Lý thuyết atbm - đề cương ôn tập ATBM thầy Hiếu

An toàn và bảo mật hệ thống thông tin (Trường Đại học Kinh tế, Đại học Đà Nẵng)

CHƯƠNG 1

1. **An toàn thông tin là** bảo vệ chống truy cập, sử dụng, tiết lộ, sửa đổi phá hủy thông tin một cách trái phép => an toàn phần cứng + phần mềm => duy trì tính bí mật, toàn vẹn, sẵn sàng
   - Mục tiêu: bảo vệ tài sản thông tin
   - 2 lĩnh vực chính của ATTT:
     + An toàn công nghệ thông tin + Đảm bảo thông tin
2. **Hệ thống thông tin:** là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ,, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số
   - Một HTTT dựa trên máy tính là một hệ thống thông tin use công nghệ máy tính để thực thi các nhiệm vụ
   - **Các thành phần:**
     + Hardware: phần cứng để thu thập, lưu trữ, xử lý và biểu diễn dl
     + Software: các phần mềm chạy trên phần cứng để xử lý dữ liệu
     + Database, Networks, Procedures (tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý)
   - Mối đe dọa/ nguy cơ: bất kỳ một hđ nào có thể gây hư hại tới tài nguyên hệ thống
   - Điểm yếu: khiếm khuyết/ lỗi tồn tại trong hệ thống
   - Lỗ hổng: bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây hại
   - Rủi ro: một mối đe dọa có thể khai khác 1 lỗ hổng để tấn công/gây nguy hiểm cho ht
3. **Các yêu cầu đảm bảo ATTT và HTTT**
   a. **Tính bí mật:**
   - TT chỉ đc phép truy cập bởi ~ đối tượng đc cấp phép
   - Kẻ tấn công lợi dụng điểm yếu để truy cập trái phép
   - Giới hạn truy cập về mặt vật lý (tiếp cận trực tiếp tới thiết bị lưu trữ TT đó)

     ➢ **Một số cách**: ▪ Khóa kín và niêm phong thiết bị ▪ Yêu cầu đối tượng cung cấp (user + password) ▪ Sử dụng firewall hoặc ACL ▪ Mã hóa thông tin

     ➢ **Các thông tin bí mật có thể gồm:** ▪ Dữ liệu riêng của cá nhân; ▪ Các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan/tổ chức; ▪ Các thông tin có liên quan đến an ninh quốc gia.

   b. **Tính toàn vẹn:**
   - TT chỉ được xóa/ sửa bởi đối tượng được phép và có thẩm quyền
   - Kẻ tấn công lợi dụng điểm yếu lặng lẽ sửa đổi => phá vỡ tính toàn vẹn

     ➢ Tính toàn vẹn liên quan đến tính hợp lệ và chính xác của dữ liệu.

     ➢ Dữ liệu là toàn vẹn nếu: ▪ DL k bị thay đổi; ▪ Dữ liệu hợp lệ; ▪ Dữ liệu chính xác.

     ➢ Tính toàn vẹn của thông tin bị phá vỡ khi:
       ▪ Thay đổi giao diện trang chủ của một website
       ▪ Chặn đứng và thay đổi gói tin được gửi qua mạng
       ▪ Chỉnh sửa trái phép các file được lưu trữ trên máy tính

▪ Do có sự cố trên đường truyền mà tín hiệu bị nhiễu hoặc suy hao dẫn đến thông tin bị sai lệch

c. Tính sẵn dùng

- bảo đảm các người sử dụng hợp pháp có khả năng truy cập đúng lúc và không bị ngắt quãng
- Kẻ tấn công lợi dụng điểm yếu => ngăn chặn, gây khó khăn cho ng dùng hợp pháp
- đảm bảo độ ổn định đáng tin cậy của thông tin, là thước đo, xác định phạm vi tới hạn an toàn của một HTTT.
- Thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.
- Một server chỉ bị ngưng hoạt động trong vòng 5 phút trên 1 năm=> độ sẵn dùng: 99,999%.

4. An ninh mạng

- Tường lừa (Firewall)
- Mạng riêng ảo VPN
- Bảo mật dữ liệu truyền (SSL/TLS/ PGP)
- Các kỹ thuật và hệ thống pháp hiện/ ngăn chặn tấn công, xâm nhập
- Giám sát mạng

5. Các đe dọa

a. Người dùng: Thiếu ý thức, coi nhẹ/vi phạm chính sách, đưa USB, tải video, phá hoại dữ liệu, nhân viên

b. Máy trạm

- Truy cập trái phép vào máy trạm, hệ thống DL
- Lỗ hỏng an ninh (HĐH, phần mềm)
- Virus, mã độc, đưa USB, tải video

c. LAN

- Truy cập trái phép vào mạng LAN vật lý, hệ thống DL
- Lỗ hổng (HĐH, phần mềm máy chủ) - Người dùng giả mạo

d. LAN – TO – WAN

- Thăm dò rà quét trái phép các cổng DV, truy cập trái phép
- Lỗ hổng (Bộ định tuyến, tường lửa) - Người dùng giả mạo

e. WAN

- Dữ liệu đc truy cập từ wifi công cộng
- DL đc truyền dưới dạng rõ (plantext, cleantext)
- Dễ bị nghe trộm, tấn công phá hoại, DoS, DdoS. - Gửi email kèm virus

CHƯƠNG 2

1. Thách thức an ninh thông tin

- Sự phát triển của công nghệ tập trung vào giao diện
- Số lượng ứng dụng tăng nhanh, Quản trị hạ tầng TT phức tạp
- Việc bảo mật cho hệ thống là khó, vi phạm an ninh, tuân phủ pháp luật
- Phần mềm độc hại, lỗi thiết bị, lỗi ứng dụng, thảm họa tự nhiên, hacker

2. Các dạng lỗ hổng bảo mật

- Lỗi tràn bộ đệm
- Không kiểm tra đầu vào

- Các vấn đề với điều khiển truy cập
- Các điểm yếu trong xác thực, trao quyền hoặc hệ mật mã

3. <u>Nhận dạng tội phạm</u>

- **Internet scammer: gửi** tin qua email cầu giúp đỡ, k dựa vào xâm nhập để thực hiện hvi phạm tội, có động cơ là kinh tế
- **Khủng bố:** gd chợ đen, thuốc phiện, vũ khí, động cơ: kte
- **Hacker mũ xám:** xâm nhập HT trái phép, cảnh báo về tính an toàn, k làm vc cho cty, k định gây hại, chỉ tỏ ra có ích, động cơ: bốc đồng
- **Hacker mũ đen (cracker):** xâm nhập ht trái phép, lợi dụng cđề bảo mật, k làm vc cho ctt, k muốn giúp đỡ mà chỉ gây hại
- **Hacker mũ trắng:** xâm nhập ht để ktra, xác nhận vde, làm việc cho cty, k gây hại, có ích
- Công cụ: quét lỗ hổng, quét cổng, nghe trộm, phần mềm quét SĐT, nghe trộ bàn fim
    a. Quét lỗ hổng (quét cổng dv, quét lỗ hổng bảo mật hệ thống, quét ứng dụng)
    b. Quét cổng DV:
- **Port scanning** là quá trình gửi các gói tin tới cổng TCP và UDP trên hệ thống đích để xác định dịch vụ nào đang chạy hoặc trong tình trạng đang lắng nghe.
- **CáccổngTCP/IP**, UDP năm trong khoảng từ 0– 65535
  • Các cổng 0-1024 là các cổng chuẩn
  • Cổng lớn hơn 1024 là các cổng tùy gán.
- **Kẻ tấn công thường sử dụng công cụ quét cổng** để nhận dạng các điểm yếu trong hệ thống; ▪ Cáccôngcụ: Netcat, Nmap, BackTrack:Autoscan, Umit, NmapFE,

❖ **Công cụ quét cổng kết nối đến máy tính để** xác định cổng nào được mở và có thể truy nhập vào máy tính. Từ đó xác định được dịch vụ/ứng dụng nào đang chạy trên hệ thống: • Cổng 80/443 mở → dịch vụ web đang chạy • Cổng 25 mở → dịch vụ email SMTP đang chạy • Cổng 1433 mở → Máy chủ CSDL MS SQL Server đang chạy • Cổng 53 mở → dịch vụ DNS đang chạy,..

<u>4. Đảm bảo môi trường ẩn danh</u>

a. Tol

- Nhiều lớp mã hóa để bảo vệ sự riêng tư ng use => giấu dấu vết ng use
- Hạn chế: hiệu năng/ thiếu sót, xử lý chậm (video, file)

b. **VPN:** Tạo một kết nối an toàn và mã hóa giữa thiết bị của người dùng và máy chủ VPN, giúp che giấu địa chỉ IP thật.

- Ưu điểm: Bảo vệ thông tin cá nhân và cho phép truy cập vào các nội dung bị chặn.
- Nhược điểm: Nhà cung cấp VPN có thể thấy địa chỉ IP thật của người dùng.

c. Proxy Chaining:

- **Proxy:** Sử dụng nhiều máy chủ proxy để định tuyến lưu lượng truy cập, giúp che giấu địa chỉ IP gốc.
- **Ưu điểm:** Tăng cường bảo mật và ẩn danh = cách use nhiều lớp proxy.
- **Nhược điểm:** làm giảm tốc độ truy cập do phải đi qua nhiều máy chủ.

4. <u>Các giai đoạn</u>

- **Gđ 1: trinh sát**
  + Tìm kiếm, thu thập TT về mục tiêu, gồm các hđ of cty, KH
  + Trinh sát thụ động: thu thập TT mà k cần txuc với mục tiêu
  + _____ chủ động: tương tác với mục tiêu
- **Gđ 2: Dò quét** HT (dựa trên TT đã thu thập => dò quét)
- **Gđ 3: Truy cập**
  + Truy cập vào HĐH, phần mềm + Truy cập ở mức HĐH, mức ứng dụng, mức mạng
  + Nâng quyền => kiểm soát toàn bộ HT
- **Gđ 4: Duy trì đăng nhập**
  + có quyền truy cập => muốnduy trì quyền kiểm soát hệ thống
  + Sử dụng các công cụ như backdoor, rootkit hoặc Trojan
  +Khai thác dữ liệu trên hệ thống đã kiểm soát
  +Sử dụng các hệ thống đã kiểm soát để làm bàn đạp tấn công các hệ thống khác
- **Gđ 5: xóa dấu vết** (che dấu hvi tấn công = xóa bản ghi log, dấu các phần mềm độc hại)

5. Một số kĩ thuật tấn công

a. **Tấn công mật khẩu:** tấn công cổ điển chiếm quyền truy cập = tìm ra mk, tên đn
   - Vét cạn: + use tổ hợp kí tự + mật khẩu đã đc mã hóa
     + chuỗi mã hóa = cuỗi mk thu đc => mật khẩu
   - Từ điển
     + use file từ điển có sẵn chứa các hash – so với passwork để tìm ra plaint text
     +thêm/đảo kí tự
   - Kết hợp: tốc độ crack chỉ mất vài phút nếu có sẵn hash

b. **Tấn công giả mạo**: tình huống 1ng/1 chương tình giả thành công = 1ng khác = cách làm sai dữ liệu
   - Các loại tấn công (IP,MAC, URL, ARP, DNS, email)
     + IP: use IP giả để lừa máy nạn nhân vượt qua hàng rào ksoat an ninh
     + Tại sao dễ dàng giả mạo IP: do lỗi cấu hình router, router chỉ qtam địa chỉ đích, việc xác thực chỉ dựa trên địa chỉ nguồn, thay đổi các trg trog IP dễ
     + MAC: nghe lẽn địa chỉ MAC => truy cập => nhận đc all lưu tượng đi từ máy nạn nhân tới đích

c. **Sniffer: là** công cụ "bắt" các tt lưu chuyển trên mạng
   + bắt các tt trao đổi giữa nhiều trạm làn với nhau
   + **hđtheo cơ chế: mạng dạng quảng bá** dl đc truyền theo mõi hướng, các trạm bỏ qua TT để trao đổi giữa trạm nguồn – đích, ngtac roadcast(qba) các gói tin trong ethernet
   + Mức độ nguy hiểm: rất nguy hiểm vì thực hiện ở tầng rất thấp of hệ thống
   + Sniffer thụ động: nghe + bắt all gói tin lưu thông trên mạng, khó phát hiện
   + Sniffer chủ động: đánh lừa giao thức phân giải địa chỉ/ tấn công làm tràn lưu lượng
   + **Các biện pháp hạn chế:**
     - mã hóa đường truyền, k use hub, use mã hóa cho k dây và kênh cáp
     - xd chính sách bảo vệ mạng
     - qli hệ thống = quy định => hạn chế khả năng xâm nhập về mặt vật lí
     - kiểm tra tiến trình trên hệ thống

d. **Tấn công MitM:** lợi dụng quá trình chuyển gói tin đi qua nhiều trạm thuộc các mạng khác nhau, kẻ tấn công chặn bắt thông điệp giữa 2 bên, có thể xem, sửa, chuyển cho bên kia
   - Kịch bản tấn công: Có thể xảy ra trong mạng LAN hoặc từ local tới remote thông qua các phương pháp như giả mạo DNS, phá hoại ARP, và chuyển hướng ICMP.
   - Công cụ sử dụng: Các công cụ như ettercap, dsniff, và IRPAS.

e. **Session hijacking (tấn công chiếm quyền điều khiển)**: Kẻ tấn công chiếm q` điều khiển 1 phiên giao tiếp giữa hai bên = cách gửi các gói tin TCP giả mạo.
   - Sử dụng mã hóa để bảo vệ thông tin trong quá trình truyền tải, ngăn chặn kẻ tấn công không thể chèn lưu lượng có ý nghĩa.
   - Lấy quyền điều khiển của 1 phía trong kết nối TCP: kết hợp sniffer+ spoofing
   - Chi tiết tấn công: tấn công ở giữa Alice + Bob => nhảy vào, gửi gói TCP tới BoB, địa chỉ IP nguồn = IP of Alice => **phòng thủ: mã hóa**

f. **Tấn công từ chối DV (DoS): cản trở ng dùng hợp pháp truy cập vào HT**
   - **2 loại tấn công:**
     + logic: dựa vào lỗi phần mềm → DV ngưng hđ/ giảm hiệu năng
     + gây ngập lụt: gửi 1 lg lớn y/c gây cạn kiệt tài nguyên ht or băng thông
   - **Các dạng tấn công**
     + SYN floods: kĩ thuật gây ngập lụt các gói tin mở TCP, gây cạn kiệt máy chủ
     + Smurf: use kiểu quảng bá có định hướng để gây ngập lụt, gửi 1 lg lớn ICMP (Ping) với địa chỉ IP nguồn → địa chỉ qba
   - **Các kĩ thuật:**
     + Land: gửi gói tin giả mạo với địa chỉ nguồn và đích giống nhau, là 1 loại tấn công of Dos lớp 4
     + Ping of death:gửi gói tin ping quá kích cỡ, 1ping=56byte, nếu > 655536 byte -máy sập
     + Jolt2 or Teardrop, Newtear, Bonk, Syndrop:

   ❖ **DDoS là 1 dạng of Dos**, chiếm giữ nhiều máy, gọi là bots (máy dễ bị công kích)
   - Phòng thủ:
     + k để cho hệ thống ng dùng trở thành bot + lọc các gói tin nguy hiểm
     + dự phòng tài nguyên lớn + chữ ký, phát hiện bất thường, giới hạn tốc độ

g. **Tấn công lặp lại**: kẻ tấn công tái use các cuộc liên lạc trc
   - Các bước: chặn thông điệp → truyền lại thông điệp tới host đích ban đầu
   - Why thực hiện? + Chiếm quyền truy cập tới tài nguyên = cách lặp lại thông điệp xác thực + Trong tấn công DoS, đc dùng để gây nhiễu host đích

h. **Tấn công DNS**: dừng DNS seerver gốc, dừng tip-level-domain, dừng server cục bộ
   - Phá hoại bộ đệm DNS: đưa các bản ghi giả vào DNS server
   - Tấn công server gốc: thành công, tấn công đầu độc + chuyển hướng: kk

i . Social engineering là lợi dụng sự ảnh hưởng và niềm tin để lừa một người → mục đích lấy cắp thông tin hoặc thuyết phục nạn nhân để thực hiện việc gì

- **Tấn công DoS/DDoS:**
  - Gửi lượng lớn yêu cầu khiến hệ thống quá tải.
  - DDoS khác DoS ở phạm vi tấn công:

- Số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm;
- Số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc trăm ngàn máy, và đến từ rất nhiều vị trí địa lý khác nhau trêntoàn cầu.

6. <u>Phishing và pharming</u>

- Phishing: giả mạo website, là 1 dạng của social engineering, lừa ng dùng để lấy thông tin cá nhân
- Pharming: tấn công vào trình duyệt dường dùng

CHƯƠNG 6

1. Khái quát

- **Tài sản:** thông tin, thiết bị, thành phần hỗ trợ hđ có liên quan đến thông tin
- **Quản lý ATTT:** 1 tiến trình nhằm đảo bảo TS qtrọng of DN đc bảo vệ với chi phí phù hợp

2. <u>Đánh giá rủi ro an toàn TT</u>

a. **<u>PP đường cơ sở:</u>** thực thi các kiểm soát an ninh ở mức cơ bản
- Ưu điểm: + k đòi hỏi chi phí cho tài nguyên bổ sung, cùng nhóm các bf có thể triển khai nhiều ht
- Nhược điểm: k xem xét kĩ điều kiện nảy sinh, mức đường cơ sở đc xđ chung → k phù hợp

b. **<u>PP k chính thức:</u>** thực hiện 1 số dạng ptich rủi ro, use kiến thức chuyên gia, k thực hiện đza toàn diện rủi ro
- Ưu điểm: k đòi hỏi nhân viên phân tích rủi ro, thực hiện nhanh với chi phí thấp
- Nhược điểm: đza k đc thực hiện toàn diện → rủi k xem xét kĩ, kết quả đza phụ thuộc vào quan điểm cá nhân
- Phù hợp với quy mô nhỏ và vừa, nguồn lực hạn chế

c. **<u>PP phân tích chi tiết rủi ro:</u>** là pp đza toàn diện, thực hiện chính thức
- Ưu điểm; cho phép xem chi tiết rủi tom giải thích rõ ràng, cung cấp TT tốt nhất
- Nhược: chi phí lớn về time, nguồn lực, yêu cầu → chậm trễ trong việc đưa ra giải pháp
- Phù hợp với tổ chủ chính phủ, các tổ chức quy mô lớn\

d. **<u>PP kết hợp:</u>** kết hợp 3c trên
- Mục tiêu: cung cấp mức bảo vệ hợp lí → ktra và điều chỉnh bf

3. ISO/IEC 27001:2005 (tiêu chuẩn về quản lý thông tin)

a. <u>Plane</u>
- Đề ra phạm vi,chính sách of ISMS, hướng tiếp cận đza rủi ro
- Nhận dạng, đza rủi ro, các lựa chọn pp xử lý
- Lựa chọn mục tiêu và biện pháp kiểm soát

b. <u>Do</u>
- Xây dựng kế hoạch
- Thực thi kế hoạch, kiểm soát, chương trình đào tạo chuyên môn
- Quản lý các hđ, tài nguyên
- Twhjc thi thủ tục phát hiện và phản ứng lại sự cố an ninh

c. <u>Check</u>

- Thực thi thủ tục giám sát, đánh giá thường xuyên tính hiệu quả của ISMS và qli
- Thực hiện việc kiểm toán (audit) nội bộ với ISMS;
- Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS;

d. <u>Act</u>

- Thực hiện các cải tiến đã được nhận dạng, ▪ Thực hiện các hđ sửa chữa và ngăn chặn;
- Áp dụng các bài đã được học
- Thảo luận kết quả với các bên quan tâm
- Đảm bảo các cải tiến đạt được các mục tiêu

❖**Các kiểu luật:**

▪ **Luật dân sự:** là luật điều chỉnh các quan hệ dân sự giữa các tổ chức và cá nhân trong một quốc gia;

▪ **Luật hình sự:luật** điều chỉnh các hành vi gây hại cho xã hội và nhà nước

▪ **Luật công cộng:** quy định cấu trúc của các đơn vị hành chính, các quan hệ giữa công dân với công dân, giữa các tổ chức và quan hệ với các chính phủ các nước khác;

▪ **Luật riêng:** điều chỉnh các quan hệ trong phạm vi hẹp

❖**Các luật ATTT của Mỹ:**

▪ Các luật tội phạm máy tính ▪ Các luật về sự riêng tư ▪ Luật xuất khẩu và chống gián điệp ▪ Luật bản quyền ▪ Luật tự do thông tin

❖**Các luật ATTT và tổ chức luật quốc tế:** ▪ Hội đồng châu Âu về chống tội phạm mạng ▪ Hiệp ước bảo vệ quyền sở hữu trí tuệ.

❑**Luật Việt Nam về ATTT**

❖Luật An ninh mạng của Việt Nam được Quốc hội thông qua vào tháng 6 năm 2018 và có hiệu lực từ 1/1/2019:

▪ Quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật trên không gian mạng.

❖**Vấn đề vi phạm bản quyền phần mềm:**

▪ Vấn đề vi phạm bản quyền phần mềm ở mức rất nghiêm trọng, đặc biệt là tại các nước đang phát triển ở châu Á và châu Phi;

▪ Người dùng đa số có hiểu biết về vấn đề bản quyền phần mềm, nhưng coi việc sử dụng phần mềm bất hợp pháp là bình thường vì nhiều nước chưa có quy định hoặc không xử lý nghiêm vi phạm

❖**Vấn đề lạm dụng các tài nguyên của công ty, tổ chức:**

▪ Một số công ty/tổ chức chưa có các quy định cấm nhân viên sử dụng các tài nguyên của công ty, tổ chức vào việc riêng. Một số có quy định nhưng chưa được thực thi chặt chẽ và chưa có chế tài xử phạt nghiêm minh;

▪ Các hành vi lạm dụng thường gặp:

▪ In ấn tài liệu riêng;

▪ Sử dụng email cá nhân cho việc riêng;

▪ Tải các tài liệu/files không được phép;

▪ Cài đặt và chạy các chương trình/phần mềm không được phép;

Sử dụng máy tính công ty làm việc riêng;

▪ Sử dụng các loại phương tiện làm việc khác như điện thoại công ty quá mức vào việc riêng
NOTE: quá trình thu thập thông tin trên máy đích → scanning
Ngăn chặn các user hợp lệ truy xuất các tài nguyên hệ thống → DoS

Chương 3: Phần mềm mã độc

1. Phân loại phần mềm mã độc

- **Theo đặc tính thi hành:**
  - Lệ thuộc ứng dụng chủ: Virus.
  - Thực thi độc lập: Worm.
- **Theo khả năng tự sao chép:**
  - Có khả năng tự sao: Virus, Worm.
  - Không tự sao: Trojan.
- **Phân loại phần mềm độc hại**
  - **Virus**: Đoạn mã thực thi ghép vào chương trình chủ và giành quyền điều khiển khi chương trình chủ thực thi
    - Virus được thiết kế nhằm nhân bản, tránh né sự phát hiện, phá hỏng/thay đổi dữ liệu, hiển thị thông điệp hoặc làm cho hệ điều hành hđ sai lệch
      - **Virus ký sinh:** ký sinh vào các tập tin thi hành trên hệ thống đích
      - **Boot virus:** nhiễm vào mẫu tin khởi động (512byte), multi_parite: loại virus tổ hợp tính năng của virus ký sinh và boot virus
      - **Macro virus:** đính vào các tập tin dl có use maccro, data virus tự động thực hiện khi tập dl nhiễm đc mở bởi ứng dụng chủ
      - **Email virus:** sử dụng email với tập tin đính kèm có chứa 1 virus macro, kích hoạt khi ng dùng mở tập tin đính kèm,..
  - **Worm**: Là phần mềm độc hại có khả năng tự sao chép và lây lan qua mạng mà không cần sự can thiệp của người dùng, lợi dụng quyền ng dùng để phát tán hoặc khai thác lỗ hổng ht
    - **Cách thức lây lan**: Thường qua email, mạng xã hội hoặc các lỗ hổng bảo mật.
  - **Trojan (ngựa thành troa)**: Là chương trình có vẻ hợp pháp nhưng thực chất chứa mã độc, cho phép kẻ tấn công truy cập vào hệ thống.
    - **Cách thức hoạt động**: Thường được phát tán qua các ứng dụng hoặc trò chơi hấp dẫn.
    - Chương trình có ẩn tác dụng phụ, thường là bề ngoài hấp dẫn như trò chơi, nâng cấp phần mềm
    - Khi chạy thực hiện một số tác vụ bổ sung: ▪ Chophépkẻtấncôngtruy cập giántiếp
    - Thường được sử dụng để truyền bá một virus/sâu hoặc cài đặt một backdoor
    - Hoặc đơn giản chỉ để phá hủy dữ liệu

- **Ransomware**: Là phần mềm mã hóa dữ liệu của nạn nhân và yêu cầu tiền chuộc để giải mã.
  - **Tác hại**: Gây thiệt hại lớn cho cá nhân và tổ chức, làm mất dữ liệu quan trọng.
- **Spyware**: Là phần mềm gián điệp, thu thập thông tin cá nhân mà không có sự đồng ý của người dùng.
  - **Tác hại**: Rò rỉ thông tin cá nhân, làm giảm hiệu suất hệ thống.
- **Rootkit:** giúp hacker khống chế hệ thống ở mức cao nhất, có thể sửa đổi các khối cơ sở, 1 rootkit đc cài như công cụ quản trị máy cáo, sau đó nạp OS nạn nhân vào máy ảo để khiến antivirus k phát hiện
- **Spyaware và Adware**

  ❖Spyware (phần mềm gián điệp): rất đa dạng, thường k gây nguy hại về mặt dữ liệu

  ❖Tác hại của spyware: ▪ Rờithông tin cá nhân ▪ Tiêuthụtài nguyên máyđích ▪ Hệthốngmấtổnđịnh

  ❖Spyware lây nhiễm qua download phần mềm

  ❖Adware: spyware quảng cáo
- **Bot và botnet:** ❖Bot biến máy tính nạn nhân thành một zombie, khi đó kẻ tấn công có thể điều khiển được từ xa. ❖Rất nhiều zombie tập hợp thành botnet– thường bao gồm hàng trăm nghìn PC

2. Giải pháp phòng chống mã độc

- Sử dụng phần mềm diệt virus.
- Cập nhật hệ điều hành và ứng dụng thường xuyên.
- Giám sát mạng để phát hiện mã độc lây lan.

3. Loại bỏ các nguy cơ

3.1 Sử dụng phần mềm diệt virus

- Đảm bảo loại bỏ các nguy cơ từ phần mềm mã độc
- **Tính năng:** quét thành phần quan trọng, theo dõi hệ thống trong tgian thực, theo dõi hành vi của phần mềm phổ dụng, quét các file để ktra virus, thực hiện cadc hđ loại bỏ, cô lập, ngăn ngừa phần mềm mã độc

3.2 Sử dụng công cụ phát hiện và loại bỏ phần mềm mã độc

3.3 Sử dụng hệ thống IPS

- Sử dụng các chữ ký của các loại tấn công + phân tích về mạng + giao thức để phát hiện hành vi độc hại
- Giúp ngăn chặn phần mềm mã độc = phát viện + chặn mối đe dọa ch biết
- IPS giúp vảo vệ thành phần k được phần mềm diệt virus bảo vệ như DNS, chặn lưu lượng lớn phát sinh từ phần mềm mã độc

3.4 Tường lửa và bộ định tuyến

- Tường lửa: bảo vệ mạng và HT khỏi mối đe dọa từ bên ngoài
  + Giúp bảo vệ mục tiêu k được phần mềm diệt virus và IPS theo dõi bảo vệ
  + Chặn phần mềm mã độc với địa chỉ IP cụ thể
  + ngăn phần mềm mã độc phát tán
- Bộ định tuyến: đứng trc tường lửa → phát hiện hđ kết nối internet
  + Ktra đơn giản cho gđ mạng (lọc đầu vào, đầu ra, chặn phần mềm mã độc)

+ cấu hình để chặn hvi phát tán worm

3.5 Cầu hình ứng dụng

- Nhiều phần mềm mã độc sử dụng các tính năng của các ứng dụng phổ biến như email client, trình duyệt Web, hay soạn thảo văn bản để lây nhiễm và phát tán.
- Người dùng cần vô hiệu hóa các tính năng không cần thiết để hạn chế khả năng phát tán của phần mềm mã độc

4. Phương pháp phát hiện và loại trừ phần mềm mã độc

4.1 Quét cổng đáng ngờ

- Trojan sử dụng các cổng rảnh rỗi để kẻ tấn công duy trì kết nối ❖Cần kiểm tra các kết nối đến các địa chỉ IP đáng ngờ
- Công cụ: netstat, currport, TCPView

4.2 Quét các tiến trình chạy đáng ngờ

- Trojan nguyej trang bản thân = dvu/giấu tiến trình hoạt động của mình
- Trojan đưa mã vào các tiến trình khác → sinh ra tiến trình k thể nhìn thấy
- Sử dụng công cụ giám sát để phát hiện

4.3 Quét các registry đáng ngờ

- Windows thực hiện tự động chạy các lệnh trong một số mục registry khi khởi động
- Quét các giá trị registry cho các mục đáng ngờ liên quan đến Trojan do chúng chèn dữ liệu để chỉ dẫn thực hiện hoạt động
- Sử dụng các công cụ quét registry: regsho

4.4 Quét các trình điều khiển thiết bị đáng ngờ

- Trojan được cài đặt cùng với các trình điều khiển thiết bị tải về từ các nguồn không tin cậy
- Quét và xác minh các trình điều khiển đáng ngờ xem có phải chính hãng không
- Công cụ: Driverview, Driverscanner

5. Phương pháp xử lý, loại trừ phần mềm mã độc

5.1 Chuẩn bị

5.2 Phát hiện và phân tích

5.3 Ngăn chặn, loại bỏ, khôi phục

a. Ngăn chặn

- 2 thành phần chính: ngăn chặn sự lây lan của phần mềm độc hại và ngăn chặn thiệt hại thêm cho hệ thống
- Người sử dụng tham gia:
- Tự động phát hiện
- Vô hiệu hóa dịch vụ (đóng/khóa dvu được use bởi phần mềm độc hại có chứa 1 sự cố và cần hiểu đc hậu quả)
- Vô hiệu hóa kết nối: đặt các hạn chế bổ sung trên kết nối mạng chứa sự cố phần mềm độc hại

b. **Loại bỏ:** xóa bỏ phần mềm độc hại khỏi ht bị nhiễm

c. Khôi phục

5.4 Hoạt động sau sự cố

Nắm được bài học sau việc xử lý sự cố phần mềm độc hại giúp cải thiện khả năng xử lý sự cố và phòng chống phần mềm độchại ▪ Thayđổichínhsáchbảomật ▪ Thayđổicấuhìnhphầnmềm ▪ Thay đổi trong việc phát hiện phần mềm độc hại và triển khai phần mềm phòng chốn