UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

BẢO MẬT
HỆ THỐNG THÔNG TIN

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Nội dung

Tầm quan trọng của bảo mật thông tin

Các mối đe dọa và rủi ro bảo mật trong hệ thống thông tin

Chính sách, quy trình và công nghệ bảo mật thông tin

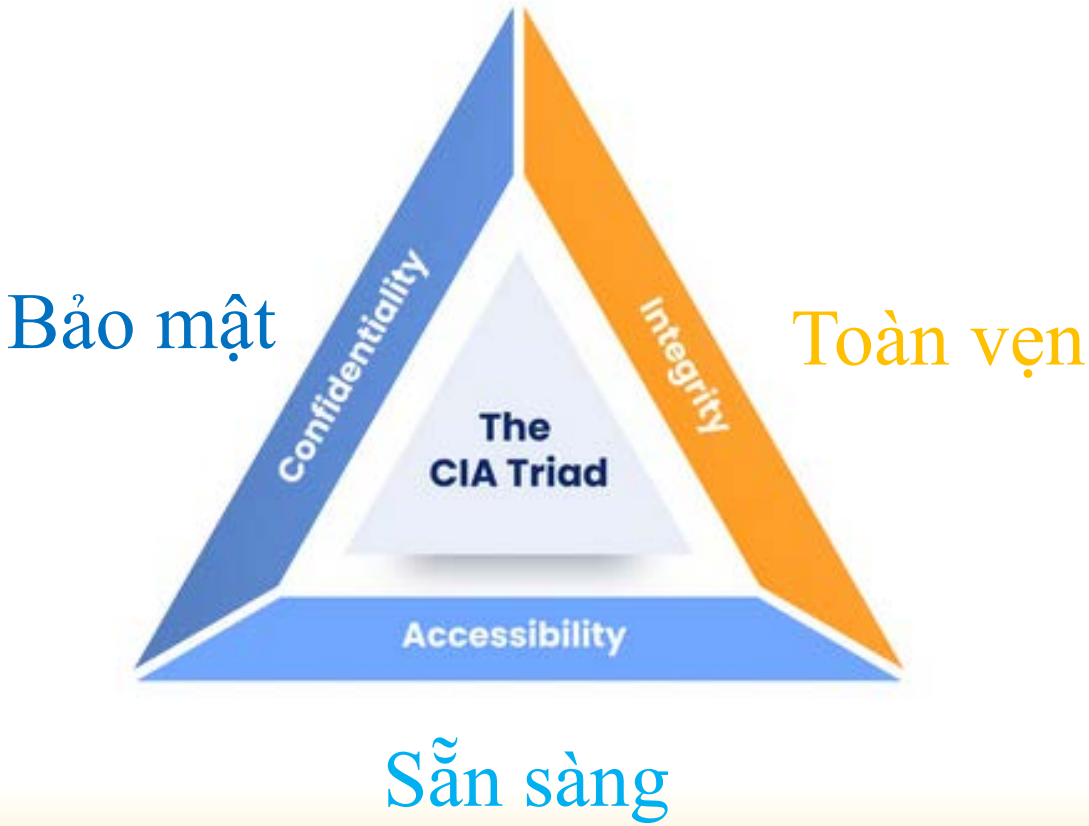
Bảo mật mạng, bảo vệ dữ liệu và quản lý truy cập người dùng

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Bảo mật hệ thống thông tin

Bảo mật HTTT

Bảo mật hệ thống thông tin (Information Systems Security): là bảo vệ hệ thống **chống lại** việc truy cập, sử dụng, chỉnh sửa, phá hủy, làm lộ và làm gián đoạn thông tin và hoạt động của hệ thống một cách trái phép



Những yêu cầu bảo mật

- **Tính bảo mật (Confidentiality):** bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép

Ví dụ: Sử dụng mã hóa SSL/TLS cho các giao dịch trực tuyến để đảm bảo rằng thông tin tài khoản khách hàng (số tài khoản, mật khẩu) không bị hacker đánh cắp khi truyền qua internet

- **Tính toàn vẹn (Integrity):** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu

Ví dụ: Sử dụng cơ chế checksum hoặc mã hóa SHA-256 để kiểm tra tính toàn vẹn của dữ liệu giao dịch

Những yêu cầu bảo mật (tt)

- **Tính sẵn sàng (Availability):** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu

Ví dụ: Trong hệ thống ngân hàng, cần đảm bảo rằng khách hàng có thể truy vấn thông tin số dư tài khoản bất kỳ lúc nào theo như quy định

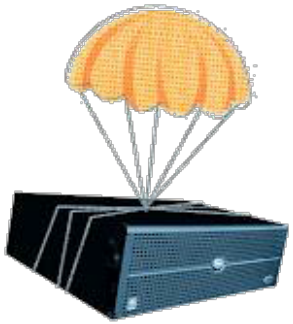
- **Tính không thể chối bỏ (Non-repudiation):** Đảm bảo rằng một bên không thể phủ nhận việc đã thực hiện hành động nào đó, như gửi hoặc nhận dữ liệu

Ví dụ: Trong hệ thống ngân hàng, có khả năng cung cấp bằng chứng để chứng minh một hành vi khách hàng đã làm, như rút tiền, chuyển tiền

Mục tiêu của bảo mật (tt)

Ngăn chặn kẻ tấn công vi phạm các chính sách bảo mật

Phát hiện các vi phạm chính sách bảo mật



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

Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công

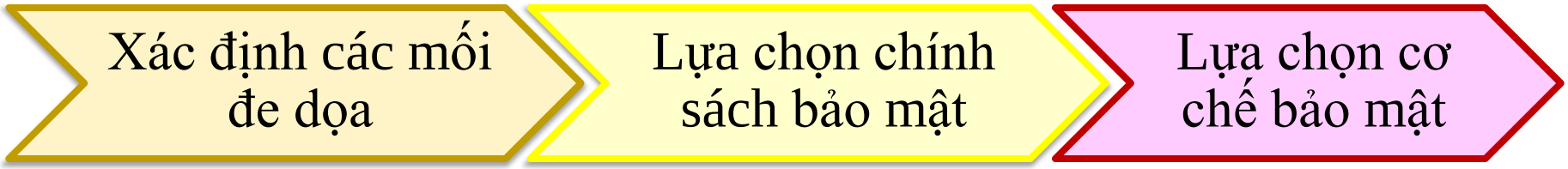
- **Mối đe dọa (Threat):** là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống. Các tài nguyên hệ thống bao gồm phần cứng, phần mềm, cơ sở dữ liệu, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…
- **Các điểm yếu hệ thống (System weaknesses):** là các lỗi hay các khiếm khuyết tồn tại trong hệ thống. Nguyên nhân của sự tồn tại các điểm yếu có thể do lỗi thiết kế, lỗi cài đặt, lỗi lập trình, hoặc lỗi quản trị, cấu hình hoạt động

Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công (tt)

- **Lỗ hổng bảo mật (Security vulnerability):** là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó, bao gồm tính toàn vẹn, tính bí mật, tính sẵn dùng. Nói chung, lỗ hổng bảo mật tồn tại trong tất cả các thành phần của hệ thống
- **Tấn công (Attack):** là một, hoặc một chuỗi các hành động vi phạm các chính sách an ninh an toàn của cơ quan, tổ chức, gây tổn hại đến các thuộc tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và mạng

Tấn công = Mối đe dọa + Lỗ hổng

Các bước cơ bản trong bảo mật



- **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

Xác định các mối đe dọa

- **Xác định các mối đe dọa (threat)**
  - 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

Lỗi và thiếu soát của người dùng

- Mối đe dọa của hệ thống thông tin xuất phát từ những lỗi bảo mật, lỗi thao tác của những người dùng trong hệ thống
- Là mối đe dọa hàng đầu đối với một hệ thống thông tin
- **Giải pháp:**
  - Huấn luyện thao tác, hạn chế sai sót
  - Sử dụng nguyên tắc quyền tối thiểu (least privilege)
  - Thường xuyên backup hệ thống

Gian lận và đánh cắp thông tin

- Mối đe dọa này do những kẻ tấn công từ bên trong hệ thống (inner attackers), gồm những người dùng giả mạo hoặc những người dùng có ý đồ xấu
- Những người tấn công từ bên trong luôn rất nguy hiểm
- **Giải pháp:**
  - Định ra những chính sách bảo mật tốt: có chứng cứ xác định được kẻ tấn công từ bên trong

Kẻ tấn công nguy hiểm

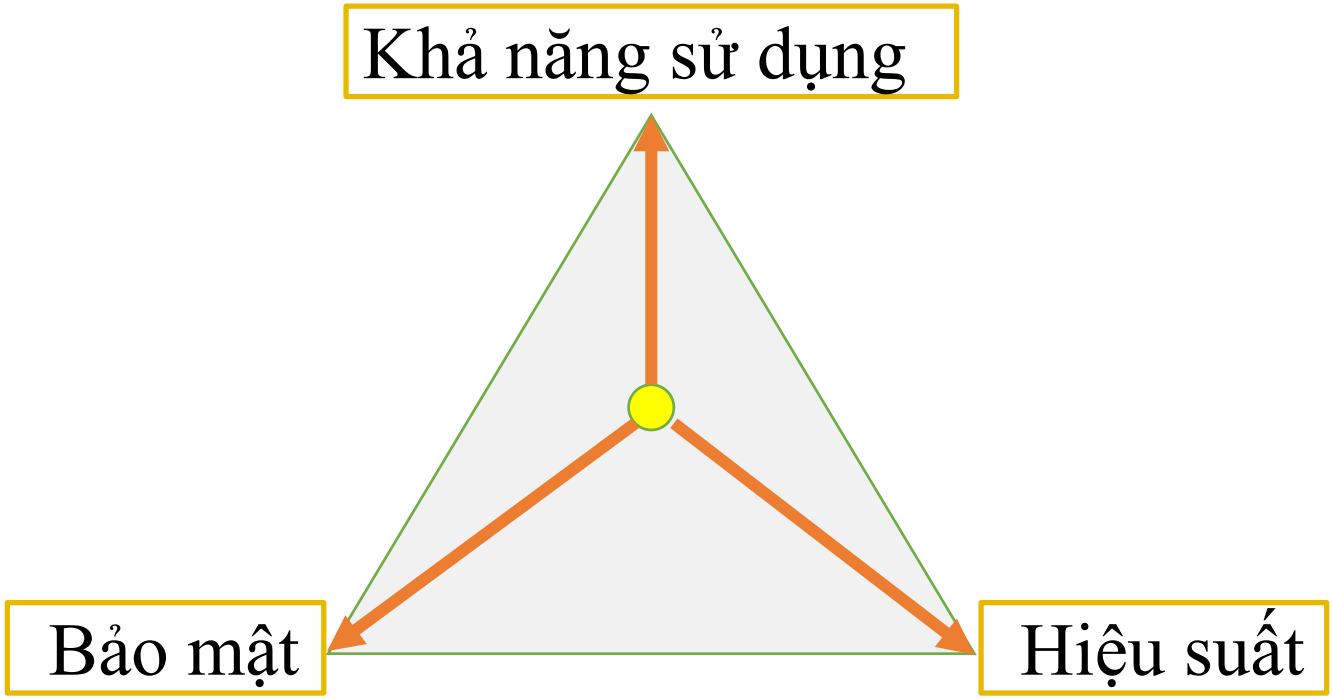
- Kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm thông tin, phá hủy dữ liệu, phá hủy hệ thống
- **5 bước để tấn công vào một hệ thống:**
  - Thăm dò (Reconnaisance)
  - Quét lỗ hổng
  - Cố gắng lấy quyền truy cập (Gaining access)
  - Duy trì kết nối (Maintaining access)
  - Xóa dấu vết (Cover his track)

Lựa chọn chính sách bảo mật

Lựa chọn chính sách bảo mật

- Việc bảo mật hệ thống cần có một chính sách bảo mật rõ ràng
- Cần có những 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 như: NIST, SP800, ISO17799, HIPAA

Lựa chọn chính sách bảo mật (tt)



Lựa chọn chính sách bảo mật

- 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)

Điều khiển truy cập

Điều khiển truy cập (Access control): là cơ chế điều khiển, quản lý các truy cập vào hệ thống cơ sở dữ liệu

- **Các bước trong điều khiển truy cập:**

Định danh (Identification):
Người dùng cung cấp thông tin để định danh

1

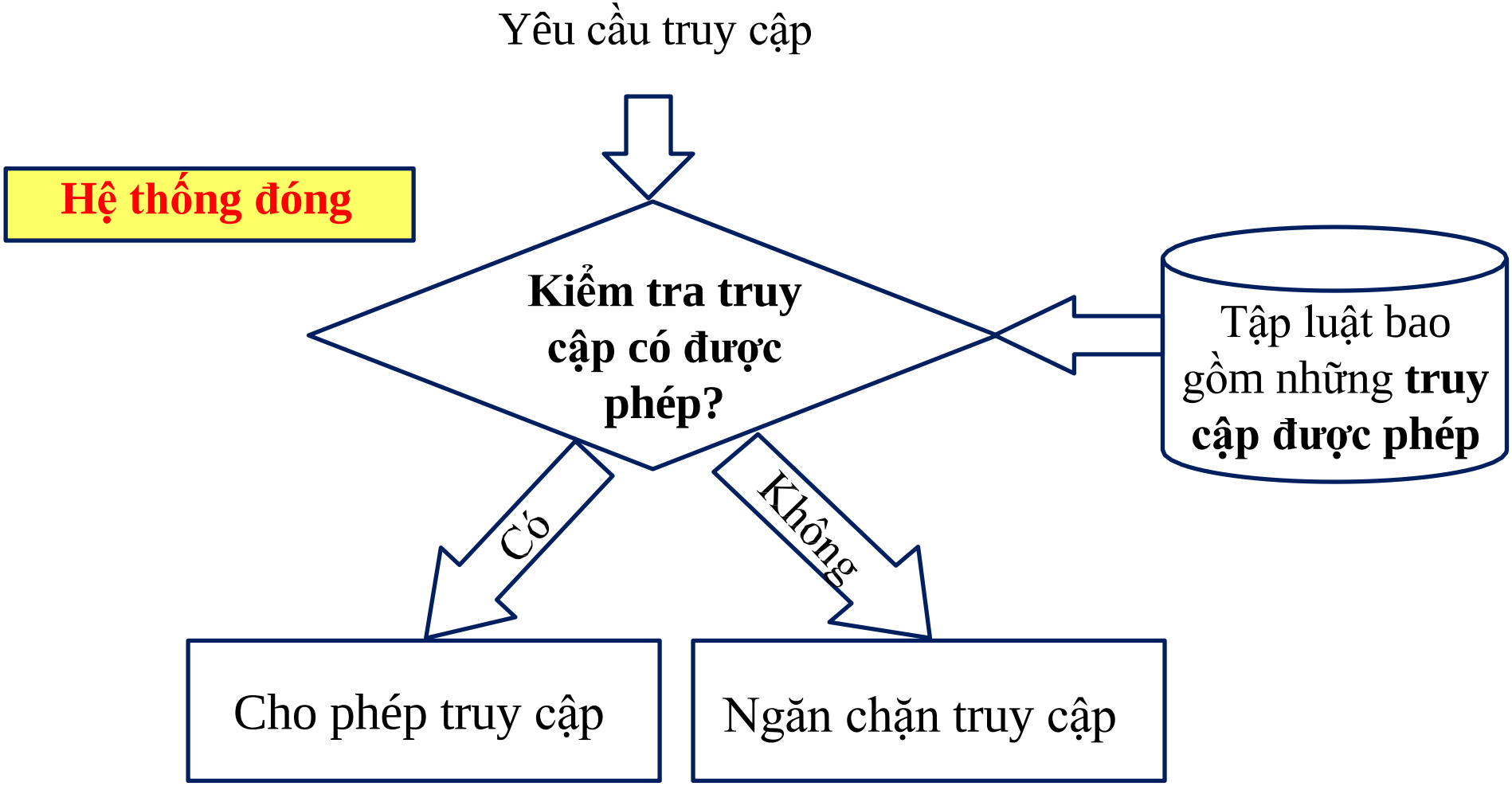
Xác thực (Authentication):
Người dùng chứng minh danh định đó là đúng

2

Ủy quyền (Authorization):
Xác định quyền mà người dùng có

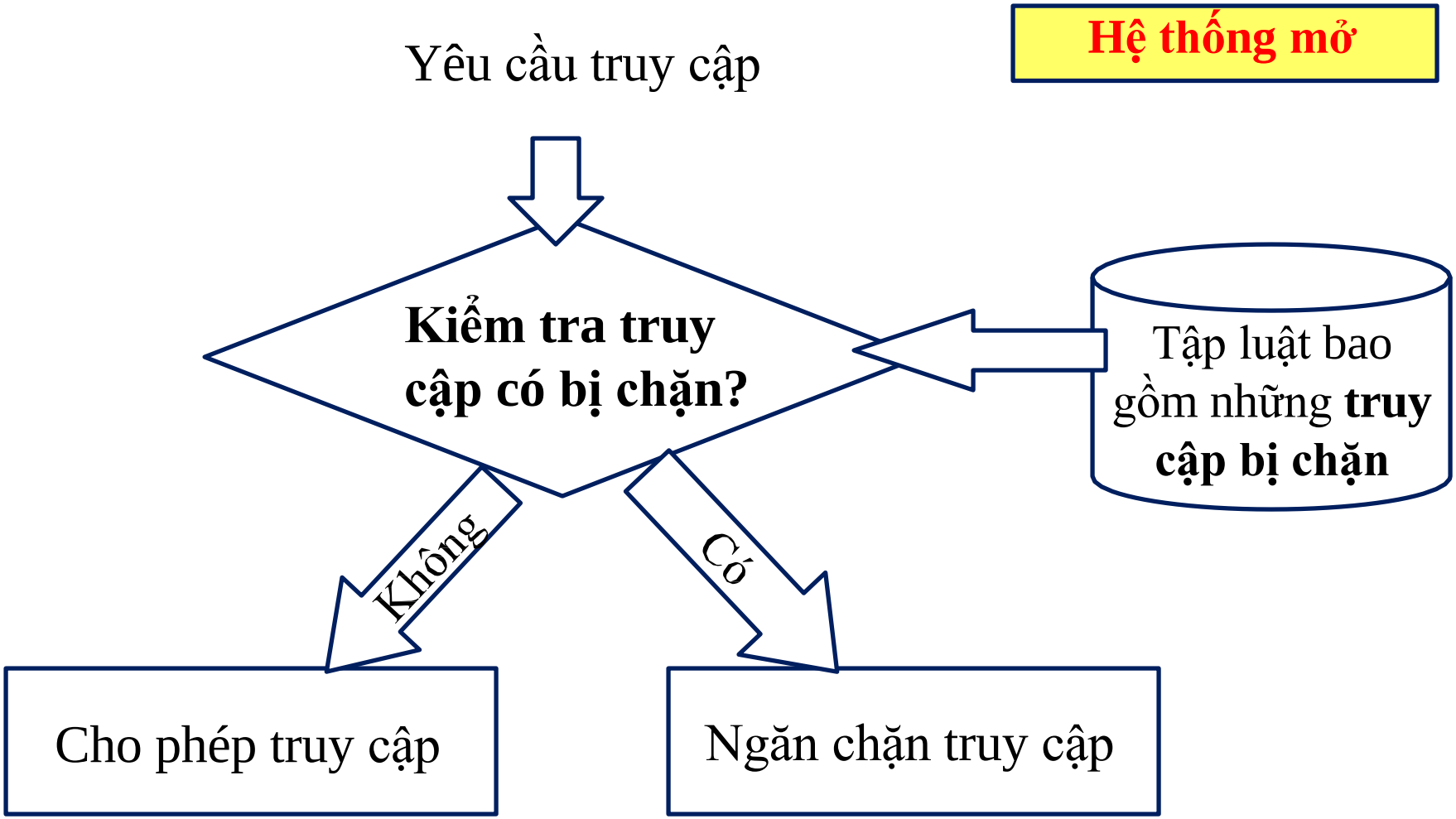
3

2 loại hệ thống điều khiển



2 loại hệ thống điều khiển (tt)

Hệ thống mở



Mã hóa

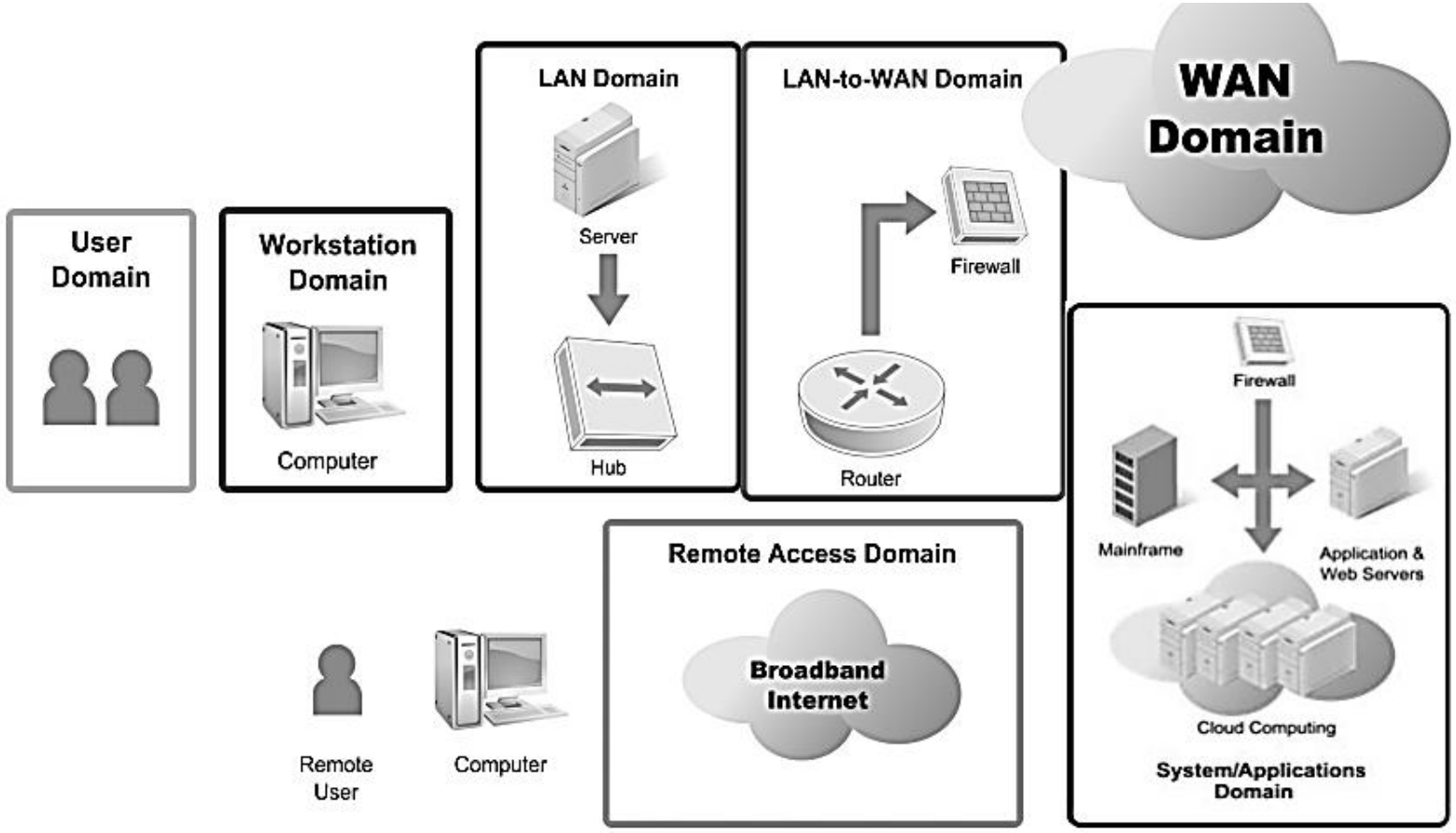
- Mã hóa (Encryption) là những giải thuật tính toán nhằm chuyển đổi những văn bản gốc (plaintext), dạng văn bản có thể đọc được, sang dạng văn bản mã hóa (cyphertext), dạng văn bản không thể đọc được
- Chỉ người dùng có được khóa đúng mới có thể giải mã được văn bản mã hóa về dạng văn bản rõ ban đầu
- Mã hóa dữ liệu được sử dụng để bảo vệ những dữ liệu nhạy cảm

Các thành phần cần bảo mật trong HTTT

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Bảy vùng trong cơ sở hạ tầng CNTT

- Hạ tầng công nghệ thông tin (IT Infrastructure) của các cơ quan, tổ chức, doanh nghiệp có thể có quy mô lớn hay nhỏ khác nhau, nhưng thường gồm bảy vùng theo mức kết nối mạng



Vùng người dùng

Vùng có nhiều mối đe dọa và nguy cơ nhất do người dùng có bản chất khó đoán định và khó kiểm soát hành vi

- **Các vấn đề thường gặp như:**
  - Thiếu ý thức, coi nhẹ vấn đề an ninh an toàn, vi phạm các chính sách an ninh an toàn
  - Đưa CD/DVD/USB với các file cá nhân vào hệ thống
  - Tải ảnh, âm nhạc, video trái phép
  - Phá hoại dữ liệu, ứng dụng và hệ thống
  - Các nhân viên bất mãn có thể tấn công hệ thống từ bên trong, hoặc nhân viên có thể tống tiền hoặc chiếm đoạt thông tin nhạy cảm, thông tin quan trọng

Vùng máy trạm

Tiếp xúc trực tiếp với vùng người dùng

Các nguy cơ thường gặp gồm:

- Truy nhập trái phép vào máy trạm, hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành, trong các phần mềm ứng dụng máy trạm
- Các hiểm họa từ vi rút, mã độc và các phần mềm độc hại. Ngoài ra, vùng máy trạm cũng chịu các nguy cơ do hành vi bị cấm từ người dùng, như đưa CD/DVD/USB với các file cá nhân vào hệ thống

Vùng mạng LAN

- Truy nhập trái phép vào mạng LAN vật lý, truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành và các phần mềm ứng dụng máy chủ; nguy cơ từ người dùng giả mạo trong mạng WLAN
- Tính bí mật dữ liệu trong mạng WLAN có thể bị đe dọa do sóng mang thông tin của WLAN truyền trong không gian có thể bị nghe trộm
- Ngoài ra, các hướng dẫn và cấu hình chuẩn cho máy chủ LAN nếu không được tuân thủ nghiêm ngặt sẽ dẫn đến những lỗ hổng an ninh mà tin tặc có thể khai thác

Vùng mạng LAN – to - WAN

- Vùng chuyển tiếp từ mạng nội bộ ra mạng diện rộng, nên nguy cơ lớn nhất là tin tặc từ mạng WAN có thể thăm dò và rà quét trái phép các cổng dịch vụ, nguy cơ truy nhập trái phép
- Ngoài ra, một nguy cơ khác cần phải xem xét là lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác

Vùng mạng WAN

- Vùng mạng WAN, hay mạng Internet là vùng mạng mở, trong đó hầu hết dữ liệu được truyền dưới dạng rõ, nên các nguy cơ lớn nhất là dễ bị nghe trộm và dễ bị tấn công phá hoại
- Tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS)
- Kẻ tấn công có thể tự do, dễ dàng gửi email có đính kèm vi rút, sâu và các phần mềm độc hại

Vùng truy cập từ xa

- Tấn công kiểu vét cạn vào tên người dùng và mật khẩu, tấn công vào hệ thống đăng nhập và điều khiển truy nhập
- Truy nhập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu
- Các thông tin bí mật có thể bị đánh cắp từ xa
- Vấn đề rò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu

Vùng hệ thống và ứng dụng

- Truy nhập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp
- Các khó khăn trong quản lý các máy chủ với yêu cầu tính sẵn dùng cao
- Các lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ
- Các vấn đề an ninh trong các môi trường ảo của điện toán đám mây
- Vấn đề hỏng hóc hoặc mất dữ liệu

Những mối đe dọa an toàn thông tin (Các dạng tấn công và phần mềm độc hại)

Các loại tấn công

Các mối đe dọa và rủi ro bảo mật trong hệ thống thông tin năm 2025 tiếp tục phát triển với sự gia tăng của công nghệ mới và các phương thức tấn công tinh vi

- Mã nguy hiểm (Phần mềm độc hại)
- Mã độc tống tiền (Ransomware)
- Lừa đảo qua mạng
- Tấn công có chủ đích (APT - Advanced Persistent Threat)
- Tấn công từ chối dịch vụ
- Lừa đảo phi kỹ thuật (Social engineering)
- Tấn công chuỗi cung ứng (Supply chain attack)

Mã nguy hiểm

- Mã nguy hiểm là một đoạn mã không mong muốn được nhúng trong một chương trình nhằm thực hiện các truy cập trái phép vào hệ thống máy tính để thu thập các thông tin nhạy cảm, làm gián đoạn hoạt động hoặc gây hại cho hệ thống máy tính
- **Bao gồm:** virus, worm, trojan horses, spyware, adware, backdoor, …

Mã nguy hiểm (tt)

Ví dụ: WannaCry (2017)

Cách thức: Worm khai thác lỗ hổng EternalBlue trên Windows

Hậu quả: Tấn công hàng trăm ngàn máy tính, mã hóa dữ liệu, yêu cầu tiền chuộc

Phòng tránh: Cập nhật phần mềm, dùng phần mềm diệt virus, sao lưu dữ liệu

Mã độc tống tiền

Mã độc mã hóa dữ liệu, yêu cầu tiền chuộc để giải mã

- **Lây lan qua:** Email lừa đảo, phần mềm độc hại
- **Đặc điểm:** Tiền chuộc thường bằng Bitcoin, gây mất dữ liệu hoặc thiệt hại tài chính
- **Tác động:** Gián đoạn hoạt động doanh nghiệp, tổ chức

Ví dụ: Ryuk (2018)

- **Cách thức:** Lây qua email lừa đảo hoặc trojan
- **Hậu quả:** Mã hóa dữ liệu tổ chức lớn, yêu cầu tiền chuộc hàng triệu USD
- **Phòng tránh:** Không mở email nghi ngờ, dùng tường lửa, sao lưu định kỳ

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Lừa Đảo Qua Mạng (Phishing)

Tấn công dùng email, tin nhắn, hoặc website giả mạo để lừa lấy thông tin nhạy cảm

- **Mục tiêu:** Mật khẩu, thông tin tài khoản ngân hàng, dữ liệu cá nhân
- **Dấu hiệu:** Email từ nguồn lạ, yêu cầu nhấp liên kết hoặc cung cấp thông tin
- **Tác động:** Mất cắp danh tính, thiệt hại tài chính

Ví dụ: Email Giả Mạo Ngân Hàng (2023)

- **Cách thức:** Email giả danh ngân hàng yêu cầu "xác minh tài khoản", dẫn đến website giả
- **Hậu quả:** Người dùng mất tiền, bị đánh cắp danh tính
- **Phòng tránh:** Kiểm tra địa chỉ email, không nhấp liên kết lạ, dùng xác thực hai yếu tố

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Tấn Công Có Chủ Đích (APT)

Tấn công tinh vi, kéo dài, nhắm vào tổ chức, chính phủ

- **Đặc điểm:** Do nhóm hacker có tổ chức, được tài trợ
- **Mục tiêu:** Đánh cắp dữ liệu nhạy cảm, gián điệp, phá hoại hệ thống
- **Phương thức:** Khai thác lỗ hổng, kỹ thuật xã hội, mã độc tùy chỉnh

Ví dụ: SolarWinds (2020)

- **Cách thức:** Hacker chèn mã độc vào bản cập nhật phần mềm SolarWinds Orion
- **Hậu quả:** Dữ liệu nhạy cảm từ chính phủ, doanh nghiệp bị đánh cắp
- **Phòng tránh:** Giám sát mạng, kiểm tra phần mềm từ nguồn tin cậy, phát hiện bất thường

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Tấn công từ chối dịch vụ

Tấn công làm quá tải hệ thống, mạng hoặc website bằng lưu lượng truy cập lớn, khiến dịch vụ bị gián đoạn

- **Mục tiêu:** Làm tê liệt hoạt động của website, ứng dụng hoặc mạng
- **Phương thức:** Sử dụng nhiều thiết bị (botnet) để gửi yêu cầu ồ ạt đến mục tiêu
- **Tác động:** Gây gián đoạn kinh doanh, mất uy tín, thiệt hại tài chính

Ví dụ: Mirai Botnet (2016)

- **Cách thức:** Sử dụng botnet từ các thiết bị IoT bị nhiễm (camera, router) để tấn công các nhà cung cấp DNS như Dyn
- **Hậu quả:** Nhiều website lớn (Twitter, Netflix, Reddit) bị gián đoạn trong nhiều giờ
- **Phòng tránh:** Sử dụng giải pháp chống DDoS, giám sát lưu lượng mạng, cập nhật bảo mật thiết bị IoT

Lừa đảo phi kỹ thuật

- Social engineering sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó
- Kẻ tấn công có thể lợi dụng các đặc điểm sau của con người để tấn công:
  - Mong muốn trở nên hữu dụng
  - Tin người
  - Nỗi sợ gặp rắc rối
  - Đơn giản đến mức cẩu thả

Lừa đảo phi kỹ thuật (tt)

- Social engineering dựa trên con người liên quan đến sự tương tác giữa con người với con người để thu được thông tin mong muốn:
  - Nhân viên gián điệp/ giả mạo
  - Giả làm người cần được giúp đỡ
  - Giả làm người quan trọng
  - Giả làm người được ủy quyền
  - Giả làm nhân hỗ trợ kỹ thuật

Lừa đảo phi kỹ thuật (tt)

- Social engineering dựa trên máy tính: liên quan đến việc sử dụng các phần mềm để cố gắng thu thập thông tin cần thiết:
  - Phising: lừa đảo qua thư điện tử
  - Vishing: lừa đảo qua điện thoại
  - Pop-up Windows
  - File đính kèm trong email
  - Các website giả mạo
  - Các phần mềm giả mạo

Tấn công mạng sử dụng trí tuệ nhân tạo

- **Mô tả:** Tin tặc sử dụng AI để tự động hóa và tối ưu hóa các cuộc tấn công, như tạo mã độc thông minh, giả mạo danh tính (deepfake), hoặc tấn công lừa đảo (phishing) siêu cá nhân hóa
- **Rủi ro:** Khó phát hiện, tốc độ lây lan nhanh, và khả năng vượt qua các hệ thống bảo mật truyền thống

Ví dụ: Tấn công phishing sử dụng AI để tạo email hoặc tin nhắn giả mạo gần như không thể phân biệt với thật

Tấn công chuỗi cung ứng phần mềm

- **Mô tả:** Tin tặc nhắm vào các nhà cung cấp phần mềm hoặc dịch vụ để chèn mã độc vào chuỗi cung ứng, ảnh hưởng đến nhiều tổ chức
- **Rủi ro:** Phạm vi ảnh hưởng rộng, khó truy vết nguồn gốc, và thiệt hại lớn cho các doanh nghiệp phụ thuộc vào phần mềm bị xâm phạm

Ví dụ: Các vụ tấn công tương tự SolarWinds (2020) nhưng phức tạp hơn với công nghệ mới

Tấn công vào hệ thống đám mây

- **Mô tả:** Với sự phụ thuộc ngày càng lớn vào dịch vụ đám mây, tin tặc nhắm vào cấu hình sai, lỗ hổng API, hoặc đánh cắp thông tin xác thực để truy cập dữ liệu nhạy cảm
- **Rủi ro:** Rò rỉ dữ liệu, gián đoạn dịch vụ, và tổn thất uy tín doanh nghiệp

Ví dụ: Xâm phạm tài khoản quản trị đám mây do thiếu xác thực đa yếu tố (MFA)

Tấn công vào cơ sở hạ tầng quan trọng

- **Mô tả:** Các ngành như năng lượng, giao thông, y tế, và tài chính là mục tiêu của các cuộc tấn công mạng do tầm quan trọng chiến lược
- **Rủi ro:** Gây rối loạn xã hội, thiệt hại kinh tế lớn, và nguy cơ mất an ninh quốc gia

Ví dụ: Tấn công vào hệ thống điều khiển lưới điện hoặc bệnh viện

Đe dọa từ nội bộ (Insider Threats)

- **Mô tả:** Nhân viên, nhà thầu, hoặc đối tác cố ý hoặc vô tình làm rò rỉ dữ liệu, cung cấp quyền truy cập trái phép, hoặc gây ra sự cố bảo mật
- **Rủi ro:** Khó phát hiện, đặc biệt khi liên quan đến nhân viên có quyền truy cập cao

Ví dụ: Nhân viên bất mãn chia sẻ thông tin nhạy cảm với đối thủ cạnh tranh

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Giải pháp giảm thiểu mối đe dọa

- **Đào tạo nhân sự**
- **Áp dụng công nghệ tiên tiến:** Sử dụng AI và học máy để phát hiện và ngăn chặn tấn công thời gian thực
- **Cập nhật và vá lỗi:** Xác thực đa yếu tố (MFA): Triển khai MFA trên mọi hệ thống quan trọng
- **Mã hóa hậu lượng tử:** Chuẩn bị chuyển đổi sang các thuật toán mã hóa chống lại máy tính lượng tử
- **Giám sát và phản ứng nhanh:** Thiết lập hệ thống giám sát liên tục và kế hoạch ứng phó sự cố
- **Hợp tác quốc tế:** Chia sẻ thông tin về mối đe dọa mạng giữa các quốc gia và tổ chức

Chính sách bảo mật thông tin mới nhất

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Chính sách bảo mật thông tin

Một số văn bản pháp lý nổi bật có hiệu lực hoặc được đề xuất năm 2025 bao gồm:

- Luật Viễn thông 2023 (Hiệu lực từ 01/01/2025)
- Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân
- Đề xuất Luật An ninh mạng 2025
- Quyết định 2345/QĐ-NHNN của Ngân hàng Nhà nước (Hiệu lực từ 01/07/2024)
- Tiêu chuẩn quốc tế được áp dụng tại Việt Nam

Quy trình bảo mật thông tin

- **Đánh giá và kiểm tra hệ thống bảo mật**
  - Kiểm thử thâm nhập (Penetration Testing) và kiểm tra an toàn ứng dụng web để xác định lỗ hổng
  - Phối hợp đa phòng ban để thu thập thông tin về quy trình hoạt động và công nghệ, đảm bảo đánh giá toàn diện
  - Ưu tiên khắc phục lỗ hổng dựa trên mức độ nghiêm trọn

Quy trình bảo mật thông tin (tt)

- **Quản lý quyền truy cập đặc quyền:**
  - Giới hạn và giám sát quyền truy cập vào hệ thống quan trọng
  - Sử dụng các giải pháp như BeyondTrust Privileged Access Management (PAM) để quản lý tài khoản đặc quyền, giảm thiểu rủi ro lạm dụng quyền hạn

PAM: là giải pháp quản lý truy cập đặc quyền, giúp kiểm soát và giám sát các tài khoản có quyền cao trong hệ thống CNTT

- Quản lý mật khẩu đặc quyền
- Kiểm soát truy cập
- Giám sát và báo cáo
- Bảo mật điểm cuối và máy chủ
- Tích hợp và tự động hóa

Quy trình bảo mật thông tin (tt)

- **Diễn tập và ứng phó sự cố:**
  - Tổ chức các buổi mô phỏng tấn công mạng (phishing, ransomware, xâm nhập trái phép) để nâng cao kỹ năng ứng phó
  - Xây dựng quy trình phản ứng nhanh, bao gồm ghi lưu log file (tối thiểu 3 tháng) để điều tra và khắc phục sự cố

Quy trình bảo mật thông tin (tt)

- **Quản lý nhật ký hệ thống:**
  - Ghi nhận các sự kiện như đăng nhập, cấu hình, và truy xuất hệ thống để truy vết nguồn gốc sự cố
  - Tự động khóa tài khoản sau 3 lần đăng nhập sai liên tiếp và giám sát truy cập từ xa
- **Đào tạo nhân sự liên tục:**
  - Tổ chức các khóa học cập nhật hàng quý về xu hướng tấn công mạng và kỹ thuật bảo mật mới
  - Nâng cao nhận thức cho toàn bộ nhân viên, không chỉ đội ngũ IT
- **Tuân thủ quy định pháp lý**

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Công nghệ bảo mật thông tin mới nhất

- Trí tuệ nhân tạo (AI) và Học máy (Machine Learning)
- Blockchain
- Mã hóa hậu lượng tử (Post-Quantum Cryptography)
- Bảo mật đám mây
- Tường lửa và phần mềm chống xâm nhập
- Công nghệ nhận diện sinh trắc học
- Bảo mật thiết bị di động và IoT

Bảo mật mạng, bảo vệ dữ liệu và quản lý truy cập người dùng

Tại sao cần bảo mật mạng

- **Ngăn chặn các cuộc tấn công mạng:** mã độc, phishing, DDoS
- **Bảo vệ thông tin nhạy cảm:** dữ liệu khách hàng, tài sản trí tuệ
- **Đảm bảo tuân thủ các quy định pháp lý: GDPR, Luật An ninh mạng Việt Nam**
  - **Bảo mật mạng:** Các biện pháp bảo vệ hạ tầng mạng
  - **Bảo vệ dữ liệu:** Đảm bảo tính toàn vẹn, bí mật và sẵn sàng của dữ liệu
  - **Quản lý truy cập:** Kiểm soát quyền truy cập vào hệ thống và dữ liệu

Các mối đe dọa an ninh mạng phổ biến

- **Mã độc (Malware):** Virus, ransomware, spyware.Tấn công phishing: Lừa đảo qua email, tin nhắn
- **Tấn công DDoS:** Làm quá tải hệ thống mạng.
- **Tấn công SQL Injection:** Khai thác lỗ hổng cơ sở dữ liệu.

  ➔ Mất dữ liệu nhạy cảm, thiệt hại tài chính và uy tín, gián đoạn hoạt động kinh doanh

Sử dụng tường lửa (firewall) và phần mềm chống virus. Đào tạo nhân viên về nhận thức an ninh mạng.Cập nhật phần mềm và vá lỗi bảo mật định kỳ

Phương pháp bảo vệ dữ liệu

- **Tính bí mật (Confidentiality):** Chỉ người được ủy quyền mới truy cập được dữ liệu
- **Tính toàn vẹn (Integrity):** Dữ liệu không bị thay đổi trái phép
- **Tính sẵn sàng (Availability):** Dữ liệu luôn sẵn sàng khi cần

➔ Mã hóa dữ liệu, sao lưu dữ liệu, kiểm tra bảo mật định kỳ

Tuân thủ Luật An ninh mạng Việt Nam và các tiêu chuẩn quốc tế như ISO 27001. Xây dựng chính sách bảo vệ dữ liệu rõ ràng

Quản lý truy cập người dùng

- **Xác thực (Authentication):** Xác minh danh tính người dùng (mật khẩu, OTP, sinh trắc học)
- **Phân quyền (Authorization):** Quy định quyền truy cập của từng người dùng
- **Kiểm tra (Auditing):** Theo dõi và ghi lại hoạt động truy cập

Các phương pháp quản lý truy cập:

- **Mô hình RBAC (Role-Based Access Control):** Phân quyền dựa trên vai trò
- **Xác thực đa yếu tố (MFA):** Kết hợp mật khẩu, OTP, hoặc dấu vân tay
- **Zero Trust:** Không tin tưởng bất kỳ ai, luôn xác minh

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Kế hoạch triển khai

- **Đánh giá rủi ro:** Xác định các lỗ hổng trong hệ thống
- **Xây dựng chính sách bảo mật:** Quy định về mật khẩu, mã hóa, và truy cập
- **Áp dụng công nghệ:** Tường lửa, mã hóa, MFA, hệ thống SIEM (Security Information and Event Management)
- **Đào tạo nhân viên:** Nâng cao nhận thức về an ninh mạng
- Giám sát và cải thiện: Định kỳ đánh giá và cập nhật hệ thống

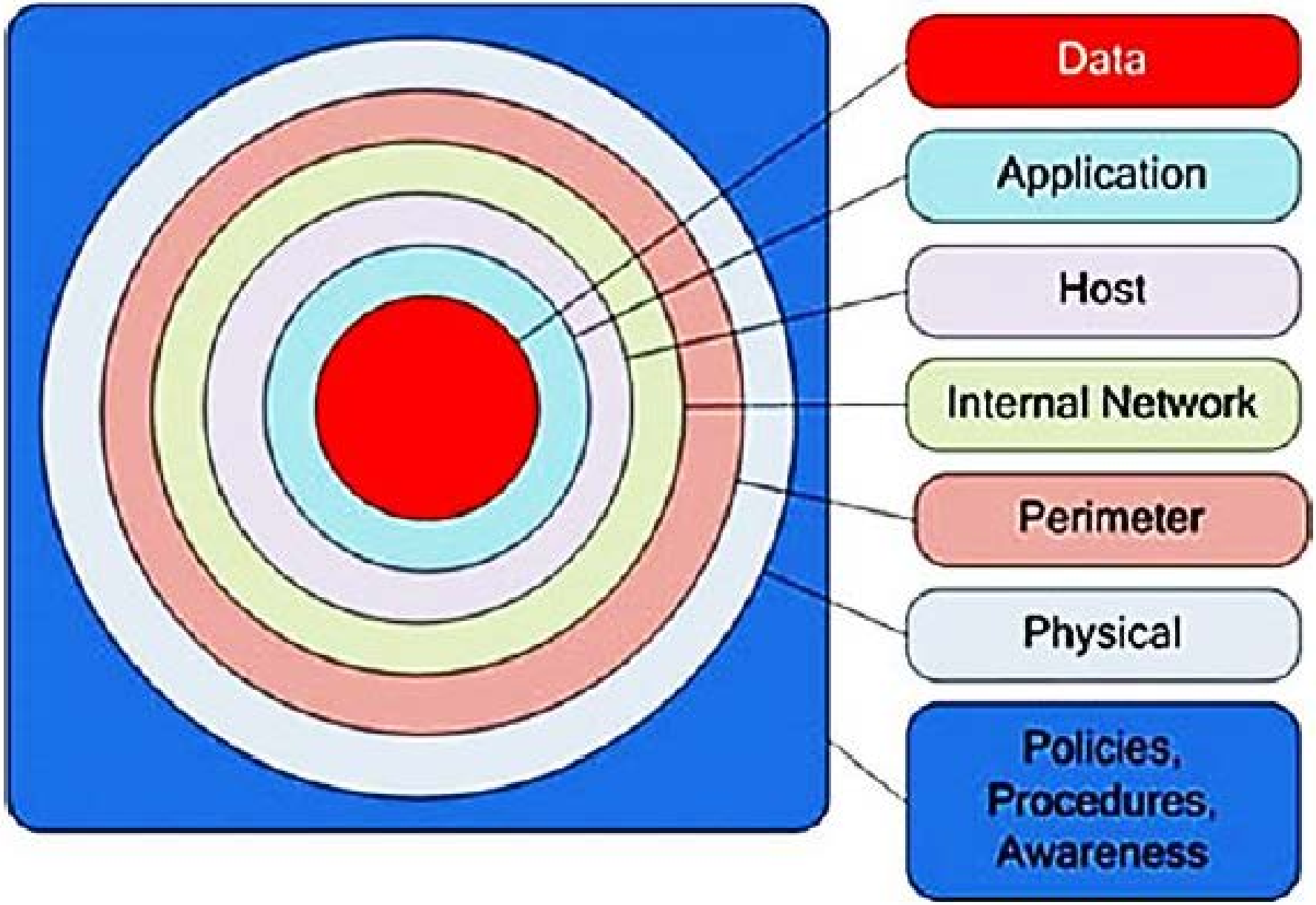
UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Khuyến nghị

- Đầu tư vào các giải pháp bảo mật hiện đại như AI và máy học để phát hiện mối đe dọa
- Thường xuyên sao lưu và kiểm tra khả năng khôi phục dữ liệu
- Xây dựng văn hóa an ninh mạng trong tổ chức

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Mô hình đảm bảo an toàn thông tin



UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

7 lớp bảo vệ

1. Ý thức (Policies, procedures, awareness)
2. Lớp vật lý (Physical)
3. Lớp ngoại vi (Perimeter)
4. Lớp mạng nội bộ (Internal network)
5. Lớp host (Host)
6. Lớp ứng dụng (Application)
7. Lớp dữ liệu (Data)

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Quy trình bảo mật HTTT

UTH UNIVERSITY OF TRANSPORT HOCHIMINH CITY

Case Study_An toàn bảo mật

Một công ty thương mại điện tử quy mô vừa, hoạt động trong lĩnh vực bán lẻ trực tuyến, đã phát hiện một vụ vi phạm bảo mật dữ liệu vào tháng 4 năm 2025. Thông tin cá nhân của hơn 500.000 khách hàng, bao gồm tên, địa chỉ, số điện thoại và một phần dữ liệu thẻ tín dụng, đã bị rò rỉ. Vụ việc gây ra thiệt hại tài chính và ảnh hưởng nghiêm trọng đến uy tín của công ty

Yêu cầu:

Phân tích nguyên nhân, tác động và các biện pháp khắc phục