SỞ Y TẾ TỈNH LÂM ĐỒNG

BỆNH VIỆN PHỤC HỒI CHỨC NĂNG

PHƯƠNG ÁN

CẢNH BÁO VÀ CHỐNG TẤN CÔNG CÓ CHỦ ĐÍCH ĐỐI VỚI CÁC HỆ THỐNG CUNG CẤP DỊCH VỤ QUA INTERNET TẠI BỆNH VIỆN PHỤC HỒI CHỨC NĂNG TỈNH LÂM ĐỒNG

(Ban hành kèm theo Quyết định số /QĐ-PHCN ngày ..... tháng .... năm 2025)

Lâm Đồng, tháng ..... năm 2025

PHƯƠNG ÁN CẢNH BÁO VÀ CHỐNG TẤN CÔNG CÓ CHỦ ĐÍCH ĐỐI VỚI CÁC HỆ THỐNG CUNG CẤP DỊCH VỤ QUA INTERNET CỦA BỆNH VIỆN PHỤC HỒI CHỨC NĂNG TỈNH LÂM ĐỒNG

I. MỤC ĐÍCH YÊU CẦU

1. Mục đích

- Xây dựng phương án cảnh báo và chống tấn công có chủ đích để bảo đảm an toàn thông tin mạng của đơn vị, trong đó tập trung an toàn thông tin cho các hệ thống thông tin quan trọng của đơn vị, có khả năng thích ứng một số cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng.

- Đề ra các cơ chế, cảnh báo và phòng ngừa tấn công có chủ đích đối với các hệ thống cung cấp dịch vụ qua internet của bệnh viện.

- Nâng cao năng lực, hiệu quả hoạt động của đơn vị CNTT ứng cứu sự cố an toàn thông tin mạng nội bộ, gắn kết với các đơn vị cung cấp phần mềm, hợp tác, kết nối chặt chẽ, điều phối kịp thời, phối hợp đồng bộ, hiệu quả của các lực lượng để ứng cứu sự cố mạng, chống tấn công mạng.

- Nâng cao nhân lực cho cán bộ, nhân viên, người lao động đơn vị khi tham gia khai thác, sử dụng các hệ thống thông tin của đơn vị;

- Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng.

2. Yêu cầu

- Phải khảo sát, đánh giá hiện trạng hạ tầng công nghệ thông tin tại đơn vị để đưa ra các giải pháp hiệu quả nhất nhằm đảm bảo an toàn thông tin hệ thống thông tin của đơn vị.

- Cơ chế cảnh báo phải kịp thời, hiệu quả cao nhất đối với hệ thống thông tin của đơn vị.

- Đưa ra các giải pháp cụ thể để phòng chống các cuộc tấn công có chủ đích nhắm vào hệ thống thông tin của đơn vị

II. MỘT SỐ KHÁI NIỆM CƠ BẢN VỀ TẤN CÔNG CÓ CHỦ ĐÍCH

1. Khái niệm về tấn công có chủ đích

Tấn công có chủ đích APT (Advanced Persistent Threat) được dùng để chỉ kiểu tấn công dai dẳng có chủ đích vào một thực thể. Kẻ tấn công có thể được hỗ trợ bởi một tổ chức, cá nhân nào đó nhằm tìm kiếm thông tin của một tổ chức, cá nhân khác.

2. Mục đích của tấn công có chủ đích:

- Thu thập thông tin tình báo có tính chất thù địch.

- Đánh cắp dữ liệu và bán lại bí mật kinh doanh cho các đối thủ;
- Làm mất uy tín của cơ quan tổ chức, đơn vị;
- Phá hoại, gây bất ổn hạ tầng CNTT, viễn thông;

3. Các phương thức tấn công có chủ đích:

- Tấn công bị động (Passive attack);
- Tấn công rải rác (Distributed attack);
- Tấn công nội bộ (Insider attack);
- Tấn công Phishing;
- Các cuộc tấn công của không tặc (Hijack attack);
- Tấn công mật khẩu (Password attack);
- Khai thác lỗ hổng tấn công (Exploit attack);
- Lỗi tràn bộ đệm (Buffer overflow);
- Tấn công từ chối dịch vụ (Denial of service attack);
- Tấn công theo kiểu Man-in-the-Middle Attack;
- Tấn công phá mã khóa (Compromised-key Attack);
- Tấn công trực tiếp;
- Nghe trộm;
- Giả mạo địa chỉ;
- Vô hiệu hóa các chức năng của hệ thống;
- Lỗi của người quản trị hệ thống;
- Tấn công vào yếu tố con người.

III. CÁC GẢI PHÁP PHÒNG NGỪA TÁN CÔNG CÓ CHỦ ĐÍCH

- Tấn công APT (Advanced Persistent Threat) là hình thức tấn công mạng có mục tiêu cụ thể do tin tặc chọn, sử dụng các công nghệ tiên tiến và kỹ thuật lừa đảo để đột nhập mạng mục tiêu và dai dẳng tập trung vào mục tiêu đó trong nhiều tuần, nhiều tháng hoặc nhiều năm cho đến khi cuộc tấn công diễn ra thành công (hoặc bị chặn đứng). Một khi vào được trong mạng, tin tặc cố giấu mình để không bị phát hiện trong khi sử dụng một số loại phần mềm độc hại (malware) để đánh cắp thông tin quan trọng.

- Các cuộc tấn công ATP được tổ chức chặt chẽ, có nguồn lực tài chính và công nghệ dồi dào. Tuy có thể sử dụng các công cụ đột nhập thông thường, nhưng thường thì các cuộc tấn công ATP sử dụng phần mềm tùy biến tinh vi khó bị hệ thống bảo mật phát hiện. Từ những đánh giá mức độ nguy hiểm của tấn công APT,

để phòng ngừa tấn công có chủ đích và hệ thống thông tin, Bệnh viện Y học cổ truyền Phạm Ngọc Thạch đã triển khai các giải pháp cụ thể sau:

1. Triển khai phòng thủ theo chiều sâu

- Hệ thống hạ tầng CNTT của Bệnh viện được bảo vệ theo chiều sâu, phân thành nhiều tầng và tách thành nhiều lớp khác nhau. Mỗi tầng và lớp đó sẽ được thực hiện các chính sách bảo mật hay ngăn chặn khác nhau. Mặt khác cũng là để phòng ngừa khi một tầng hay một lớp nào đó bị xâm nhập thì xâm nhập trái phép đó chỉ bó hẹp trong tầng hoặc lớp đó thôi và không thể ảnh hưởng sang các tầng lớp khác.

- Phòng thủ theo chiều sâu hay bảo mật theo lớp không thể thiếu trong chiến lược an ninh mạng, đây là một trong những phương pháp tốt nhất để ngăn chặn cuộc tấn công mạng ATP. Nó có nghĩa kiểm soát các điểm ra vào mạng, sử dụng tường lửa thế hệ mới, triển khai các hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS) hệ thống giám sát thông tin và sự cố bảo mật (SIEM), bổ sung hệ thống quản lý lỗ hổng, sử dụng phương thức xác thực quản lý danh tính chắc chắn, cập nhật các bản vá và bảo mật và thực hiện bảo vệ đầu cuối.

1.1. Giải pháp về quy hoạch thiết kế hạ tầng

Bệnh viện Phục hồi chức năng tỉnh Lâm Đồng đã triển khai thiết kế, quy hoạch hệ thống mạng nội bộ hiện đại kết nối thông suốt đến các phòng, khoa trong toàn Bệnh viện đáp ứng đầy đủ nhu cầu khai thác sử dụng của bệnh viện, đặc biệt chú trọng đến vấn đề an toàn an ninh thông tin của hệ thống:

a. Thiết kế cơ sở hạ tầng theo mô hình tổng thể

Thiết kế tổng thể hệ thống CNTT của đơn vị đáp ứng yêu cầu về quản lý, giám sát, lưu trữ, chia sẻ dữ liệu đáp ứng được các yêu cầu về công tác chuyên môn, nghiệp vụ, quản lý, điều hành và đảm bảo an toàn an ninh thông tin cho Bệnh viện.

b. Kiến trúc hệ thống mạng Bệnh viện:

- Kiến trúc mạng Bệnh viện được thiết kế theo mô hình đa tầng phân cấp chuẩn (3 lớp: core layer, distribbution layer, access layer) và sử dụng công cụ mạng tiên tiến như dịch vụ Backup, VLAN... nhằm đảm bảo tính sẵn sàng, tính phân quyền tăng tốc đường truyền ....

- Hệ thống mạng LAN của Bệnh viện là hệ thống có đường truyền băng thông cao và có thể kết nối với hệ thống khác để thành hệ thống mạng WAN đáp ứng nhu cầu sử dụng của bệnh viện. Hệ thống mạng thiết kế tuân thủ nguyên tắc mạng khách và mạng nội bộ.

- Bệnh viện đã triển khai các giải pháp đảm bảo an toàn, bảo mật hệ thống và các dữ liệu nhạy cảm của Bệnh viện, cụ thể như sau:

+ Cài đặt chương trình diệt virus

+ Lập dự toán lắp đặt trang thiết bị hệ thống firewall chuyên dụng; (triển khai giai đoạn 2)

+ Triển khai hệ thống VPN server cho phép người dùng có thể truy cập vào hệ thống của Bệnh viện thông qua kết nối VPN đảm bảo an toàn và bảo mật;

+ Triển khai hệ thống Gateway kết nối internet (Bảo vệ và kiểm soát kết nối từ bên ngoài vào và từ bên trong ra ngoài internet).

1.2. Giải pháp ngăn chặn phát hiện tấn công có chủ đích

- Để đảm bảo cơ chế bảo mật nhằm ngăn chặn phát hiện các cuộc tấn công có chủ đích vào hệ thống mạng thông tin. Hệ thống mạng của Bệnh viện được tổ chức thành nhiều nhóm mạng tách biệt như:

+ Lớp mạng bên ngoài (Outside network) các giao tiếp giữa hệ thống mạng Bệnh viện và bên ngoài đều được kết nối với các thiết bị router chuyên dụng có khả năng lọc gói tin, ánh xạ địa chỉ IP .... tạo ra một cấp tường lửa (Firewall) cho hệ thống;

+ Các máy tính bên ngoài chỉ được truy cập thông tin của Bệnh viện trên các server dịch vụ được thiết lập trong một thiết bị mạng khác. Nhằm đảm bảo tính an toàn cho các database server chính trong hệ thống;

+ Lớp trong (Inside network): các giao tiếp giữa các máy tính và các Server database của Bệnh viện đều phải qua thiết bị Routing switch Bệnh viện cũng được bảo vệ bằng kỹ thuật firewall (tích hợp sẵn trong thiết bị) tạo nên một vành đai an toàn bảo vệ dữ lệu của hệ thống. Ngoài ra giữa các khu vực kết nối có thiết lập các VLAN tách biệt đảm bảo an toàn cho hệ thống;

+ Backbone của hệ thống được đấu nối tập trung về một thiết bị Routing switch layer 3 tạo thành một core network;

- Hệ thống đã triển khai hệ thống Firewall đảm bảo an toàn cho hệ thống (Unifi security Gateway) sẽ áp dụng chính sách bảo mật hệ thống:

+ Lọc gói (Packet Filtering) đây là phương pháp ứng dụng phổ biến nhất. Firewall này nhận gói tin từ Internet, kiểm tra thông tin về địa chỉ IP trong phần tiêu đề gói tin và đối chiếu với danh sách cho phép truy cập để xác định xem gói tin đó được chấp nhận hay từ chối.

+ Kiểm tra trạng thái sâu (Deep packet Inspection): Đây là giải pháp Firewall tinh lọc gói cấp cao nó kiểm tra cả tiêu đề và thông tin gói tin để xác định chi tiết hơn đi ngoài thông tin về địa chỉ nguồn và địa chỉ đích. Đây là cách đảm bảo tất cả các phiên truyền thông tin được khởi tạo bởi máy tính đích và diễn ra chỉ với những nguồn đã biết và tin cậy. Biện pháp này giúp tăng cường khả năng chống các hành động tấn công quét cổng.

2. Triển khai hệ thống giám sát phát hiện và chống xâm nhập

Giám sát chặt chẽ việc kiểm soát an ninh giúp nhận diện các dấu hiệu cảnh báo sớm của một cuộc tấn công APT, thường xuất hiện dưới dạng file log và lưu lượng dữ liệu bất thường, hay các hoạt động bất thường khác. Việc giám sát tất cả các lưu lượng ra vào mạng, lưu lượng nội bộ và tất cả các thiết bị truy cập mạng là hết sức quan trọng. việc giám sát liên tục không chỉ giúp phát hiện hoạt động đáng ngờ sớm nhất có thể mà còn làm giảm khả năng các cuộc xâm nhập leo thang hoặc kéo dài. Kết quả giám sát còn có thể dùng làm chứng chỉ pháp lý nếu cuộc tấn công xảy ra.

2.1. Quản lý danh sách điều khiển truy xuất, an toàn công thiết bị, lọc địa chỉ mạng

** Danh sách điều khiển truy xuất*

Danh sách truy nhập là gồm các luật cho phép hay ngăn chặn các gói tin sau lần khi tham chiếu vào thông tin trong tiêu đề của gói tin để giới hạn các người dùng hiển có thể truy xuất vào các hệ thống nội bộ, v.v…

**Bảo mật cổng của thiết bị, lọc địa chỉ vật lý của thiết bị mạng*

- Ở các điểm truy cập mạng công cộng, việc mở rộng LAN của người dùng; việc truy xuất vào các máy chủ nội bộ cần được kiểm soát.

- Các giải pháp như cấu hình bảo mật cổng của thiết bị, quản lý địa chỉ vật lý là giải pháp cực kỳ an ninh và hiệu quả trong trường hợp này.

- Cấu hình bảo mật cổng của thiết bị trên các switch nhằm đảm bảo không thể mở rộng LAN khi chưa có sự đồng ý của người quản trị hệ thống, nếu vi phạm điều đó, port trên switch đó sẽ chuyển về trạng thái cấm hoặc trạng thái ngừng hoạt động.

- Địa chỉ vật lý là địa chỉ được cài đặt sẵn từ nhà sản xuất. về nguyên tắc tất cả các máy tính trên mạng sẽ không trùng nhau về địa chỉ này. Sự kiểm soát theo địa chỉ này là rất cụ thể tới từng máy tính trong mạng, trừ khi người dùng có quyền cài đặt phần mềm và làm giả địa chỉ này ở máy tính đó, hoặc là mở máy tính rồi thay thế địa chỉ giao tiếp mạng mới.

2.2. Một số giải pháp khác

2.2.1. Xây dựng hệ thống cập nhật sửa lỗi tập trung

- Công đoạn đầu tiên của hacker khi tiến hành tấn công có chủ đích là khảo sát hệ thống đích để tìm ra các lỗi của hệ điều hành, của các ứng dụng khi chúng chưa được cập nhật trên website của nhà cung cấp.

- Thực trạng ở các cơ quan, đơn vị nói chung, tại Bệnh viện Y học cổ truyền Phạm Ngọc Thạch nói riêng cho thấy việc sử dụng các sản phẩm phần mềm hầu

như ít Tin cập nhật các bản vá lỗi, có chăng cũng đang riêng lẽ trên các máy tính cá nhân, chưa đồng bộ, đó chính là cơ hội cho hacker dùng các công để khai thác lỗ hổng bảo mật. Để cập nhật bản vá lỗi cho tất cả các máy khách trong toàn bộ hệ thống qua internet mất thời gian và tốn nhiều băng thông đường truyền và không thống nhất.

- Đơn vị triển khai giải pháp xây dựng hệ thống tự động cập nhật từ nhà cung cấp trên Internet về máy chủ rồi từ máy chủ này, triển khai cho tất cả các máy khách trong toàn mạng, mặt khác các cán bộ kỹ thuật thường xuyên theo dõi để cập nhật kịp thời những bản vá trên các hệ điều hành đảm bảo hệ thống máy chủ máy trạm luôn được an toàn.

- Hệ thống WSUS (Windows Server Update Services) của Microsoft không những cập nhật bản vá lỗi cho tất cả các sản phẩm khác của hãng bao gồm Internet Explorer, SQL server, Office, Mail; máy chủ Web.

2.2.2. Ghi nhật ký, theo dõi, giám sát hệ thống

a) Ghi nhật ký

- Giải pháp ghi lại các phiên bản kết nối, các phiên bản đăng nhập của người dùng, các tiến trình hoạt động sẽ giúp quản trị mạng có thể tìm lại dấu vết người dùng, hacker và các lỗi gây ra cho hệ thống trước đó. Các máy chủ Web, máy chủ ứng dụng khác đã được khích hoạt tính năng ghi nhật ký, việc quản lý lưu trữ các làm thông tin này là rất cần thiết.

- Chính vì triển khai hệ thống ghi nhật ký tập trung lại một máy chủ chuyên dụng khác là rất hiệu quả. Hệ thống sẽ giúp chúng ta ghi các cảnh báo, thông báo từ các thiết bị cứng như: tường lửa, router, switch, từ các máy chủ web, database và các hệ thống khác.

b) Theo dõi, giám sát

- Theo dõi, giám sát là công việc thưởng xuyên và quan trọng của nhà quản trị mạng chuyên nghiệp, đó chính là công việc phòng chống hiệu quả trước khi sự cố xuất hiện. Theo dõi, giám sát có thể:

+ Phát hiện trên hệ thống mạng có nhiều virus phát tán.

+ Giám sát các máy trính trong mạng LAN và trên môi trường Internet.

+ Theo dõi hiệu năng hoạt động các phần cứng của máy chủ để tiến hành nâng cấp, bảo trì, bảo dưỡng.

+ Phát hiện các công cụ nghe lén mật khẩu, quét các lỗi của hệ thống và các ứng dụng.

+ Thống kê số lượng các kết nối, các session cũng như các lưu lượng bất thường trên hệ thống mạng, v.v…

2.2.3. Giải pháp mã hóa dữ liệu và đường truyền

- Dữ liệu trên máy chủ, máy tính cá nhân của Bệnh viện đã được mã hóa nội dung trước khi đưa vào lưu trữ và cả khi đi trên đường truyền.

- Tại các máy chủ và máy tính có thể lưu trữ dữ liệu quan trọng, có dữ liệu cần chia sẻ; tại các thiết bị lưu trữ cần thiết phải tiến hành mã hóa nội dung, điều đó đảm bảo rằng nếu có thể mất thiết bị lưu trữ, máy tính, người tấn công cũng không thể giải mã được dữ liệu.

- Giải pháp Ipsec sẽ được triển khai tại các hệ thống máy chủ và người dùng cũng như các thiết bị mạng phải được cấu hình.

3. Sử dụng dịch vụ đánh giá, phân tích mối đe dọa

Từ các giải pháp đã đưa ra ở trên để phòng chống tấn công có chủ đích; đơn vị Công nghệ thông tin Bệnh viện thường xuyên theo dõi giám sát tình hình hoạt động của hệ thống mạng, máy chủ, máy trạm cũng như các thiết bị khác để từ đó đưa ra các phân tích, đánh giá về các mối đe dọa tấn công vào hệ thống của trung tâm, từ đó lập kế hoạch xử lý các tình huống cụ thể để phòng chống các tấn công có chủ đích vào hệ thống.

4. Lập kế hoạch ứng phương án phòng chống tấn công có chủ đích đối với hệ thống thông tin tại Bệnh viện

Dù có đầu tư trang thiết bị với những công nghệ đắt tiền thì việc bảo mật của Bệnh viện vẫn đứng trước nguy cơ bị tấn công. Do đó phải xây dựng một kế hoạch ứng phó sự cố nhằm dập tắt các cuộc tấn công, giảm thiểu thiệt hại và chặn bớt rò rỉ dữ liệu, giảm thiểu tổn hại uy tín, thiệt hại của đơn vị. Cụ thể tại Bệnh viện đã triển khai các quy chế, cơ chế cảnh báo, phương án phòng ngừa các sự cố về CNTT tại Bệnh viện.

STT	Tình huống	Cách phòng ngừa
Tình huống sự cố do bị tấn công mạng		
1.	Tấn công Phishing (hay tấn công giả mạo): là hình thức tấn công mạng phổ biến khi kẻ tấn công làm giả Website của một đơn vị uy tín để lừa đảo người dùng nhập thông tin.	- Kiểm tra kỹ các email, tin nhắn, đường link website trước khi thực hiện nhập thông tin. - Cài đặt các phần mềm cảnh báo, quét mã độc cho Website. - Cảnh giác với website sử dụng HTTP (kém an toàn) thay vì HTTPS (an toàn hơn).
2.	Tấn công mạng từ bên trong: tin tặc có thể cài phần mềm gián điệp vào máy tính cá nhân của các thành viên trong công ty, hoặc lấy	- Hạn chế sử dụng mạng wifi công cộng bởi chúng có thể khiến thiết bị nhiễm mã độc.

	được tài khoản và mật khẩu của nhân viên sau đó thực hiện hành vi tấn công của mình.	- Đặt mật khẩu phức tạp để tránh các cuộc tấn công Password. - Bật tính năng xác thực 2 lớp qua tin nhắn.
3.	Tấn công gián tiếp: Tin tặc có thể tấn công một đối tượng thông qua việc tấn công một đối tác của đối tượng đó. Điển hình là tấn công chuỗi cung ứng.	- Sử dụng Firewall và các chương trình diệt Virus, Malware. - Luôn kiểm tra dữ liệu vào – ra. - Lựa chọn các sản phẩm ứng dụng có nguồn gốc rõ ràng đảm bảo độ tin cậy.
4.	Tấn công theo tệp đính kèm: File đính kèm email, tệp đính kèm tin nhắn facebook là những công cụ tấn công mạng phổ biến của tin tặc, sau khi người dùng click vào tệp đính kèm sẽ lập tức dính virus, gây nhiều hậu quả nghiêm trọng.	- Người sử dụng email: luôn kiểm tra người gửi, không dowload các tệp tin không rõ nguồn gốc. - Với mạng xã hội và các dịch vụ khác: khuyến cáo người sử dụng tải file đính kèm không rõ nguồn gốc
5.	Tấn công truy cập trái phép, chiếm quyền điều khiển: truy cập vào dữ liệu, chiếm đoạt truy cập và leo thang đặc quyền.	- Với kiểu tấn công vào mật khẩu: + Đặt mật khẩu mạnh: Không sử dụng mật khẩu dễ đoán liên quan đến cá nhân, cả khi lưu trữ hoặc truyền trên mạng. + Trong các khuyến nghị về chính sách an ninh mạng, đều yêu cầu phải ghi lại nhật ký hệ thống, bằng cách xem xét các bản ghi nhật ký. Admin có thể biết được các thông tin về số lần truy cập không thành công. Nếu phát hiện từ một địa chỉ IP có số lần truy cập không thành công vượt quá giới hạn cho phép thì đây có thể là do tấn công vào mật khẩu. Ví dụ về việc phân tích nhật ký hệ thống để phát hiện về số lần đăng nhập, ví dụ trong bài viết này.

		+ Với kiểu tấn công lợi dụng sự tin cậy, admin cần giảm thiểu việc cấu hình giữa các hệ thống. Ví dụ, khi bạn dùng trình duyệt IE trên máy chủ windows server, mỗi khi bạn vào một website thì máy chủ IE đều hỏi bạn xem có trust cái site đó không. Bạn hãy cân nhắc kỹ trước khi đưa website đó vào danh mục Trust bởi vì nếu máy chủ web đó bị khống chế bởi hacker thì bạn sẽ gặp phải nguy cơ… + Với kiểu tấn công MITM: vì kẻ đứng giữa cần nhân bản dữ liệu mà bạn chặn bắt, do vậy sẽ tiêu tốn nhiều băng thông. Admin cần có công cụ giám sát băng thông để phát hiện ra việc này. Ví dụ về các phần mềm giám sát hoặc phần mềm giám sát băng thông. + Với kiểu tấn công tràn bộ đệm, ban đầu cần có công cụ giám sát trạng thái của các tiến trình đang chạy trong hệ thống, ví dụ hai công cụ Event Viewer kết hợp với Performance Monitor trên Windows.
6	Tấn công thay đổi giao diện	- Xem những thông tin nhật ký, file log của máy chủ và truy tìm xem hacker đã làm gì và làm như thế nào trên hệ thống của mình
7	Tấn công mã hóa phần mềm, dữ liệu thiết bị	- Cài đặt duy trì phần mềm chống virus. - Công cụ chống phần mềm độc hại.
8	Tấn công phá hoại thông tin, dữ liệu phần mềm	- Cài đặt duy trì phần mềm chống virus. - Công cụ chống phần mềm độc hại.

9	Tấn công nghe trộm, gián điệp lấy cắp thông tin, dữ liệu Tấn công tổng hợp sử dụng kết hợp nhiều hình thức; Các hình thức tấn công mạng	- Cập nhật máy tính , phần mềm. - Cài đặt và duy trì phần mềm virus. - Công cụ chống phần mềm độc hại.
10	Tấn công vào con người: Kẻ tấn công có thể liên lạc với người quản trị hệ thống tạo nên một hộp thoại đăng nhập sau đó yêu cầu người dùng thay đổi cấu hình hệ thống, phương thức tấn công mạng này rất khó tìm ra giải pháp ngăn chặn triệt để ngoài con người	- Nâng cao nhận thức, Kiến thức khi sử dụng internet và các dịch vụ online. - Một số hình thức, phương thức tấn công vào hệ thống mạng, máy tính khác như: Thông qua USB, đĩa CD, địa chỉ IP, server, qua đầu vào của máy in.....