Chương 2

CÁC MỐI ĐE DỌA, PHÁP LUẬT AN TOÀN THÔNG TIN

Giáo viên: Lê Quốc Anh

Nội dung

1. Các mối đe dọa (Threats) và rủi ro (Risks)
2. Các phương pháp tấn công
3. Mã độc và phòng chống mã độc
4. Một số vấn đề an toàn thông tin tại Việt Nam
5. Pháp luật và Quy định về an toàn thông tin
6. Câu hỏi và Bài tập

1. Các mối đe dọa (Threats) và rủi ro (Risks)

- Mục tiêu an toàn HTTT là **GIẢM các RỦI RO**, **không có nghĩa là LOẠI TRỪ** chúng mà là chỉ giảm chúng đến một **mức chấp nhận được**

- Để đảm bảo ATTT một cách hiệu quả: dự đoán sự **cố nào** có thể xảy ra, nhận dạng **CÁI GÌ, Ở ĐÂU** cần an toàn. Trả lời: **Những gì cần bảo vệ? Mối đe dọa nào? Điểm yếu nào có thể bị khai thác?**

Slide: 3

Threat – Mối đe dọa

- Mối đe dọa đề cập đến một sự cố mới được phát hiện có khả năng gây hại cho một hệ thống hoặc tổ chức nào đó.
- Là một thuật ngữ, mô tả nơi mà mối đe dọa bắt nguồn và con đường cần để đạt được mục tiêu
- Ví dụ một e-mail lạ có tiêu đề hấp dẫn và có chứa mã độc trong tập tin đính kèm
- Có ba loại mối đe dọa chính:
  - Các mối đe dọa tự nhiên (ví dụ: lũ lụt hoặc lốc xoáy),
  - Các mối đe dọa không chủ ý (chẳng hạn như một nhân viên truy cập sai thông tin sai)
  - Các mối đe dọa có chủ ý. (Ví dụ: phần mềm gián điệp, phần mềm độc hại, công ty phần mềm quảng cáo hoặc hành động phá hoại của con người, virus…)

Slide: 4

Threat – Mối đe dọa

- Biện pháp phòng tránh
  - Thông báo về các xu hướng hiện tại trong an ninh mạng để họ có thể nhanh chóng xác định các mối đe dọa mới.
  - Thực hiện đánh giá mối đe dọa thường xuyên để xác định các phương pháp tốt nhất để bảo vệ hệ thống chống lại một mối đe dọa cụ thể, cùng với việc đánh giá các loại mối đe dọa khác nhau.
  - Ngoài ra, kiểm tra các mối đe dọa trong thế giới thực để khám phá các lỗ hổng bảo mật.

Slide: 5

Vulnerability – Lỗ hổng

- Là một số lỗ hổng hoặc điểm yếu trong phần cứng, phần mềm, con người, các quy trình, thiết kế, cấu hình…tất cả mọi thứ liên quan đến hệ thống thông tin – HTTT) mà kẻ tấn công có thể sử dụng nó để gây thiệt hại cho tổ chức.
- Ví dụ, khi một thành viên trong công ty từ chức và bạn quên vô hiệu hóa quyền truy cập của họ, điều này khiến doanh nghiệp của bạn bị cả hai mối đe dọa cố ý và không chủ ý.

Slide: 6

Vulnerability – Lỗ hổng

- Một số câu hỏi để xác định các lỗ hổng bảo mật của bạn:
  - Dữ liệu của bạn có được sao lưu và lưu trữ ở một địa điểm an toàn bên ngoài trang web không?
  - Dữ liệu của bạn có được lưu trữ trên đám mây không? Nếu có, làm thế nào chính xác là nó được bảo vệ khỏi các lỗ hổng trên đám mây?
  - Bạn có loại bảo mật mạng nào để xác định ai có thể truy cập, sửa đổi hoặc xóa thông tin từ bên trong tổ chức của bạn?
  - Loại bảo vệ chống virus nào đang được sử dụng? Giấy phép có hiện hành không? Nó có chạy thường xuyên khi cần thiết không?
  - Bạn có kế hoạch khôi phục dữ liệu trong trường hợp lỗ hổng bị khai thác không?

Slide: 7

Risk – Rủi ro

- Rủi ro đề cập đến khả năng mất mát hoặc thiệt hại khi một mối đe dọa khai thác lỗ hổng bảo mật.
- Ví dụ về rủi ro bao gồm tổn thất về tài chính do gián đoạn kinh doanh, mất quyền riêng tư, thiệt hại có uy tín, các tác động pháp lý và thậm chí có thể bao gồm mất mạng.

RISK = Threat + Vulnerability

Slide: 8

Risk – Rủi ro

- Biện pháp giảm rủi ro: tạo và triển khai một kế hoạch quản lý rủi ro.
  - Đánh giá rủi ro và xác định nhu cầu phải được thực hiện thường xuyên, định kỳ.
  - Bao gồm quan điểm của các bên liên quan (doanh nghiệp, nhân viên, khách hàng, các nhà cung cấp).
  - Chỉ định một nhóm nhân viên trung tâm chịu trách nhiệm quản lý rủi ro và xác định mức tài trợ thích hợp cho hoạt động này.
  - Thực hiện các chính sách thích hợp và kiểm soát các bên liên quan đảm bảo người dùng được thông báo về tất cả các thay đổi.
  - Giám sát và đánh giá hiệu quả chính sách và kiểm soát.

Slide: 9

Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn

- Có 3 hình thức chủ yếu đe dọa đối với hệ thống:
  - Phá hoại: kẻ thù phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ thống.
  - Sửa đổi: Tài sản của hệ thống bị sửa đổi trái phép. Điều này thường làm cho hệ thống không làm đúng chức năng của nó. Chẳng hạn như thay đổi mật khẩu, quyền ngườ̀i dùng trong hệ thống làm họ không thể truy cập vào hệ thống để làm việc.
  - Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền. Các truyền thông thực hiện trên hệ thống bị ngăn chặn, sửa đổi.

Slide: 10

Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn

- Các đe dọa đối với một hệ thống thông tin có thể đến từ ba loại đối tượng như sau:
  - Các đối tượng từ ngay bên trong hệ thống (insider), đây là những người có quyền truy cập hợp pháp đối với hệ thống.
  - Những đối tượng bên ngoài hệ thống (hacker, cracker), thường các đối tượng này tấn công qua những đường kết nối với hệ thống như Internet chẳng hạn.
  - Các phần mềm (chẳng hạn như spyware, adware …) chạy trên hệ thống.

Slide: 11

Các mối đe dọa thường gặp

- Lỗi và thiếu sót của người dùng (Errors and Omissions)
- Gian lận và đánh cắp thông tin (Fraud and Theft)
- Kẻ tấn công nguy hiểm (Malicious Hackers)
- Mã độc (Malicious Code)
- Tấn công từ chối dịch vụ (Denial-of-Service Attacks)
- Social Engineering

Slide: 12

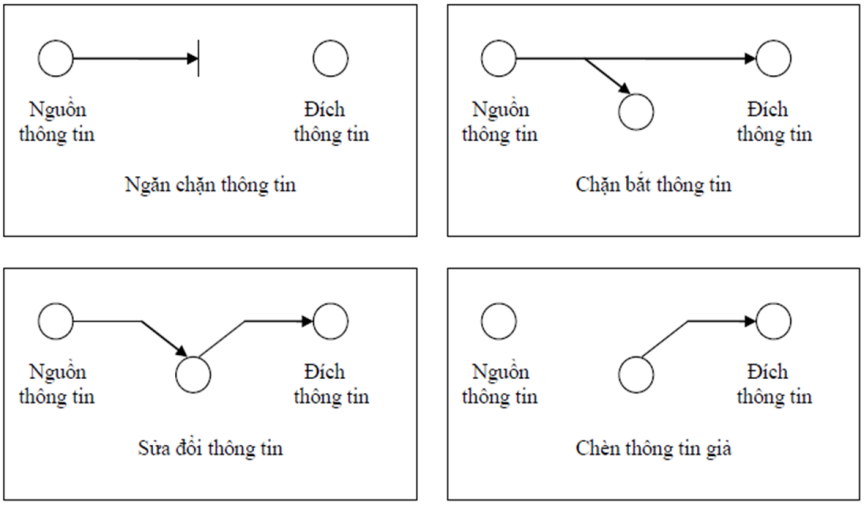
2. Các phương pháp tấn công

- **Định nghĩa chung:** Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.

- Tấn công HTTT là các tác động hoặc là trình tự liên kết giữa các tác động với nhau để phá huỷ, dẫn đến việc hiện thực hoá các nguy cơ bằng cách lợi dụng đặc tính dễ bị tổn thương của các hệ thống thông tin này.

Slide: 13

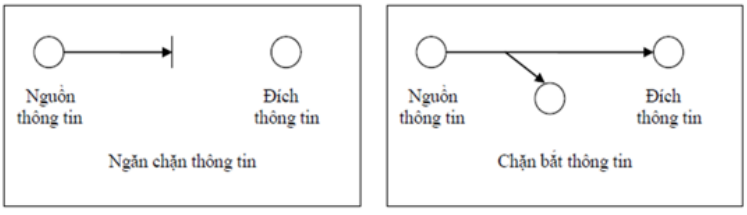
Các loại hình tấn công



Slide: 14

Các loại hình tấn công

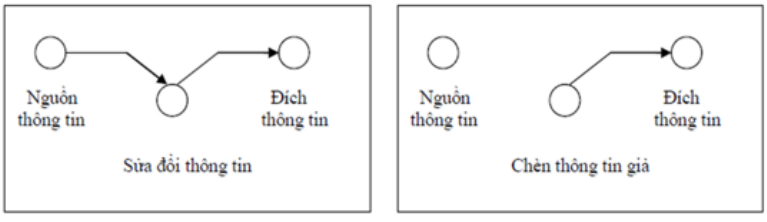
- Tấn công ngăn chặn thông tin (interruption)
  - Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- Tấn công chặn bắt thông tin (interception)
  - Kẻ tấn công có thể truy nhập tới tài nguyên thông tin. Đây là hình thức tấn công vào tính bí mật của thông tin.



Slide: 15

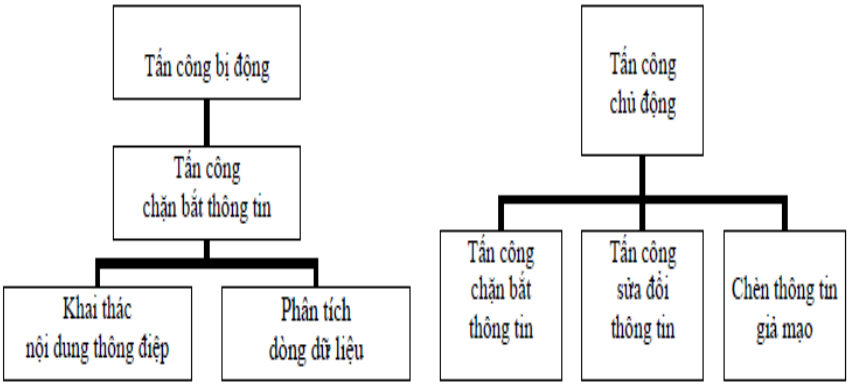
Các loại hình tấn công

- Tấn công sửa đổi thông tin (Modification)
  - Kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng.
  - Đây là hình thức tấn công vào tính toàn vẹn của thông tin.
- Chèn thông tin giả mạo (Fabrication)
  - Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống.
  - Đây là hình thức tấn công vào tính xác thực của thông tin.



Slide: 16

Tấn công bị động và chủ động



Slide: 17

Tấn công bị động (passive attacks)

- Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.
- Có hai kiểu tấn công bị động là khai thác nội dung thông điệp và phân tích dòng dữ liệu.
- Tấn công bị động rất khó bị phát hiện vì nó không làm thay đổi dữ liệu và không để lại dấu vết rõ ràng. Biện pháp hữu hiệu để chống lại kiểu tấn công này là ngăn chặn (đối với kiểu tấn công này, ngăn chặn tốt hơn là phát hiện).

Slide: 18

Tấn công chủ động (active attacks)

- Tấn công chủ động được chia thành 4 loại sau:
  - Giả mạo (Masquerade): Một thực thể (người dùng, máy tính, chương trình…) đóng giả thực thể khác.
  - Dùng lại (replay): Chặn bắt các thông điệp và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
  - Sửa thông điệp (Modification of messages): Thông điệp bị sửa đổi hoặc bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.
  - Từ chối dịch vụ (Denial of Service - DoS): Ngăn cấm việc sử dụng bình thường hoặc làm cho truyền thông ngừng hoạt động.

Slide: 19

Các hình thức tấn công mạng phổ biến

- Tấn công trực tiếp
- Kỹ thuật đánh lừa *(Social Engineering)*
- Kỹ thuật tấn công vào vùng ẩn
- Tấn công vào các lỗ hổng bảo mật
- Khai thác tình trạng tràn bộ đệm
- Nghe trộm
- Kỹ thuật giả mạo địa chỉ
- Kỹ thuật chèn mã lệnh
- Tấn công vào hệ thống có cấu hình không an toàn
- Tấn công dùng Cookies
- Can thiệp vào tham số trên URL
- Vô hiệu hóa dịch vụ
- **Lỗ hổng không cần login**
- **Thay đổi dữ liệu**
- **Password-base Attact**
- **Identity Spoofing**

Slide: 20

Một số kỹ thuật tấn công mạng

- Tấn công thăm dò.
- Tấn công sử dụng mã độc.
- Tấn công xâm nhập.
- Tấn công từ chối dịch vụ.
- Tấn công sử dụng kỹ nghệ xã hội

Slide: 21

Tấn công thăm dò

- Thăm dò là việc thu thập thông tin trái phép về tài nguyên, các lỗ hổng hoặc dịch vụ của hệ thống.
- Tấn công thăm dò thường bao gồm các hình thức:
  - Sniffing (Nghe lén)
  - Ping Sweep: Chủ yếu hoạt động trên các mạng sử dụng thiết bị chuyển mạch (switch).
  - Ports Scanning: là một quá trình kết nối các cổng (TCP và UDP) trên một hệ thống mục tiêu nhằm xác định xem dịch vụ nào đang "chạy" hoặc đang trong trạng thái "nghe". Xác định các cổng nghe là một công việc rất quan trọng nhằm xác định được loại hình hệ thống và những ứng dụng đang được sử dụng.

Slide: 22

Tấn công từ chối dịch vụ (Denial of Service)

- Về cơ bản, tấn công từ chối dịch vụ là tên gọi chung của kiểu tấn công làm cho một hệ thống nào đó bị quá tải không thể cung cấp dịch vụ, gây ra gián đoạn hoạt động hoặc làm cho hệ thống ngừng hoạt động.

Slide: 23

Tấn công từ chối dịch vụ (Denial of Service)

- Tùy theo phương thức thực hiện mà nó được biết dưới nhiều tên gọi khác nhau.
- Khởi thủy là lợi dụng sự yếu kém của giao thức TCP (Transmision Control Protocol) để thực hiện tấn công từ chối dịch vụ DoS (Denial of Service), mới hơn là tấn công từ chối dịch vụ phân tán DDoS (Distributed DoS), mới nhất là tấn công từ chối dịch vụ theo phương pháp phản xạ DRDoS (Distributed Reflection DoS).

Slide: 24

Tấn công sử dụng mã độc (malicious code)

- **Khái niệm:** Mã độc là những chương trình khi được khởi chạy có khả năng phá hủy hệ thống, bao gồm Virus, sâu (Worm) và Trojan, ...
- Tấn công bằng mã độc có thể làm cho hệ thống hoặc các thành phần của hệ thống hoạt động sai lệch hoặc có thể bị phá hủy.

Slide: 25

Tấn công xâm nhập (Intrusion attack)

- Là hình thức tấn công, nhằm truy nhập bất hợp pháp vào các HTTT.
- Kiểu tấn công này được thực hiện với mục đích đánh cắp dữ liệu hoặc thực hiện phá hủy bên trong HTTT

Slide: 26

Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

- Là một nhóm các phương pháp được sử dụng để đánh lừa người sử dụng tiết lộ các thông tin bí mật.
- Là phương pháp tấn công phi kỹ thuật, dựa trên sự thiếu hiểu biết của người dùng để lừa gạt họ cung cấp các thông tin nhạy cảm như password hay các thông tin quan trọng khác.

Slide: 27

Xu hướng tấn công HTTT

1. Sử dụng các công cụ tấn công tự động
   - Những kẻ tấn công sẽ sử dụng các công cụ tấn công tự động có khả năng thu thập thông tin từ hàng nghìn địa chỉ trên Internet một cách nhanh chóng, dễ dàng và hoàn toàn tự động.
   - Các HTTT có thể bị quét từ một địa điểm từ xa để phát hiện ra những địa chỉ có mức độ bảo mật thấp. Thông tin này có thể được lưu trữ, chia sẻ hoặc sử dụng với mục đích bất hợp pháp.

Slide: 28

Xu hướng tấn công HTTT

2. Sử dụng các công cụ tấn công khó phát hiện

- Một số cuộc tấn công được dựa trên các mẫu tấn công mới, không bị phát hiện bởi các chương trình bảo mật, các công cụ này có thể có tính năng đa hình, siêu đa hình cho phép chúng thay đổi hình dạng sau mỗi lần sử dụng.

Slide: 29

Xu hướng tấn công HTTT

3. Phát hiện nhanh các lỗ hổng bảo mật

- Thông qua các lỗ hổng bảo mật của hệ thống, phần mềm kẻ tấn công khai thác các lỗ hổng này để thực hiện các cuộc tấn công.
- Hàng năm, nhiều lỗ hổng bảo mật được phát hiện và công bố, tuy nhiên điều này cũng gây khó khăn cho các nhà quản trị hệ thống để luôn cập nhật kịp thời các bản vá. Đây cũng chính là điểm yếu mà kẻ tấn công tận dụng để thực hiện các hành vi tấn công, xâm nhập bất hợp pháp.

Slide: 30

Xu hướng tấn công HTTT

4. Tấn công bất đối xứng và tấn công diện rộng

- Tấn công bất đối xứng xảy ra khi bên tấn công mạnh hơn nhiều so với đối tượng bị tấn công.
- Tấn công diện rộng thực hiện khi kẻ tấn công tạo ra một mạng lưới kết hợp các hoạt động tấn công.

Slide: 31

Xu hướng tấn công HTTT

5. *Thay đổi mục đích tấn công*

- Thời gian trước, các tấn công chỉ từ mục đích thử nghiệm, hoặc khám phá hệ thống an ninh.
- Hiện nay, mục đích tấn công với nhiều lý do khác nhau như về tài chính, giả mạo thông tin, phá hủy, và đặc biệt nguy hiểm đó là mục đích chính trị, chính vì vậy mà độ phức tạp của các cuộc tấn công đã tăng lên và tác hại lớn hơn rất nhiều so với trước đây.

Slide: 32

Mối đe dọa an ninh mạng hàng đầu năm 2020

1. Intelligent Edge - Vùng mạng biên thông minh là một cơ hội đồng thời cũng là một nguy cơ

- Trong vài năm gần đây, đường rìa bên ngoài của hệ thống mạng truyền thống đã bị thay thế bằng môi trường đa biên, mạng WAN, nền tảng multi -cloud, trung tâm dữ liệu (data center), đội ngũ nhân viên làm việc từ xa, IoT, và hơn thế nữa, mang theo những rủi ro khác nhau. Một trong những lợi thế đáng kể nhất đối với những tội phạm mạng đó là trong khi tất cả những biên này đều được kết nối lẫn nhau thì rất nhiều tổ chức đã hy sinh khả năng hiển thị tập trung và kiểm soát thống nhất để đổi lấy hiệu suất và chuyển đổi số. Kết quả là, những kẻ xấu trên mạng đã tìm cách cải tiến những đợt tấn công của chúng bằng cách nhắm vào những môi trường này và sẽ khai thác tốc độ và quy mô từ khả năng của công nghệ 5G.

Slide: 33

Mối đe dọa an ninh mạng hàng đầu năm 2020

2. Trojan tiến hóa để nhắm vào vùng mạng biên

- Trong khi những người dùng cuối và tài nguyên tại nhà của họ đã là mục tiêu cho những tên tội phạm mạng, những kẻ tấn công tinh vi còn sử dụng chúng như một bàn đạp để tiếp tục triển khai những kế hoạch khác. Những cuộc tấn công mạng doanh nghiệp bắt đầu từ mạng tại nhà của một nhân viên làm việc từ xa, đặc biệt khi xu hướng sử dụng mạng được thấu hiểu một cách rõ ràng, có thể được kết hợp một cách cẩn thận, do vậy không tạo ra bất kỳ điểm đáng nghi nào.
- Dần dần, mã độc nâng cao có thể cũng khám phá được thậm chí nhiều dữ liệu và xu hướng giá trị hơn bằng cách sử dụng mã độc EAT mới (mã độc Trojan Truy cập Vùng biên), đồng thời thực hiện những hoạt động xâm lấn như ngăn chặn những yêu cầu đến từ mạng địa phương nhằm gây hại tới những hệ thống khác hoặc bổ sung thêm những lệnh tấn công.

Slide: 34

Mối đe dọa an ninh mạng hàng đầu năm 2020

3. Tấn công swarm từ vùng biên (được hỗ trợ bởi AI)

- Xâm nhập và lợi dụng những thiết bị sử dụng công nghệ 5G mới mở ra những cơ hội cho những mối đe dọa nâng cao hơn. Một quy trình đã được tạo ra bởi những tên tội phạm mạng nhằm phát triển và triển khai những cuộc tấn công swarm. Những cuộc tấn công này lợi dụng những thiết bị bị chiếm quyền điều khiển được chia ra thành những nhóm nhỏ, mỗi nhóm với những kỹ năng chuyên môn riêng.
- Chúng nhắm vào những mạng hoặc thiết bị như một hệ thống được tích hợp, sau đó chia sẻ thông tin theo thời gian thực để tối ưu hiệu quả của cuộc tấn công khi chúng diễn ra. Những công nghệ swarm yêu cầu năng lực xử lý lớn để tiến hành kích hoạt các con swarmbot đơn lẻ và để chia sẻ thông tin giữa chúng với nhau. Điều này cho phép chúng nhanh chóng khám phá, chia sẻ và tương quan những lỗ hổng an ninh, từ đó thay đổi phương thức tấn công để khai thác tốt hơn những gì chúng đã khám phá ra được trong hệ thống mạng.

Slide: 35

Mối đe dọa an ninh mạng hàng đầu năm 2020

4. Phát tán những cuộc tấn công từ không gian

- Sự kết nối các hệ thống vệ tinh nhân tạo và viễn thông có thể trở thành một mục tiêu hấp dẫn đối với tội phạm mạng. Do các hệ thống giao tiếp mới phát triển và bắt đầu dựa nhiều hơn vào một mạng lưới các hệ thống vệ tinh, tội phạm mạng có thể nhắm vào việc kết hợp này và theo đuổi nó.
- Kết quả là, việc xâm nhập các trạm vệ tinh và phát tán mã độc thông qua hệ thống vệ tinh có thể đem tới cho những kẻ tấn công khả năng nhắm tới hàng triệu người dùng đang kết nối mạng tiềm năng ở quy mô lớn hoặc giáng xuống những cuộc tấn công DDoS có thể gây cản trở những giao tiếp quan trọng.

Slide: 36

Mối đe dọa an ninh mạng hàng đầu năm 2020

5. Mối đe dọa từ máy tính lượng tử

- Từ quan điểm của an ninh mạng, máy tính lượng tử có thể tạo ra rủi ro mới, dần dần có thể thách thức hiệu quả của việc mã hóa trong tương lai. Công suất tính toán khổng lồ của các máy tính lượng tử có thể khiến các thuật toán mã hóa bất đối xứng được giải mã. Kết quả là tổ chức sẽ cần chuẩn bị chuyển đổi sang các thuật toán crypto chống lượng tử bằng cách sử dụng các nguyên lý về tính linh hoạt của crypto (tiền ảo), nhằm đảm bảo khả năng bảo vệ dữ liệu hiện tại và tương lai.
- Mặc dù tội phạm mạng thông thường không truy cập được vào máy tính lượng tử, các tổ chức chính phủ cấp quốc gia lại có thể, do vậy mối đe dọa cuối cùng vẫn sẽ xảy ra nếu các kế hoạch phòng bị bằng cách ứng dụng tính linh hoạt của crypto không được thiết lập bây giờ để chống lại rủi ro này.

Slide: 37

Mối đe dọa an ninh mạng hàng đầu năm 2020

6. AI sẽ trở nên rất quan trọng để bảo vệ mạng chống lại những cuộc tấn công trong tương lai

- Khi những xu hướng tấn công có thể dự đoán trước phía trên dần trở thành hiện thực, điều đó sẽ chỉ là vấn đề thời gian trước khi triển khai các tài nguyên trở nên chuẩn hóa và biến thành hàng hóa sẵn có như một dịch vụ mạng đen, hoặc như một phần của bộ công cụ nguồn mở. Do vậy việc kết hợp cẩn trọng giữa công nghệ, con người, đào tạo và hợp tác đối tác rất cần thiết để đảm bảo chống lại những thể loại tấn công đến từ những kẻ xấu trên không gian mạng trong tương lai.

Slide: 38

3. Mã độc và phòng chống mã độc

Mã độc là gì MALWARE?

- MALWARE là viết tắt của từ Malicious Software có nghĩa là phần mềm độc hại (Mã độc)
- Mã độc là một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức.
- Thực hiện các hành vi chuộc lợi cá nhân, kinh tế, chính trị hoặc đơn giản là để thỏa mãn ý tưởng và sở thích của người viết.

Slide: 39

3. Mã độc và phòng chống mã độc

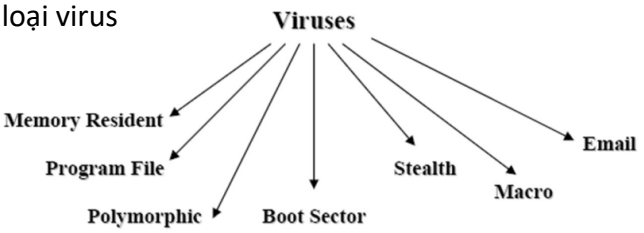
- Phân loại và đặc tính của mã độc
  - Tuỳ thuộc vào cơ chế, hình thức lây nhiễm và phương pháp phá hoại mà người ta phân biệt mã độc thành nhiều loại khác nhau: virus, trojan, backdoor, adware, spyware, Worm, Keylogger, Rookit, Attacker Tools…
  - Đặc điểm chung của mã độc là thực hiện các hành vi không hợp pháp (hoặc có thể hợp pháp, ví dụ như các addon quảng cáo được thực thi một cách hợp pháp trên máy tính người dùng) nhưng không theo ý muốn của người sử dụng máy tính.

Slide: 40

3. Mã độc và phòng chống mã độc

Một số loại mã độc:

- Virus
  - Là những chương trình nhỏ có khả năng tự sao chép, tự động chèn nó vào các chương trình thực thi khác.
  - Có thể gây phá hủy dữ liệu, chương trình, ổ cứng.
  - Mã độc ảnh hưởng đến các file thực thi, Macros trong tài liệu, được phân phối qua mail, chia sẻ file
  - Một số loại virus



Slide: 41

3. Mã độc và phòng chống mã độc

- Worms – Sâu máy tính
  - Khác với virus, nó là một chương trình độc lập, không nhiễm vào bất kỳ ứng dụng nào
  - Lây lan qua mạng một cách tự động, thường lây lan nhanh hơn virus
  - Tự sao chép vào các thư mục của hệ thống
  - Ghi thông tin khởi động vào hệ thống, để mỗi lần khởi động nó có thể làm việc
  - Worms thường đi kèm với virus, Trojan
  - Worm có thể xóa và thay đổi dữ liệu các máy bị nhiễm, chiếm dung lượng bộ nhớ làm cho máy bị chậm hoặc bị treo.
  - Chiếm băng thông của hệ thống mạng.

Slide: 42

3. Mã độc và phòng chống mã độc

- Zoombie
  - Là một chương trình cho phép chiếm quyền điều khiển của một máy tính có nối mạng Internet một cách bí mật, và sau đó sử dụng máy tính này phát động một cuộc tấn công.
- Trojan Horses
  - Là một đoạn mã ẩn với bề ngoài là một chương trình bình thường
  - Thường được sử dụng để mở back-door tạo điều kiện cho Craker thâm nhập vào hệ thống và thu thập thông tin bất hợp pháp
  - Không thể tự lây lan nhưng có thể được gắn vào virus để có thể lây lan
  - Những máy tính bị nhiễm Trojan thường bị lợi dụng để tấn công DDoS

Slide: 43

3. Mã độc và phòng chống mã độc

- Trojan thường có hai công việc. (1) Thực hiện trực tiếp các công việc gây hại cho người dung khi kích hoạt nó; (2) tự động "nằm vùng" trong máy tính sau đó kích hoạt.
- BackDoor
  - Chỉ chung các phần mềm độc hại thường trú và đợi lệnh điều khiển từ các cổng dịch vụ TCP hoặc UDP
  - Zoombie (bot): là một chương trình được cài đặt lên hệ thống nhằm mục đích tấn công hệ thống khác, những máy bị nhiễm bot, thường bị hacker sử dụng tấn công DOS mà người dung không biết
  - Remote Administration Tool: là các công cụ của hệ thống cho phép quản trị từ xa, vì vậy Hacker có thể theo dõi mọi thứ xuất hiện trên màn hình, bàn phím, hoặc tác động vào cấu hình của hệ thống

Slide: 44

3. Mã độc và phòng chống mã độc

- Keylogger
  - Là phần mềm bí mật ghi lại các phím đã được nhấn vào bàn phím, thao tác chuột hoặc screen rồi gửi tới hacker
  - Keylogger có thể ghi lại nội dung của email, văn bản, user name, passrord, thông tin bí mật
  - Keylogger có thể được phân loại thành keyloger phần mềm và keylogger phần cứng.

Slide: 45

3. Mã độc và phòng chống mã độc

- Rootkit
  - Là bộ công cụ phần mềm sử dụng cho mục đích che dấu sự tồn tại và hoạt động của những tiến trình hoặc những file mà Hacker mong muốn
  - Rootkit có khả năng ẩn các tiến trình, file, và cả dữ liệu trong registry, vì thế người dung không biết có bị nhiễm mã độc hay không.
  - Rootkit còn được giữ vai trò như keylogger.
  - Rootkit được coi là Trojan vì chúng có hành vi nghe trộm, che dấu các chương trình độc hại

Slide: 46

3. Mã độc và phòng chống mã độc

- Adware
  - Adware tạo ra các chương trình quảng cáo popup mà không có sự cho phép của người dung. Adware thường được cài đặt bởi một thành phần của phần mềm miễn phí
  - Adware thường gây sự khó chịu cho người dung vì nó thường xuất hiện quảng cáo trên screen, nên nó cũng tiêu tốn tài nguyên máy tính.
- Spyware
  - Là phần mềm cài đặt trên máy tính người dùng nhằm thu thập các thông tin người dùng một cách bí mật, không được sự cho phép của người dùng.

Slide: 47

3. Mã độc và phòng chống mã độc

- Ransomware - Phần mềm tống tiền:
  - Đây là phần mềm khi lây nhiễm vào máy tính nó sẽ kiểm soát hệ thống hoặc kiểm soát máy tính và yêu cầu nạn nhân phải trả tiền để có thể khôi phục lại điều khiển với hệ thống.
- Attacker Tool
  - Là những bộ công cụ tấn công có thể sử dụng để đẩy các phần mềm độc hại vào hệ thống
  - Các bộ công cụ này có khả năng giúp cho kẻ tấn công truy cập bất hợp pháp vào hệ thống làm cho hệ thống lây nhiễm Malware
  - Khi tải vào trong hệ thống bằng các đoạn Malware, attacker tool có thể chính là một phần trong đoạn malware đó

Slide: 48

3. Mã độc và phòng chống mã độc

Một số biện pháp phòng chống:

- **Luôn luôn cài đặt và sử dụng một phần mềm diệt virus chính hãng.** Ví dụ: Kaspersky, CyStack, Bitdifender, Avast, Norton, Bkav, …
- **Xây dựng chính sách với các thiết bị PnP:** Với các thiết bị loại này: USB, CD/DVD, … virus có thể lợi dụng để thực thi mà không cần sự cho phép của người dùng. Do đó, cần thiết lập lại chế độ cho các thiết bị và chương trình này để hạn chế sự thực thi không kiểm soát của mã độc. Ngoài ra, trong quá trình sử dụng các thiết bị như USB, chúng ta không nên mở trực tiếp bằng cách chọn ổ đĩa rồi nhấn phím Enter, hoặc nhấp đôi chuột vào biểu tượng mà nên bấm chuột phải rồi click vào explore

Slide: 49

3. Mã độc và phòng chống mã độc

- **Thiết lập quy tắc đối xử với các file:** Không nên mở hoặc tải về các file không rõ nguồn gốc, đặc biệt là các file thực thi (các file có đuôi .exe, .dll, …). Với các file không rõ nguồn gốc này, tốt nhất chúng ta nên tiến hành quét bằng phần mềm diệt virus hoặc thực hiện kiểm tra trực tiếp trên website: https://www.virustotal.com Khi có nghi ngờ được cảnh báo cần dừng việc thực thi file lại để đảm bảo an toàn.
- **Truy cập web an toàn:** Khi truy cập web cần chú ý: Không nên truy cập vào các trang web đen, các trang web độc hại, có nội dung không lành mạnh, không tuy tiện click vào các url từ các email hoặc từ nội dung chat, trên các website, … Các website và url như trên thường xuyên ẩn chứa các mã độc và chỉ đợi người dùng click, nó sẽ tự động tải về, thiết lập cài đặt để thực thi hợp pháp trên máy tính người dùng. Một ví dụ tiêu biểu đó là khi chúng ta phân tích và theo dõi các máy của các nhân viên văn phòng, các máy tính này hầu hết đều bị cài đặt các addon hoặc các phần mềm quản cáo do quá trình duyệt web chính bản thân người sử dụng đã cho phép addon hoặc phần mềm đó thực thi.

Slide: 50

3. Mã độc và phòng chống mã độc

- **Cập nhật máy tính, phần mềm:** Thường xuyên cập nhật các bản vá được cung cấp từ hệ điều hành, các bản vá cho các ứng dụng đang sử dụng và đặc biệt là cập nhật chương trình diệt virus. Đây là yếu tố quan trọng để tránh được các loại mã độc lợi dụng các lỗ hổng để lây lan, đồng thời cũng cập nhật được các mẫu mã độc mới để giúp phần mềm diệt virus làm việc hiệu quả hơn.
- **Nhờ chuyên gia can thiệp:** Khi thấy máy tính có các dấu hiệu bị lây nhiễm cần tiến hành quét ngay bằng phần mềm diệt virus, nếu vẫn không có tiến triển tốt, cần nhờ sự giúp đỡ của các chuyên gia để kiểm tra máy tính, phát hiện và tiêu diệt mã độc ngay. Có thể việc này sẽ làm tốn thời gian và tiền bạc nhưng nó thật sự cần thiết vì rất có thể tác hại của việc để nguyên máy tính còn tốn kém và thiệt hại hơn rất nhiều lần.

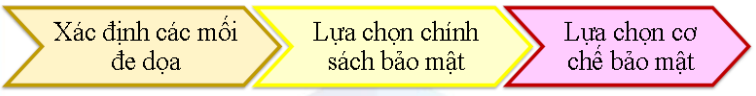
Slide: 51

Mục tiêu của bảo mật

- ***Ngăn chặn***
  - Ngăn chặn kẻ tấn công vi phạm các chính sách bảo mật
- ***Phát hiện***
  - Phát hiện các vi phạm chính sách bảo mật
- ***Phục hồi***
  - Chặn các hành vi vi phạm đang diễn ra, đánh giá và sửa lỗi
  - Tiếp tục hoạt động bình thường ngay cả khi tấn công đã xảy ra

Slide: 52

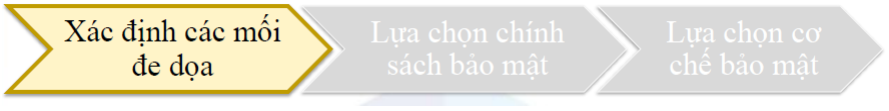
Các bước cơ bản trong bảo mật thông tin



- Xác định các mối đe dọa (threat)
  - Cái gì có thể làm hại đến hệ thống?
- Lựa chọn chính sách bảo mật (security policy)
  - Điều gì cần mong đợi ở hệ thống bảo mật?
- Lựa chọn cơ chế bảo mật (security mechanism)
  - Cách nào để hệ thống bảo mật có thể đạt được những mục tiêu bảo mật đề ra?

Slide: 53

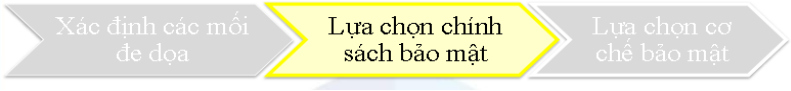
Các bước cơ bản trong bảo mật thông tin



- Các mối đe dọa bảo mật (security threat) là những sự kiện có ảnh hưởng đến an toàn của hệ thống thông tin.
- Các mối đe dọa được chia làm 4 loại:
  - Xem thông tin một cách bất hợp pháp
  - Chỉnh sửa thông tin một cách bất hợp pháp
  - Từ chối dịch vụ
  - Từ chối hành vi

Slide: 54

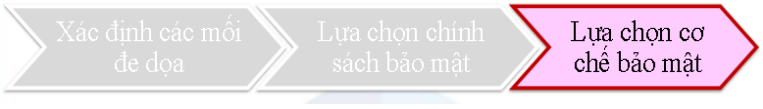
Các bước cơ bản trong bảo mật thông tin



- Việc bảo mật hệ thống cần có một chính sách bảo mật rõ ràng.
- Cần có những chính sách bảo mật riêng cho những yêu cầu bảo mật khác nhau
- Xây dựng và lựa chọn các chính sách bảo mật cho hệ thống phải dựa theo các chính sách bảo mật do các tổ chức uy tín về bảo mật định ra (compliance)
  - NIST, SP800, ISO17799, HIPAA

Slide: 55

Các bước cơ bản trong bảo mật thông tin



- Xác định cơ chế bảo mật phù hợp để hiện thực các chính sách bảo mật và đạt được các mục tiêu bảo mật đề ra
- Có 4 cơ chế bảo mật:
  - Điều khiển truy cập (Access control)
  - Điều khiển suy luận (Inference control)
  - Điều khiển dòng thông tin (Flow control)
  - Mã hóa (Encryption)

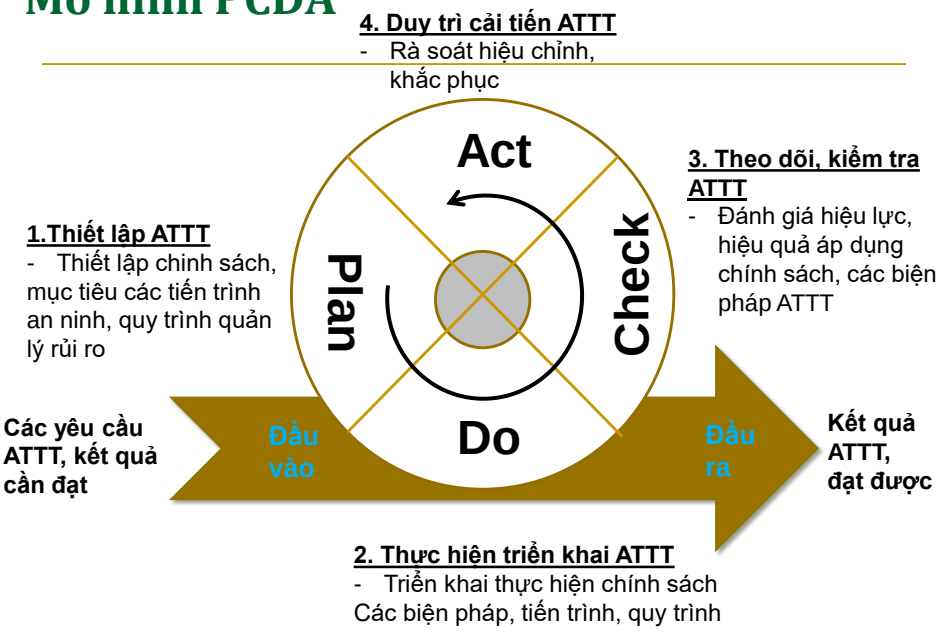
Slide: 56

Mô hình PCDA

- An toàn bảo mật thông tin không phải là trạng thái cố định, mà có sự biến động theo thời gian
- Sự biến động về quy trình nghiệp vụ, các nhiệm vụ, hạ tầng, kiến trúc của tổ chức và trang thiết bị CNTT có ảnh hưởng đến trạng thái ATTT của tổ chức.
- Cần kiểm tra định kỳ biện pháp ATTT để chúng có hiệu quả → Nếu phát hiện điểm yếu thì cần cải tiến cho phù hợp
- Cần có một quy trình đảm bảo an toàn bảo mật thông tin cho hệ thống
- Quy trình đảm bảo an toàn bảo mật thông tin có 4 pha sau: Lập kế hoạch (Plan); Thực hiện triển khai kế hoạch (Do); Kiểm tra theo dõi thực hiện kết quả (Check); Hành động giảm thiểu lỗi, điểm yếu và tối ưu hóa, cải tiến (Act)

Slide: 57

Mô hình PCDA



Slide: 58

Câu hỏi và bài tập

1) Trình bày ít nhất 5 phương thức tấn công mà website có thể gặp phải.
2) Trình bày giải pháp cụ thể cho mỗi cách tấn công trên và giải thích lý do anh/chị lựa chọn giải pháp đó.

Slide: 59

Câu hỏi và bài tập

- Website BẢO HIỂM MANULIFE của Manulife Financial cung cấp các dịch vụ xem danh mục các sản phẩm đa dạng từ sản phẩm bảo hiểm truyền thống đến sản phẩm bảo hiểm sức khoẻ, giáo dục, liên kết đầu tư, hưu trí… cho hơn 700.000 khách hàng thông qua đội ngũ đại lý hùng hậu và chuyên nghiệp tại 55 văn phòng trên 40 tỉnh thành cả nước. Khách hàng có thể chọn lựa, đặt câu hỏi, cần tư vấn hay mua gói bảo hiểm trực tuyến trên Website. Xem thông tin và quyền lợi bảo hiểm, xem hợp đồng bảo hiểm đã mua. Ngoài ra Website còn giúp cho công ty có thể quản lý toàn bộ các hoạt động của công ty như quản lý khách hang, nhân viên, hợp đồng bảo hiểm,…

- Hãy nhận dạng và giải thích được ít nhất 3 mối đe dọa ảnh hưởng đến an toàn đến các dịch vụ mà Website cung cấp.

Slide: 60

Câu hỏi và bài tập

- Công ty VCCloud là một trong nhiều công ty viễn thông, cung cấp các dịch vụ CDN cho các cá nhân và doanh nghiệp tại Việt Nam. Dịch vụ CDN là mạng lưới gồm nhiều máy chủ lưu trữ đặt tại nhiều vị trí địa lý khác nhau, cùng làm việc chung để phân phối nội dung, truyền tải hình ảnh, CSS, Javascript, Video clip, Real-time media streaming, File download đến người dùng cuối. Cơ chế hoạt động của CDN giúp cho khách hàng truy cập nhanh vào dữ liệu máy chủ web gần họ nhất thay vì phải truy cập vào dữ liệu máy chủ web tại trung tâm dữ liệu.
- Hãy nhận dạng và giải thích được ít nhất 3 mối đe dọa ảnh hưởng đến an toàn đến dịch vụ CDN mà VCCloud đang cung cấp

Slide: 61

Xin chân thành cảm ơn!

Slide: 62