xác thực 2 bước tài khoản gmail.
- Mật khẩu mạnh (strong password)
- Thay đổi mật khẩu định kỳ
- Không chia sẻ password cho người khác.
- Luôn logout tài khoản sau khi sử dụng trên máy tính của người khác

Bảo đảm an toàn hệ thống thông tin theo cấp độ

Phân loại cấp độ an toàn thông tin

Cấp độ an toàn hệ thống thông tin được phân loại tăng dần từ cấp độ 1 đến cấp độ 5 để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù theo cấp độ



Cấp độ 1 khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia.

Cấp độ 2 khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia.

Cấp độ 3 khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia.

Cấp độ 4 khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia.

Cấp độ 5 khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

Bảo đảm an toàn hệ thống thông tin theo cấp độ

Xác định cấp độ an toàn thông tin

Cấp độ 1

Phục vụ hoạt động nội bộ của cơ quan, tổ chức và chỉ xử lý thông tin công cộng.

Cấp độ 2

- Hệ thống nội bộ và có xử lý TT riêng, TTCN;
- Phục vụ người dân, doanh nghiệp, cung cấp DVCTT mức độ 2 trở xuống / DV trực tuyến không thuộc DM dịch vụ KD có ĐK / DV trực tuyến khác có xử lý TT riêng, TTCN của <10.000 NSD;
- Cơ sở hạ tầng thông tin phục vụ hoạt động của một cơ quan, tổ chức.

Cấp độ 3

- Xử lý thông tin BMNN / khi bị phá hoại sẽ làm tổn hại tới QP, AN quốc gia.
- Phục vụ người dân, doanh nghiệp cung cấp DVCTT mức độ 3 trở lên / DV trực tuyến thuộc danh DM KD có ĐK / DV trực tuyến khác có xử lý TT riêng, TTCN của >= 10.000 NSD.
- Cơ sở hạ tầng thông tin dùng chung trong phạm vi một ngành, một tỉnh hoặc một số tỉnh…

Cấp độ 4

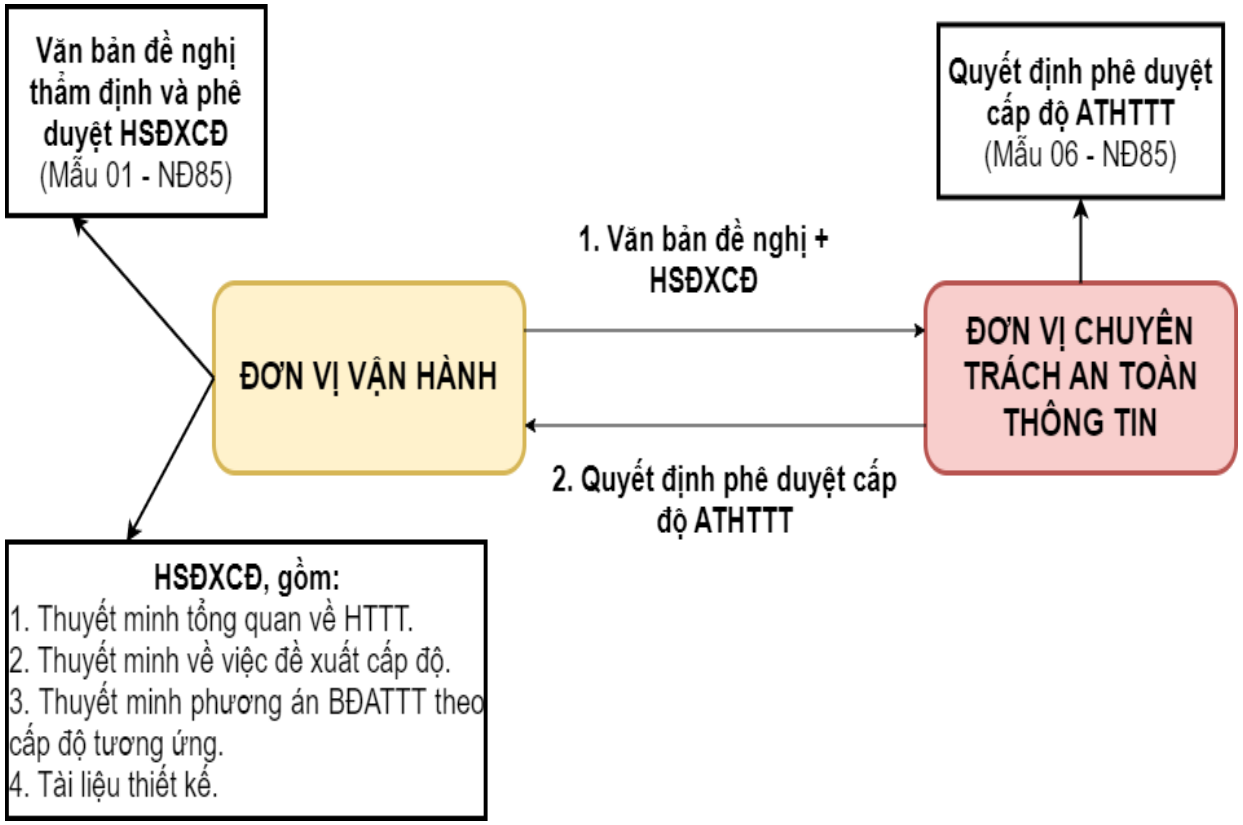
- Xử lý thông tin BMNN / khi bị phá hoại sẽ làm tổn hại nghiêm trọng QP, AN quốc gia.
- Phục vụ phát triển CPĐT / cơ sở hạ tầng thông tin dùng chung trên phạm vi toàn quốc, yêu cầu vận hành 24/7, không chấp nhận ngừng vận hành mà không có kế hoạch trước…

Cấp độ 5

- Xử lý thông tin BMNN / khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới QP, AN quốc gia.
- Phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia.
- Cơ sở hạ tầng thông tin QG phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế…

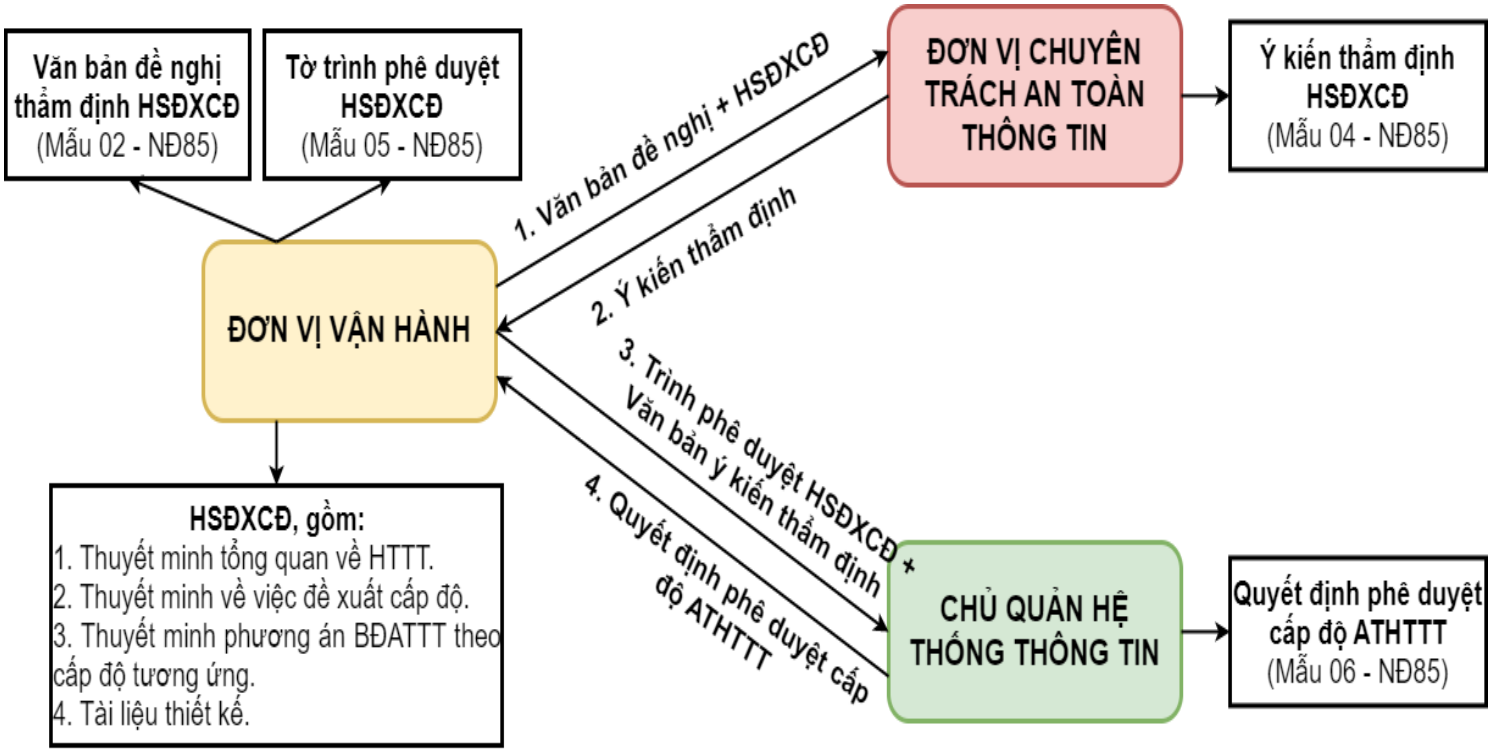
Thẩm định, phê duyệt hồ sơ đề xuất cấp độ

Hệ thống thông tin được đề xuất cấp độ 1 hoặc cấp độ 2



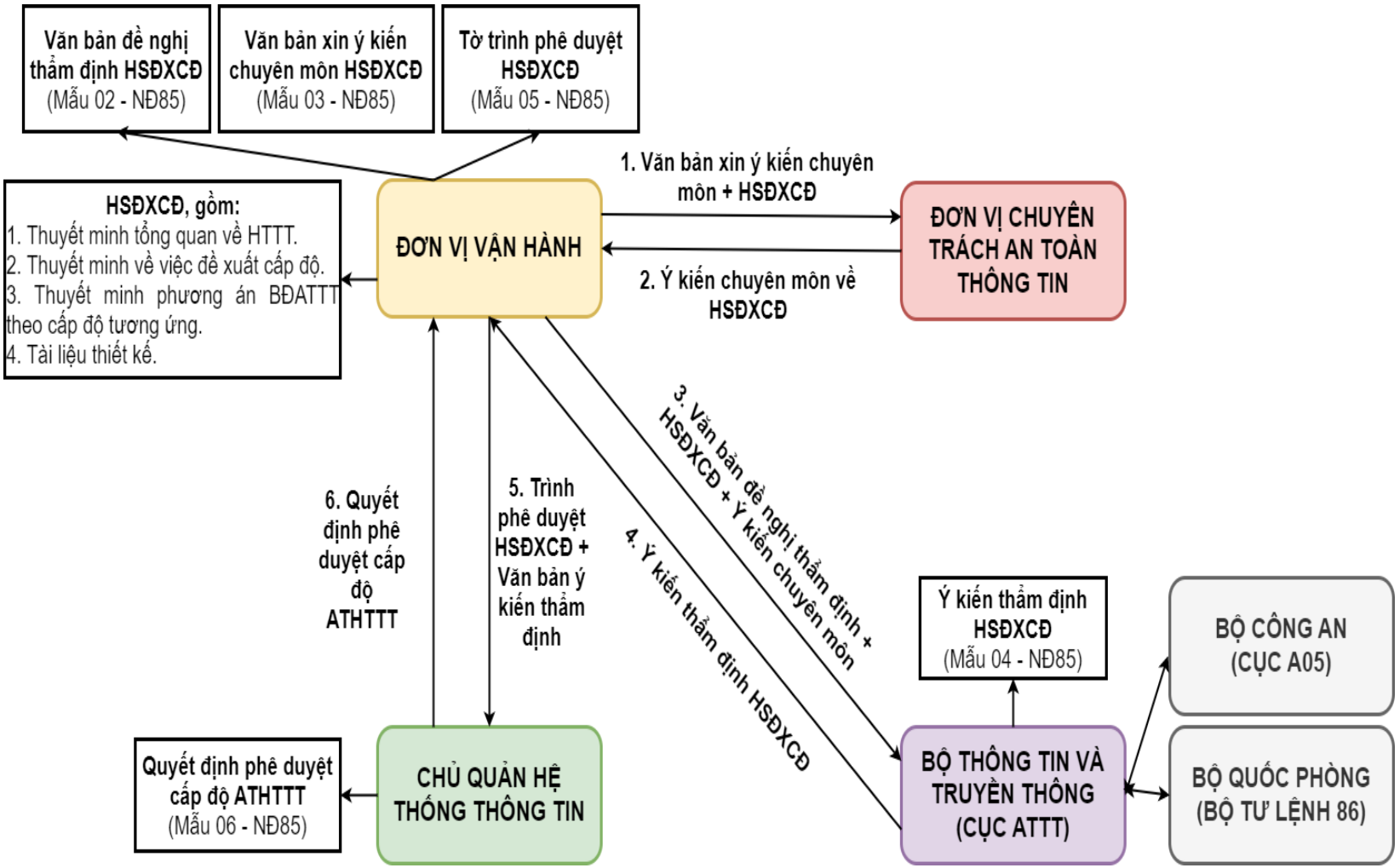
Thẩm định, phê duyệt hồ sơ đề xuất cấp độ (2)

Hệ thống thông tin được đề xuất cấp độ 3



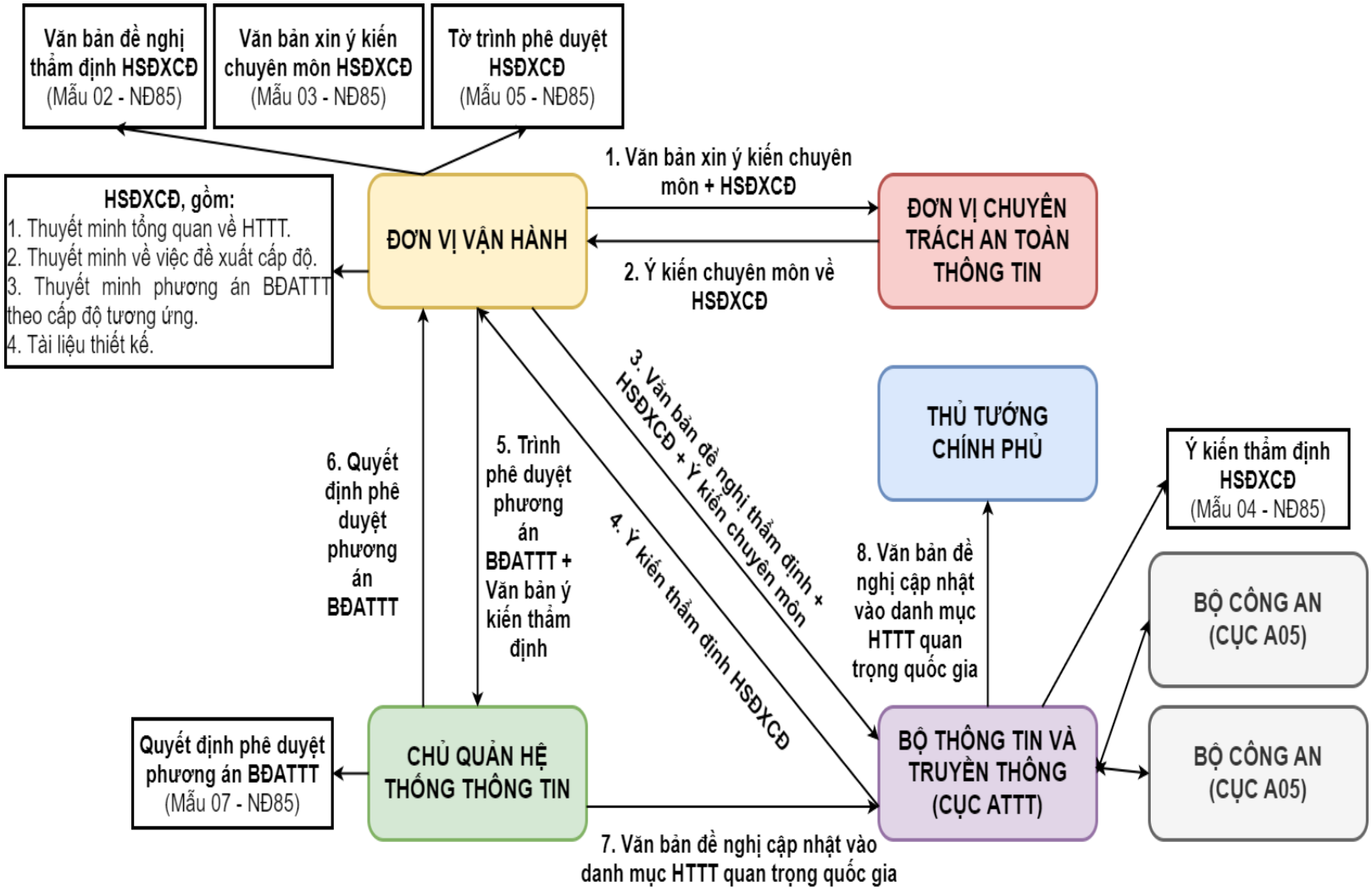
Thẩm định, phê duyệt hồ sơ đề xuất cấp độ (3)

Hệ thống thông tin được đề xuất cấp độ 4



Thẩm định, phê duyệt hồ sơ đề xuất cấp độ (4)

Hệ thống thông tin được đề xuất cấp độ 5



Xây dựng hồ sơ đề xuất cấp độ

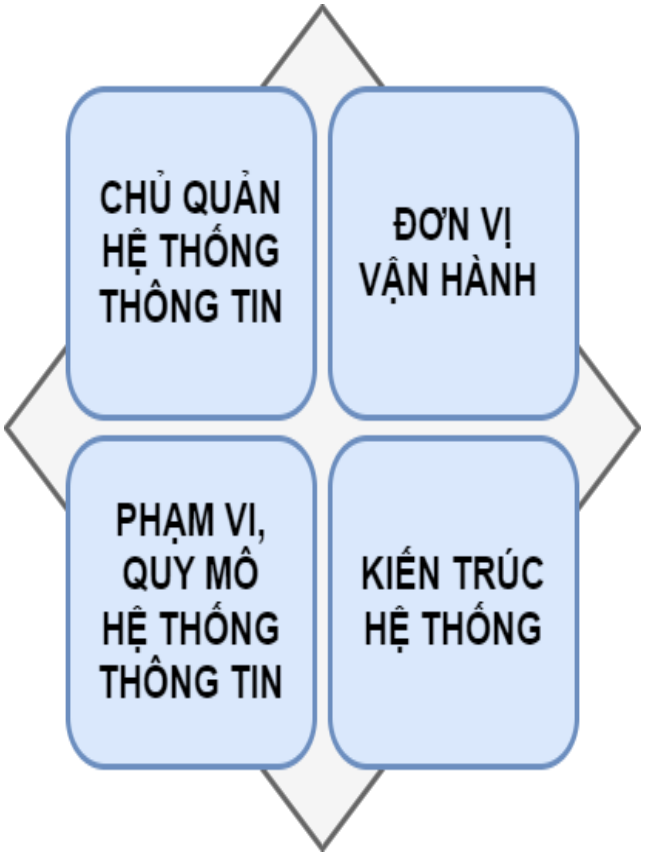
1. Thuyết minh tổng quan về hệ thống thông tin

2. Thuyết minh về việc đề xuất cấp độ

3. Thuyết minh phương án bảo đảm an toàn thông tin

Xây dựng hồ sơ đề xuất cấp độ (2)

Thuyết minh tổng quan về hệ thống thông tin (khoản 3 Điều 8 Thông tư 12/2022/TT-BTTTT):



1) Thông tin về chủ quản hệ thống thông tin, gồm: tên chủ quản hệ thống thông tin; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử).

2) Thông tin về đơn vị vận hành hệ thống thông tin, gồm: tên đơn vị vận hành; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử).

3) Mô tả phạm vi, quy mô của hệ thống thông tin, trong đó cần làm rõ phạm vi của hệ thống, quy mô của hệ thống và đối tượng phục vụ của hệ thống.

4) Mô tả hiện trạng kiến trúc hệ thống (đối với hệ thống đang vận hành) hoặc mô tả kiến trúc hệ thống (đối với hệ thống được xây dựng mới hoặc nâng cấp, mở rộng), trong đó mô tả cụ thể mô hình lô-gic, mô hình vật lý của hệ thống, danh mục thiết bị và thiết bị mạng chính trong hệ thống (bao gồm tên thiết bị/chủng loại, vị trí triển khai, mục đích sử dụng), danh mục ứng dụng/dịch vụ cung cấp bởi hệ thống (bao gồm tên dịch vụ, máy chủ triển khai/vị trí triển khai/hệ điều hành máy chủ, mục đích sử dụng dịch vụ), quy hoạch các vùng mạng và địa chỉ IP trong hệ thống (bao gồm vùng mạng, địa chỉ IP nội bộ (IP Private), địa chỉ IP công khai (IP Public)).

Xây dựng hồ sơ đề xuất cấp độ (3)

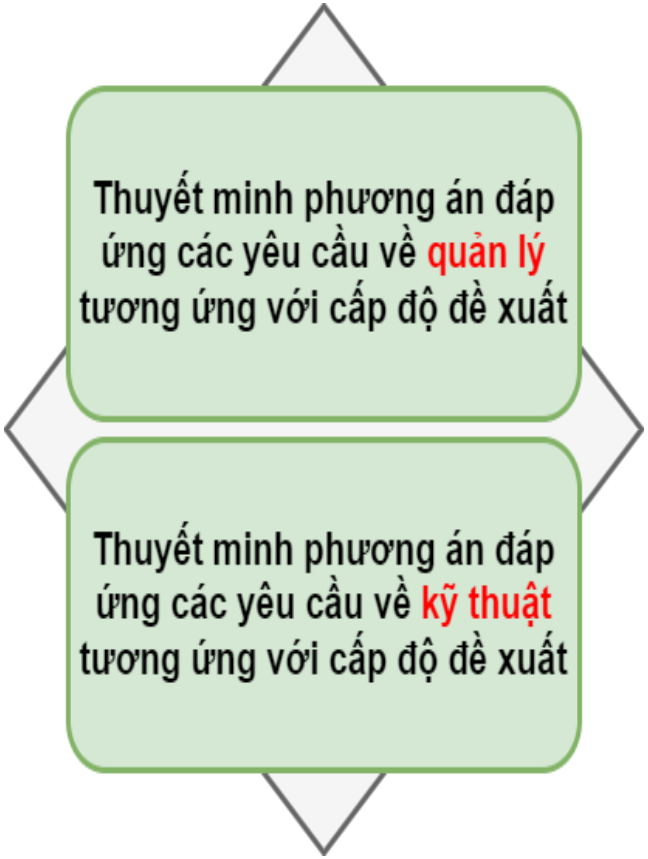
Thuyết minh về việc đề xuất cấp độ (khoản 4, 5 Điều 8 Thông tư 12/2022/TT-BTTTT):

1) Danh mục các hệ thống thông tin và cấp độ tương ứng, bao gồm: tên hệ thống thông tin, cấp độ đề xuất, căn cứ đề xuất đối với từng hệ thống thông tin.
2) Thuyết minh chi tiết đối với các hệ thống thông tin, trong đó cần làm rõ loại thông tin được xử lý, loại hệ thống thông tin, căn cứ đề xuất cấp độ đối với từng hệ thống thông tin.

3) Đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, cần làm rõ thêm các nội dung sau đây:
a) Xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất cấp độ;
b) Thuyết minh về các nguy cơ tấn công mạng và mức độ ảnh hưởng đối với hệ thống thông tin được đề xuất cấp độ;
c) Đánh giá phạm vi và mức độ ảnh hưởng tới lợi ích công cộng, trật tự an toàn xã hội hoặc quốc phòng, an ninh quốc gia khi bị tấn công mạng gây mất an toàn thông tin hoặc gián đoạn hoạt động của hệ thống thông tin được đề xuất cấp độ;
d) Thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước đối với các hệ thống thông tin theo quy định tại khoản 2 và khoản 3 Điều 10 của Nghị định 85/2016/NĐ-CP.

Xây dựng hồ sơ đề xuất cấp độ (4)

Thuyết minh phương án bảo đảm an toàn thông tin (khoản 6 Điều 8, Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT):



1) Yêu cầu cơ bản về quản lý, bao gồm:
a) Thiết lập chính sách an toàn thông tin;
b) Tổ chức bảo đảm an toàn thông tin;
c) Bảo đảm nguồn nhân lực;
d) Quản lý thiết kế, xây dựng hệ thống;
đ) Quản lý vận hành hệ thống;
e) Phương án Quản lý rủi ro an toàn thông tin;
g) Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

(Nội dung mới so với Thông tư 03/2017/TT-BTTT)

2) Yêu cầu cơ bản về kỹ thuật, bao gồm:
a) Bảo đảm an toàn mạng;
b) Bảo đảm an toàn máy chủ;
c) Bảo đảm an toàn ứng dụng;
d) Bảo đảm an toàn dữ liệu.

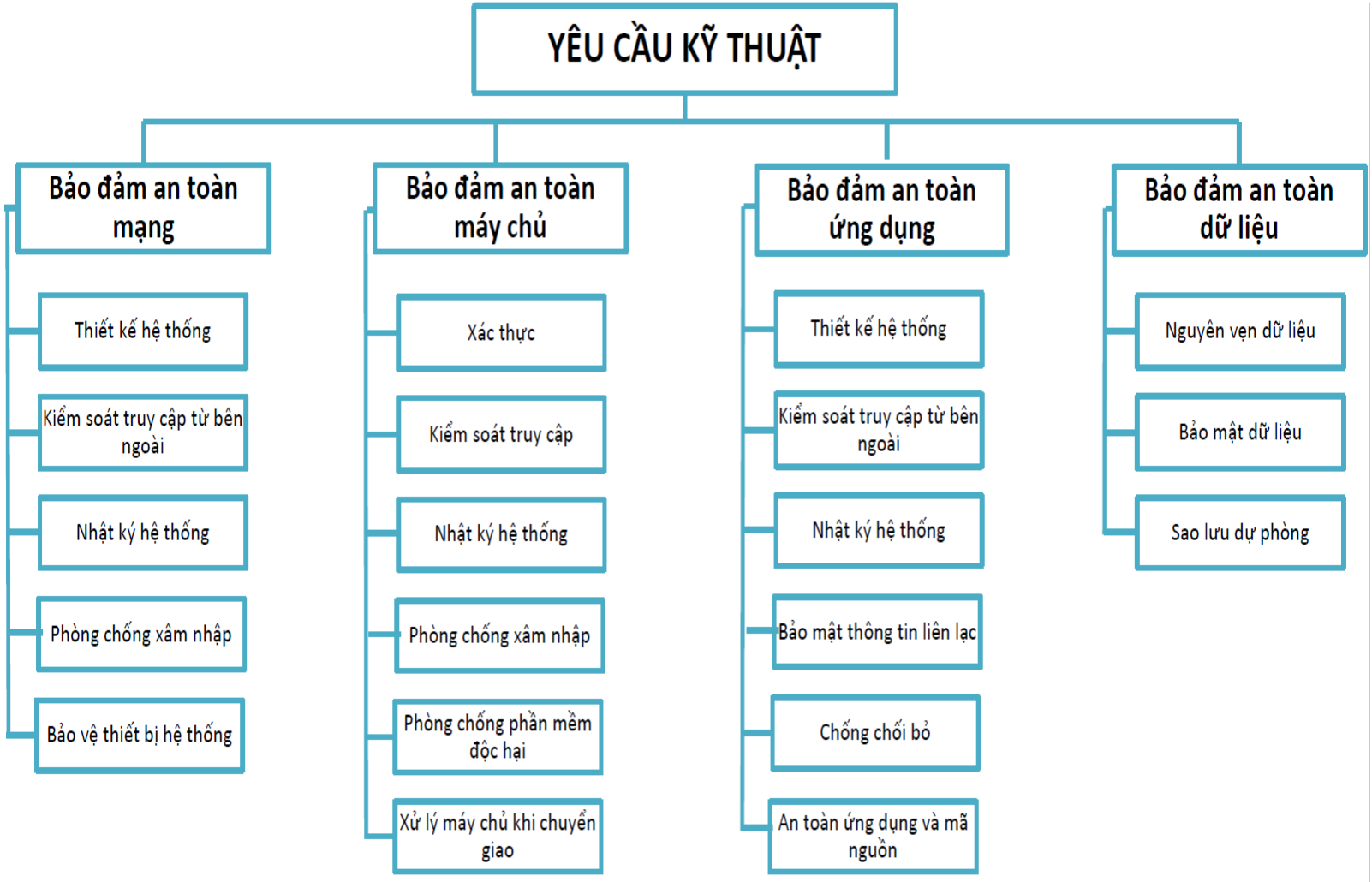
Chi tiết yêu cầu đối với từng cấp độ được quy định tại các Phụ lục I, II, III, IV, V Thông tư 12/2022/TT-BTTTT.

Xây dựng hồ sơ đề xuất cấp độ (5)

Thuyết minh phương án đáp ứng các yêu cầu về quản lý (đồng bộ với Tiêu chuẩn quốc gia TCVN 11930:2017):

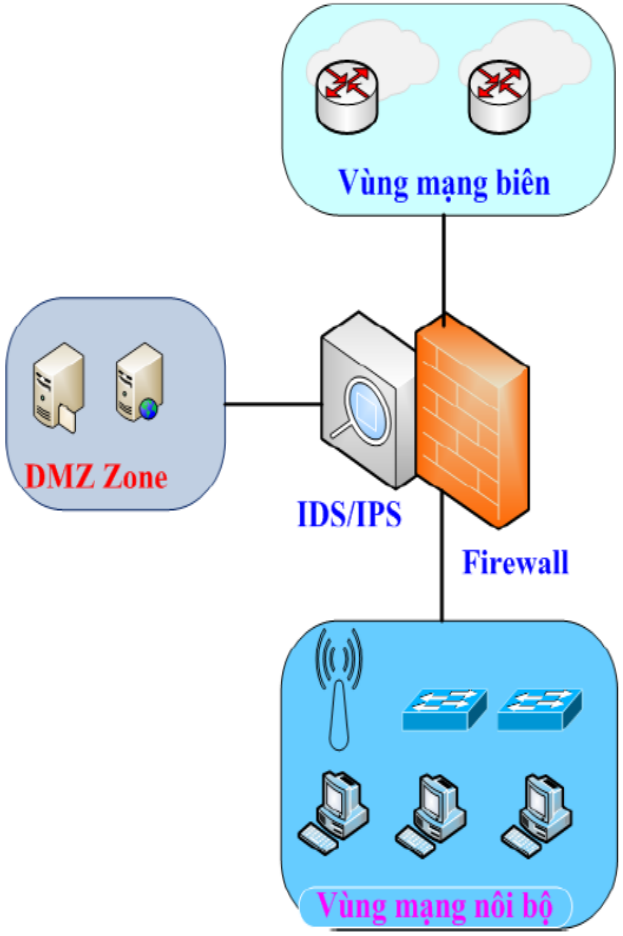
Xây dựng hồ sơ đề xuất cấp độ (6)

Thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật (đồng bộ với Tiêu chuẩn quốc gia TCVN 11930:2017



Phương án bảo vệ hệ thống thông tin

Hệ thống thông tin cấp độ 1: 03 phương án / 03 vùng mạng



Phương án thiết kế bảo đảm:

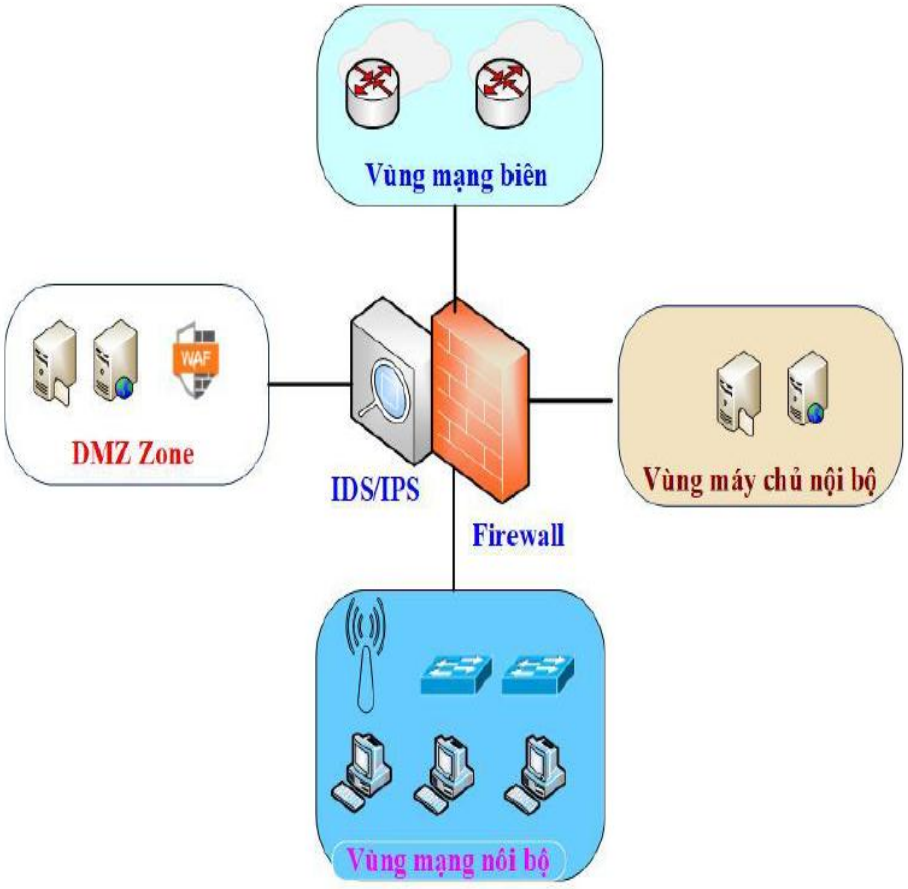
1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn.

2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập (FW tích hợp IDS/IPS)

3. Có phương án phòng chống mã độc cho máy chủ và máy trạm (AntiVirus)

Phương án bảo vệ hệ thống thông tin (2)

Hệ thống thông tin cấp độ 2: 06 phương án / 05 vùng mạng (vùng mạng không dây - nếu có)

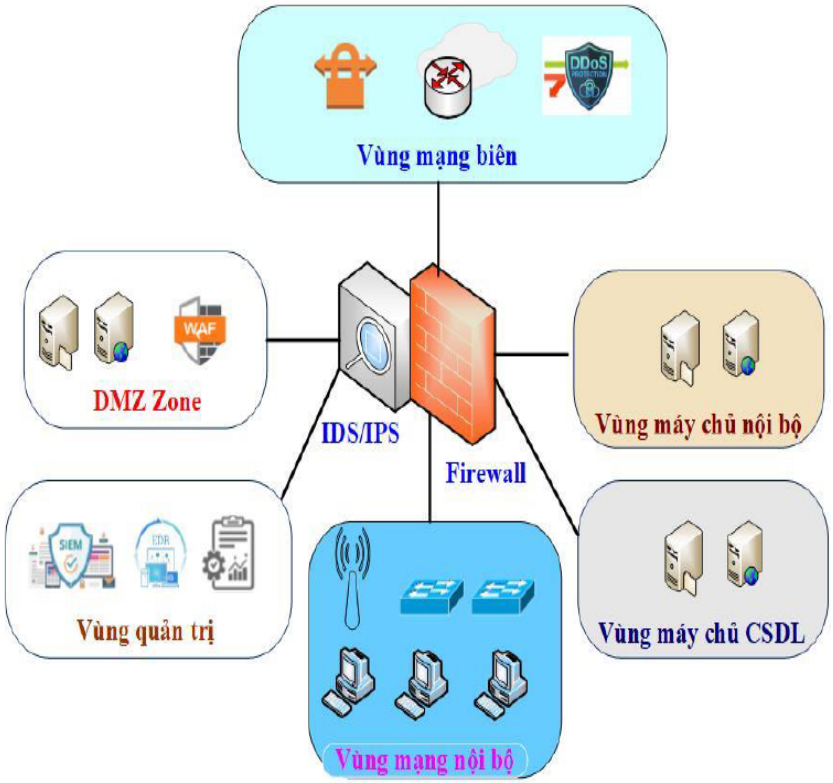


Phương án thiết kế bảo đảm:

1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn (Mạng riêng ảo VPN hoặc chức năng VPN tích hợp trên FW)
2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập (FW tích hợp IDS/IPS)
3. Có phương án phòng chống mã độc cho máy chủ và máy trạm (AntiVirus)
4. Có phương án phòng chống tấn công mạng cho ứng dụng web (WAF: HTTT được quy định tại khoản 2/Điều8/NĐ 85)
5. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử.
6. Có phương án dự phòng cho các thiết bị mạng chính

Phương án bảo vệ hệ thống thông tin (3)

Hệ thống thông tin cấp độ 3: 16 phương án / 07 vùng mạng (vùng mạng không dây - nếu có)



Phương án thiết kế bảo đảm:

1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn (SP Mạng riêng ảo VPN: HTTT xử lý thông tin bí mật nhà nước; HTTT tại điểm c khoản 3/9/NĐ 85).

2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập (FW tích hợp hoặc IDS/IPS).

3. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính

4. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu (FW CSDL đối với HT cơ sở dữ liệu tập trung tại khoản 3/9/NĐ 85).

5. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng (Giải pháp/Thiết bị phát hiện và ngăn chặn mã độc lớp mạng).

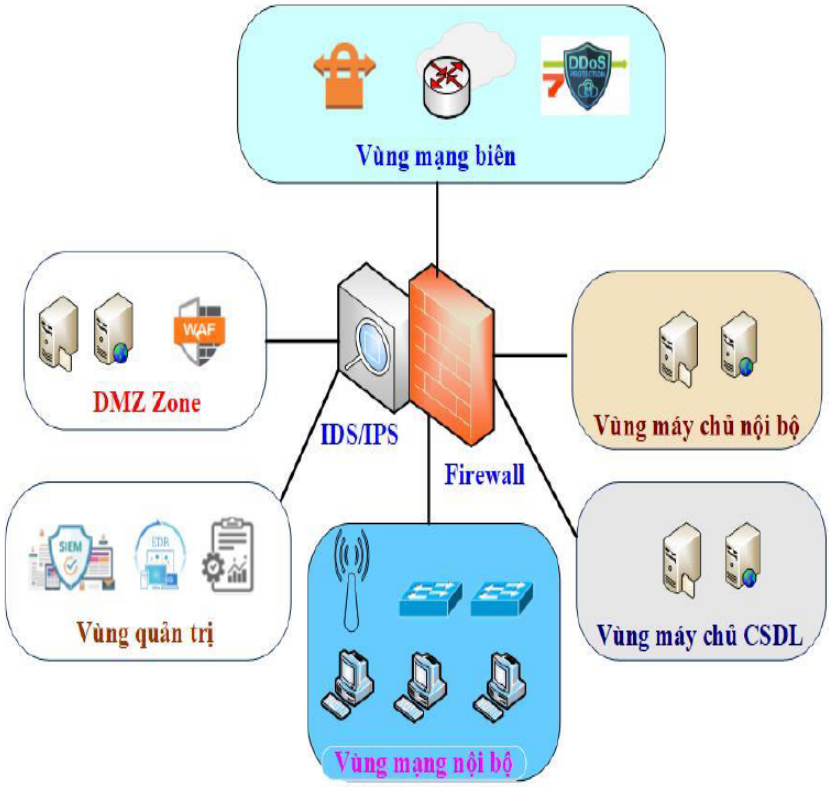
6. Có phương án phòng chống tấn công từ chối dịch vụ (Chống DDoS đối với các HT TTDL, Cloud, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu tại khoản 2/9/NĐ 85).

7. Có phương án phòng, chống tấn công mạng cho ứng dụng web (WAF được quy định tại khoản 2/9/NĐ 85)

8. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (Đối với HT Thư điện tử tại khoản 2/Điều 9/NĐ 85 – Giải pháp Email Security Gateway)

Phương án bảo vệ hệ thống thông tin (3)

Hệ thống thông tin cấp độ 3: 16 phương án / 07 vùng mạng (vùng mạng không dây - nếu có)

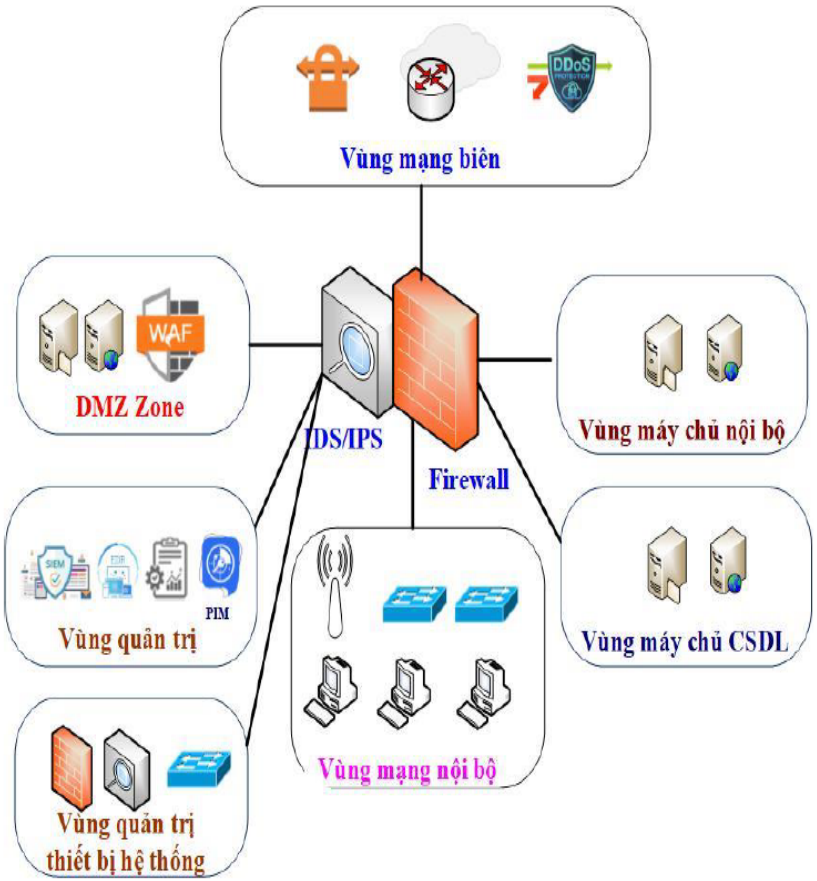


Phương án thiết kế bảo đảm:

9. Có phương án quản lý truy cập lớp mạng (SP NAC – Đối với HT Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng SOC tại khoản 3/Điều9/NĐ 85)
10. Có phương án giám sát hệ thống thông tin tập trung (Network monitoring NOC)
11. Có phương án giám sát an toàn hệ thống thông tin tập trung (SIEM)
12. Có phương án quản lý sao lưu dự phòng tập trung (Hệ thống lưu trữ và phần mềm quản lý)
13. Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung (Giải pháp AntiVirus có chức năng quản lý tập trung hoặc hệ thống EDR)
14. Có phương án phòng, chống thất thoát dữ liệu (DLP – Đối với HTTT có xử lý thông tin bí mật nhà nước hoặc HTTT quy định tại điểm c khoản 2/Điều9/NĐ 85)
15. Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (Có kết nối mạng Internet dự phòng)
16. Có phương án bảo đảm an toàn cho mạng không dây (nếu có)

Phương án bảo vệ hệ thống thông tin (4)

Hệ thống thông tin cấp độ 4: 17 phương án / 08 vùng mạng (vùng mạng không dây – nếu có)



Phương án thiết kế bảo đảm:

1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn (SP Mạng riêng ảo VPN: HTTT xử lý thông tin bí mật nhà nước).

2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập (FW tích hợp hoặc IDS/IPS).

3. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính

4. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu (FW CSDL đối với HT cơ sở dữ liệu tập trung tại khoản 3/10/NĐ 85).

5. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng (Giải pháp/Thiết bị phát hiện và ngăn chặn mã độc lớp mạng).

6. Có phương án phòng chống tấn công từ chối dịch vụ (Chống DDoS đối với các HT TTDL, Cloud, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu tại khoản 3/10/NĐ 85).

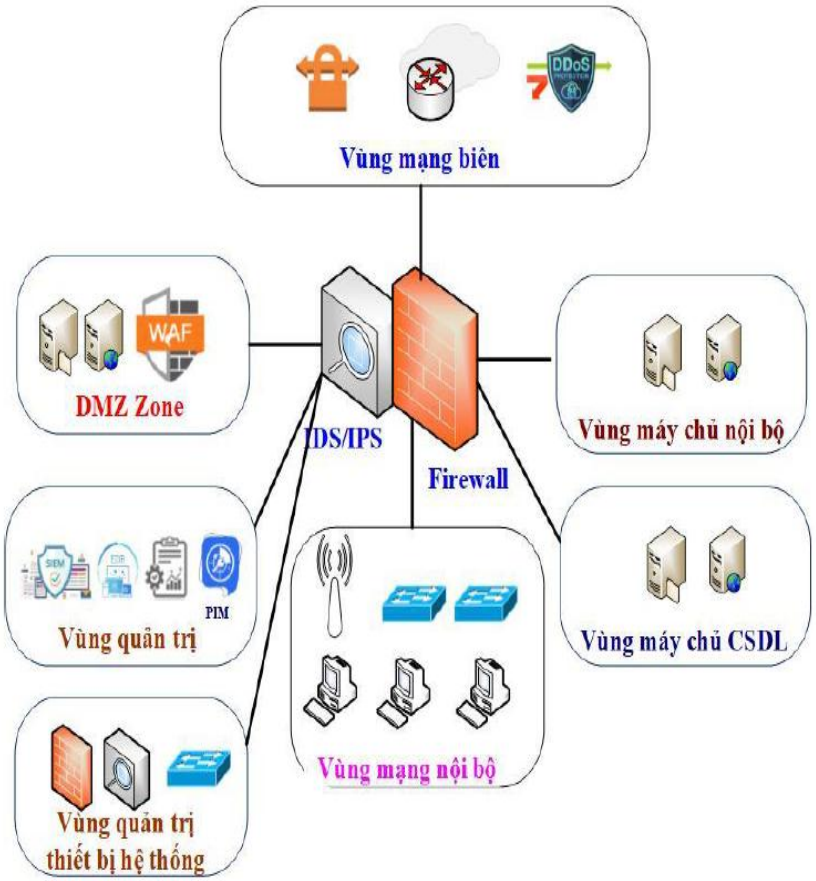
7. Có phương án phòng, chống tấn công mạng cho ứng dụng web (WAF được quy định tại khoản 2/10/NĐ 85)

8. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử

9. Có phương án quản lý truy cập lớp mạng (NAC – Đối với HT Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng SOC tại khoản 3 Điều 10/NĐ 85)

Phương án bảo vệ hệ thống thông tin (4)

Hệ thống thông tin cấp độ 4: 17 phương án / 08 vùng mạng (vùng mạng không dây – nếu có)



Phương án thiết kế bảo đảm:

10. Có phương án giám sát hệ thống thông tin tập trung (Network monitoring NOC)

11. Có phương án giám sát an toàn hệ thống thông tin tập trung (SIEM)

12. Có phương án quản lý sao lưu dự phòng tập trung (Hệ thống lưu trữ và phần mềm quản lý)

13. Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung (Giải pháp AntiVirus có chức năng quản lý tập trung hoặc hệ thống EDR)

14. Có phương án phòng, chống thất thoát dữ liệu (DLP – Đối với HTTT có xử lý thông tin bí mật nhà nước hoặc HTTT quy định tại khoản 3 Điều 10/NĐ 85)

15. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ

16. Có phương án bảo đảm an toàn cho mạng không dây (nếu có)

17. Có phương án quản lý tài khoản đặc quyền (PIM/PAM Privileged Access Management)

Bảo đảm an toàn hệ thống thông tin theo cấp độ

Phương án bảo vệ hệ thống thông tin (5)

Hệ thống thông tin cấp độ 5: 19 phương án / 08 vùng mạng (vùng mạng không dây – nếu có+vùng quản trị thiết bị hệ thống)

Phương án thiết kế bảo đảm:

1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn (SP Mạng riêng ảo VPN: HTTT xử lý thông tin bí mật nhà nước).
2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập (FW tích hợp hoặc IDS/IPS).
3. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng
4. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu (FW CSDL đối với HT cơ sở dữ liệu tập trung tại khoản 2/11/NĐ 85).
5. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng (Giải pháp/Thiết bị phát hiện và ngăn chặn mã độc lớp mạng).
6. Có phương án phòng chống tấn công từ chối dịch vụ (SD dịch vụ của DN hoặc SP Chống DDoS đối với các HTTT quy định tại khoản 2, 3/10/NĐ 85).
7. Có phương án phòng, chống tấn công mạng cho ứng dụng web (WAF được quy định tại khoản 2/11/NĐ 85)
8. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử
9. Có phương án quản lý truy cập lớp mạng (NAC – Đối với HT Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng SOC tại khoản 3 Điều 10/NĐ 85)

Bảo đảm an toàn hệ thống thông tin theo cấp độ

Phương án bảo vệ hệ thống thông tin (5)

Hệ thống thông tin cấp độ 5: 19 phương án / 08 vùng mạng (vùng mạng không dây – nếu có+vùng quản trị thiết bị hệ thống)

Phương án thiết kế bảo đảm:

10. Có phương án giám sát hệ thống thông tin tập trung (Network monitoring NOC)
11. Có phương án giám sát an toàn hệ thống thông tin tập trung (SIEM)
12. Có phương án quản lý sao lưu dự phòng tập trung (Hệ thống lưu trữ và phần mềm quản lý)
13. Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung (Giải pháp AntiVirus quản lý tập trung hoặc hệ thống EDR)
14. Có phương án phòng, chống thất thoát dữ liệu (DLP – Đối với HTTT có xử lý thông tin bí mật nhà nước hoặc HTTT quy định tại khoản 2/Điều 11/NĐ 85)
15. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ.
16. Có phương án bảo đảm an toàn cho mạng không dây (nếu có)
17. Có phương án quản lý tài khoản đặc quyền (PAM (Privileged Access Management))
18. Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau 19. Có phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng (Có kết nối vật lý theo hai hướng khác nhau giữa hai hệ thống.)


HỎI ?
& ĐÁP