An Toàn và Bảo Mật Hệ Thống Thông Tin

Dr. Hai Tran

About me

Google Scholar

Tran Son Hai

FOLLOW

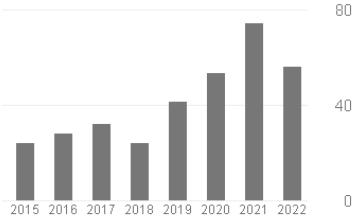
Information Technology Department
Verified email at hcmup.edu.vn
Computer Science and Com... Image Classification

GET MY OWN PROFILE

TITLE	CITED BY	YEAR
Image classification using support vector machine and artificial neural network LH Thai, TS Hai, NT Thuy International Journal of Information Technology and Computer Science 4 (5 ...	159	2012
A Facial Expression Classification System Integrating Canny, Principal Component Analysis and Artificial Neural Network TSH Le Hoang Thai, Nguyen Do Thai Nguyen International Journal of Machine Learning and Computing 1 (4)	56 *	2011
Applying Multi-CNNs model for detecting abnormal problem on chest x-ray images PN Kieu, HS Tran, TH Le, T Le, TT Nguyen 2018 10th International Conference on Knowledge and Systems Engineering (KSE ...	41	2018
Advertisement image classification using convolutional neural network	37	2017

Cited by VIEW ALL

	All	Since 2017
Citations	373	280
h-index	7	7
i10-index	7	7



Hoạt động tôi là ai

- https://docs.google.com/forms/d/e/1FAIpQLSeLR39a7o4FRBPIQX4pV1FQOv6tLwaf4ylYPKTZnAOUy3Upiw/viewform

- http://bit.ly/TTHV2023

Initial– Find a group

Nôi dung

- Khái niệm cơ bản về An toàn Thông tin
- Các loại mối đe dọa và tấn công
- Chính sách bảo mật thông tin
- Công nghệ mã hóa
- An ninh mạng
- An toàn dữ liệu
- Quản lý rủi ro
- Quy trình ứng phó sự cố và khôi phục sau sự cố bảo mật.

- **Bài 1: Giới thiệu về An toàn và Bảo mật Hệ thống Thông tin**
- **Nội dung**: Khái niệm cơ bản về an toàn thông tin, tầm quan trọng và các thành phần chính của hệ thống bảo mật.
- **Yêu cầu cần đạt**: Hiểu được các khái niệm cơ bản và tầm quan trọng của an toàn thông tin.
- **Thuật ngữ chính**: An toàn thông tin, bảo mật, rủi ro, mối đe dọa.
- **Câu hỏi thảo luận**: Tại sao an toàn thông tin lại quan trọng đối với doanh nghiệp?
- **Bài tập thực hành**: Nghiên cứu một trường hợp vi phạm an toàn thông tin gần đây và trình bày giải pháp bảo mật.
- **Bài tập lý thuyết**: Viết một bài luận ngắn về sự phát triển của an toàn thông tin trong thập kỷ qua.

- **Bài 2: Các loại mối đe dọa và tấn công**
- **Nội dung**: Phân loại các mối đe dọa, các loại tấn công mạng, và cách nhận diện chúng.
- **Yêu cầu cần đạt**: Nhận biết các loại mối đe dọa và tấn công phổ biến.
- **Thuật ngữ chính**: Malware, phishing, DoS, tấn công xã hội.
- **Câu hỏi thảo luận**: Mối đe dọa nào là nguy hiểm nhất hiện nay và tại sao?
- **Bài tập thực hành**: Mô phỏng một cuộc tấn công phishing và cách phát hiện nó.
- **Bài tập lý thuyết**: So sánh các loại tấn công mạng và đề xuất biện pháp phòng ngừa.

- **Bài 3: Chính sách bảo mật thông tin**
- **Nội dung**: Khái niệm và vai trò của chính sách bảo mật thông tin trong tổ chức.
- **Yêu cầu cần đạt**: Hiểu được cách xây dựng và triển khai chính sách bảo mật.
- **Thuật ngữ chính**: Chính sách bảo mật, quy trình, hướng dẫn.
- **Câu hỏi thảo luận**: Một chính sách bảo mật tốt cần có những yếu tố nào?
- **Bài tập thực hành**: Soạn thảo một mẫu chính sách bảo mật cho một doanh nghiệp nhỏ.
- **Bài tập lý thuyết**: Phân tích chính sách bảo mật của một tổ chức nổi tiếng.

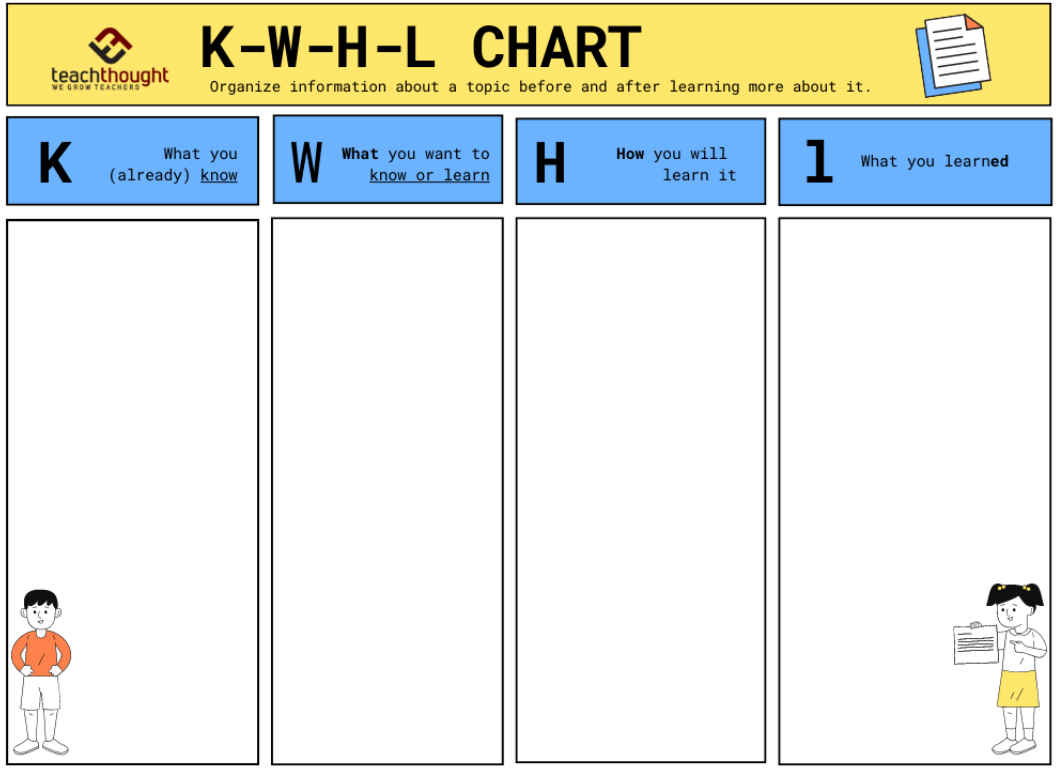
- **Bài 4: Công nghệ mã hóa**
- **Nội dung**: Giới thiệu các phương pháp mã hóa và ứng dụng của chúng trong bảo mật thông tin.
- **Yêu cầu cần đạt**: Nắm vững các khái niệm về mã hóa và giải mã.
- **Thuật ngữ chính**: Mã hóa đối xứng, mã hóa không đối xứng, chữ ký số.
- **Câu hỏi thảo luận**: Tại sao mã hóa lại quan trọng trong bảo mật thông tin?
- **Bài tập thực hành**: Thực hiện mã hóa và giải mã một thông điệp sử dụng AES.
- **Bài tập lý thuyết**: Trình bày sự khác biệt giữa mã hóa đối xứng và không đối xứng.

- **Bài 5: An ninh mạng**
- **Nội dung**: Kỹ thuật và công cụ bảo vệ mạng, bao gồm tường lửa, IDS/IPS.
- **Yêu cầu cần đạt**: Hiểu cách thức hoạt động của các công cụ bảo mật mạng.
- **Thuật ngữ chính**: Tường lửa, IDS, IPS, VPN.
- **Câu hỏi thảo luận**: Vai trò của tường lửa trong bảo mật mạng là gì?
- **Bài tập thực hành**: Cài đặt và cấu hình một tường lửa đơn giản.
- **Bài tập lý thuyết**: Phân tích các lỗi bảo mật mạng phổ biến và cách phòng tránh.

- **Bài 6: An toàn dữ liệu và sao lưu**
- **Nội dung**: Các phương pháp bảo vệ dữ liệu và quy trình sao lưu hiệu quả.
- **Yêu cầu cần đạt**: Nhận diện các phương pháp bảo vệ dữ liệu và lập kế hoạch sao lưu.
- **Thuật ngữ chính**: Sao lưu dữ liệu, phục hồi dữ liệu, mã hóa dữ liệu.
- **Câu hỏi thảo luận**: Tại sao việc sao lưu dữ liệu là cần thiết?
- **Bài tập thực hành**: Thiết lập một kế hoạch sao lưu cho một tổ chức.
- **Bài tập lý thuyết**: Trình bày các phương pháp sao lưu dữ liệu và lợi ích của chúng.

KWHL (KWLH)

1. What do I **(already) know**?
2. What do I **want** to know?
3. **How** can/should/will I learn it?
4. What **did** I learn?



Bài 1: Giới thiệu về An toàn và Bảo mật Hệ thống Thông tin

Thuật ngữ	Giải thích
An toàn thông tin	Bảo vệ thông tin khỏi các mối đe dọa, mất mát, truy cập trái phép và hư hỏng.
Bảo mật	Quy trình và công nghệ nhằm bảo vệ dữ liệu và thông tin khỏi truy cập không hợp lệ.
Rủi ro	Khả năng xảy ra sự cố hoặc sự kiện có thể gây thiệt hại cho thông tin hoặc hệ thống.
Mối đe dọa	Một yếu tố hoặc tình huống có khả năng gây hại cho an toàn thông tin, như virus hay tấn công mạng.
Tấn công mạng	Hành động có chủ đích nhằm xâm nhập, phá hoại hoặc lấy cắp thông tin từ hệ thống mạng.
Xác thực	Quy trình kiểm tra danh tính của người dùng hoặc hệ thống trước khi cho phép truy cập.
Phân quyền	Quá trình xác định ai có quyền truy cập và sử dụng tài nguyên trong hệ thống thông tin.
Bảo mật vật lý	Các biện pháp bảo vệ không gian vật lý của hệ thống thông tin, như kiểm soát ra vào.
Chính sách bảo mật	Tài liệu quy định các quy tắc và hướng dẫn nhằm bảo vệ thông tin trong tổ chức.
Đào tạo an toàn thông tin	Quá trình giáo dục nhân viên về các biện pháp bảo mật và cách nhận diện mối đe dọa.

- **Bài 1: Giới thiệu về An toàn và Bảo mật Hệ thống Thông tin**
- **Nội dung**: Khái niệm cơ bản về an toàn thông tin, tầm quan trọng và các thành phần chính của hệ thống bảo mật.
- **Yêu cầu cần đạt**: Hiểu được các khái niệm cơ bản và tầm quan trọng của an toàn thông tin.
- **Thuật ngữ chính**: An toàn thông tin, bảo mật, rủi ro, mối đe dọa.
- **Câu hỏi thảo luận**: Tại sao an toàn thông tin lại quan trọng đối với doanh nghiệp?
- **Bài tập thực hành**: Nghiên cứu một trường hợp vi phạm an toàn thông tin gần đây và trình bày giải pháp bảo mật.
- **Bài tập lý thuyết**: Viết một bài luận ngắn về sự phát triển của an toàn thông tin trong thập kỷ qua.

- **Bài 2: Các loại mối đe dọa và tấn công**
- **Nội dung**: Phân loại các mối đe dọa, các loại tấn công mạng, và cách nhận diện chúng.
- **Yêu cầu cần đạt**: Nhận biết các loại mối đe dọa và tấn công phổ biến.
- **Thuật ngữ chính**: Malware, phishing, DoS, tấn công xã hội.
- **Câu hỏi thảo luận**: Mối đe dọa nào là nguy hiểm nhất hiện nay và tại sao?
- **Bài tập thực hành**: Mô phỏng một cuộc tấn công phishing và cách phát hiện nó.
- **Bài tập lý thuyết**: So sánh các loại tấn công mạng và đề xuất biện pháp phòng ngừa.

Bài 2: Các loại mối đe dọa và tấn công

- **Những mối đe dọa từ tấn công mạng**
- 1. Tấn công Phishing (Lừa đảo trực tuyến)
- Phishing là một trong những hình thức tấn công phổ biến nhất, nhằm đánh lừa người dùng cung cấp thông tin nhạy cảm như tài khoản, mật khẩu, hoặc thông tin thẻ tín dụng. Kẻ tấn công thường gửi email hoặc tin nhắn giả mạo để dụ dỗ người dùng truy cập vào trang web giả mạo, từ đó chiếm đoạt thông tin.
- 2. Tấn công Malware (Phần mềm độc hại)
- Malware là phần mềm độc hại được kẻ tấn công sử dụng để xâm nhập vào hệ thống máy tính của nạn nhân nhằm đánh cắp dữ liệu, phá hủy hoặc làm gián đoạn hoạt động. Các loại Malware phổ biến bao gồm virus, ransomware, spyware, và trojan.
- 3. Tấn công DDoS (Tấn công từ chối dịch vụ)
- Tấn công DDoS xảy ra khi kẻ tấn công sử dụng một lượng lớn yêu cầu để làm quá tải hệ thống hoặc trang web, khiến nó không thể phục vụ người dùng bình thường. Điều này có thể làm gián đoạn hoạt động kinh doanh trong một thời gian dài.
- 4. Tấn công bằng cách lợi dụng lỗ hổng bảo mật
- Những lỗ hổng trong phần mềm hoặc hệ thống thường là mục tiêu dễ dàng cho kẻ tấn công. Chúng có thể khai thác những lỗ hổng này để xâm nhập và kiểm soát toàn bộ hệ thống.
- 5. Tấn công nội gián (Insider Threats)
- Đôi khi, mối đe dọa lại đến từ bên trong, từ những nhân viên hoặc đối tác có quyền truy cập vào hệ thống. Những người này có thể lợi dụng quyền hạn của mình để đánh cắp thông tin, làm gián đoạn hoạt động, hoặc gây thiệt hại cho tổ chức.

Bài 2: Các loại mối đe dọa và tấn công

- **Cách phòng ngừa tấn công mạng**
- 1. Xây dựng hệ thống Giám sát ATTT và SOC
- Hệ thống SOC đóng vai trò quan trọng trong việc giám sát, phát hiện và phản ứng kịp thời trước các mối đe dọa tấn công mạng. SOC là trung tâm điều hành an ninh, nơi các chuyên gia an ninh thông tin theo dõi và phân tích các hoạt động trong hệ thống để phát hiện những dấu hiệu bất thường hoặc nguy cơ tấn công. Giám sát ATTT giúp đảm bảo rằng mọi hoạt động và luồng dữ liệu đều được theo dõi chặt chẽ để phát hiện các hành vi nghi ngờ.
- 2. Nâng cao nhận thức về an ninh mạng
- Đào tạo và nâng cao nhận thức của nhân viên về an ninh mạng là một trong những biện pháp phòng ngừa hiệu quả nhất. Việc nhận diện các email, đường link và tệp tin đáng ngờ giúp giảm nguy cơ bị lừa đảo hoặc bị nhiễm phần mềm độc hại.
- 3. Cập nhật và vá lỗi phần mềm thường xuyên
- Các lỗ hổng bảo mật thường xuyên được phát hiện và khai thác bởi kẻ xấu. Do đó, việc cập nhật và vá lỗi hệ thống, phần mềm là cực kỳ quan trọng để bảo vệ tổ chức trước những mối đe dọa từ bên ngoài.
- 4. Sử dụng công cụ bảo mật tiên tiến
- Đảm bảo hệ thống được trang bị các công cụ bảo mật tiên tiến như tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), và giải pháp phòng chống phần mềm độc hại. Các công cụ này giúp giảm thiểu nguy cơ tấn công và bảo vệ toàn bộ hệ thống an ninh mạng. Bạn có thể tham khảo trọn bộ giải pháp và dịch vụ bảo mật ATTT của HPT, cung cấp đầy đủ các dịch vụ và giải pháp bảo mật cho doanh nghiệp.
- 5. Xác thực hai yếu tố (2FA)
- Xác thực hai yếu tố giúp tăng cường bảo mật bằng cách yêu cầu người dùng cung cấp hai hình thức xác thực trước khi truy cập vào tài khoản hoặc hệ thống. Điều này giúp ngăn chặn kẻ tấn công chiếm đoạt tài khoản ngay cả khi chúng có được mật khẩu.
- Tấn công mạng là một thực tế không thể tránh khỏi trong thời đại số hóa. Tuy nhiên, việc xây dựng một hệ thống SOC mạnh mẽ và triển khai quy trình giám sát ATTT hiệu quả có thể giúp doanh nghiệp phát hiện sớm và phòng ngừa các mối đe dọa này. Ngoài ra, nâng cao nhận thức an ninh mạng cho nhân viên và áp dụng các biện pháp bảo mật kỹ thuật tiên tiến là điều cần thiết để đảm bảo an toàn cho tổ chức.

Mối đe dọa an toàn HTTT

- Mục tiêu ATHTTT 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?**

THREAT – MỐI ĐE DỌA

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…)

THREAT – MỐI ĐE DỌA

Biện pháp phòng tránh

- Đảm bảo rằng các thành viên trong nhóm của bạn được 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. Họ nên đăng ký với các blog (như Wired) và podcast (như Techgenix Extreme IT) bao gồm những vấn đề này cũng như tham gia các hiệp hội chuyên nghiệp để họ có thể hưởng lợi từ việc chia sẻ tin tức, hội nghị và hội thảo trên web.
- 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.

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.

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?

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

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.

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 ngơời 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.

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.

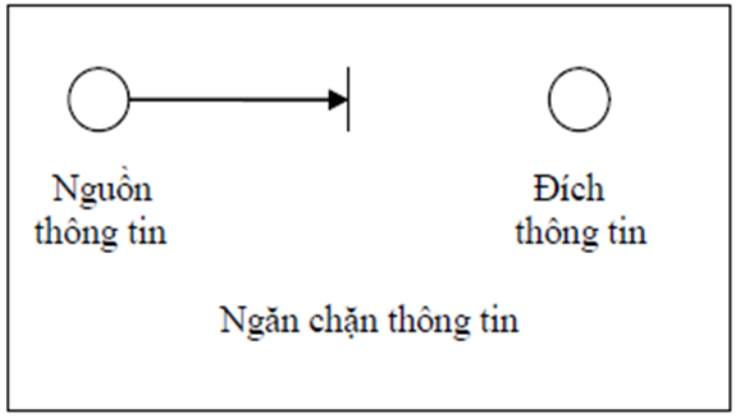
Các mối đe dọa thường gặp

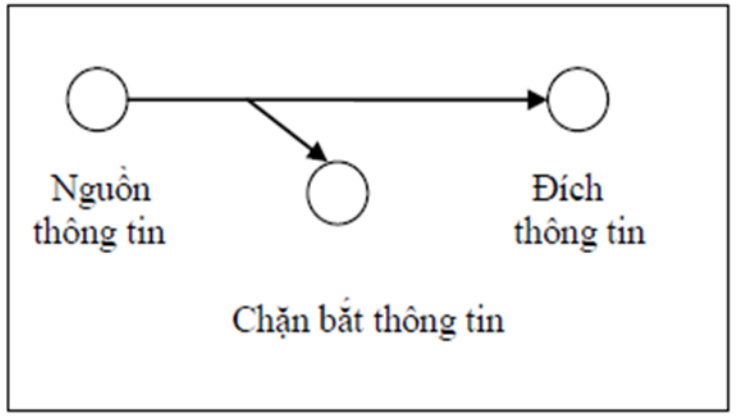
- Lỗi và thiếu sót của người dùng (Errors and Omissions)
- Gian lận và đánh cắp thông tin (Fraud and Theft)
- Kẻ tấn công nguy hiểm (Malicious Hackers)
- Mã độc (Malicious Code)
- Tấn công từ chối dịch vụ (Denial-of-Service Attacks)
- Social Engineering

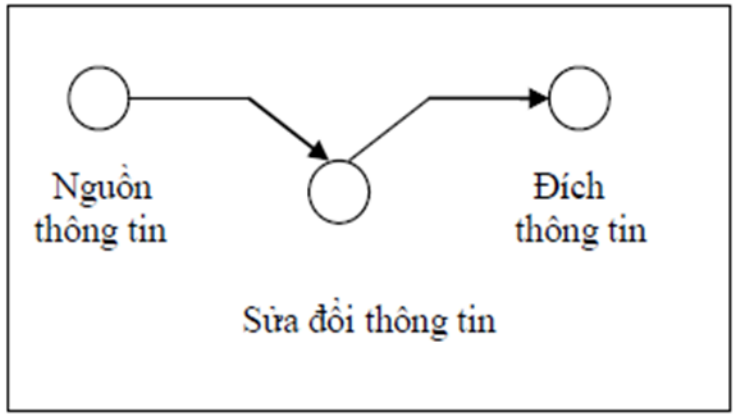
Các loại hình tấn công

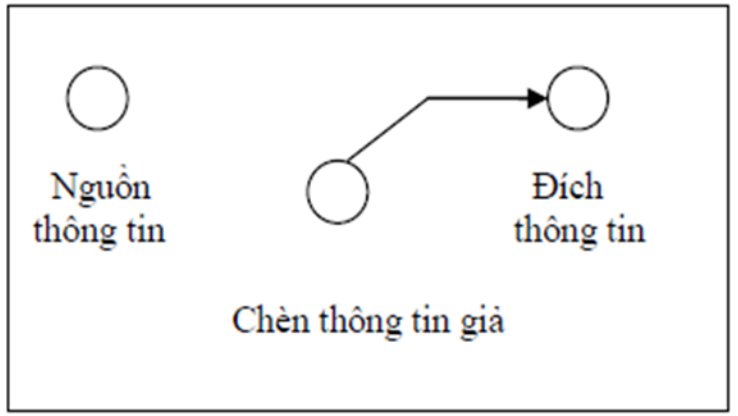
- **Định nghĩa chung**: Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.
- Tấn công HTTT là các tác động hoặc là trình tự liên kết giữa các tác động với nhau để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

Các loại hình tấn công (tiếp)



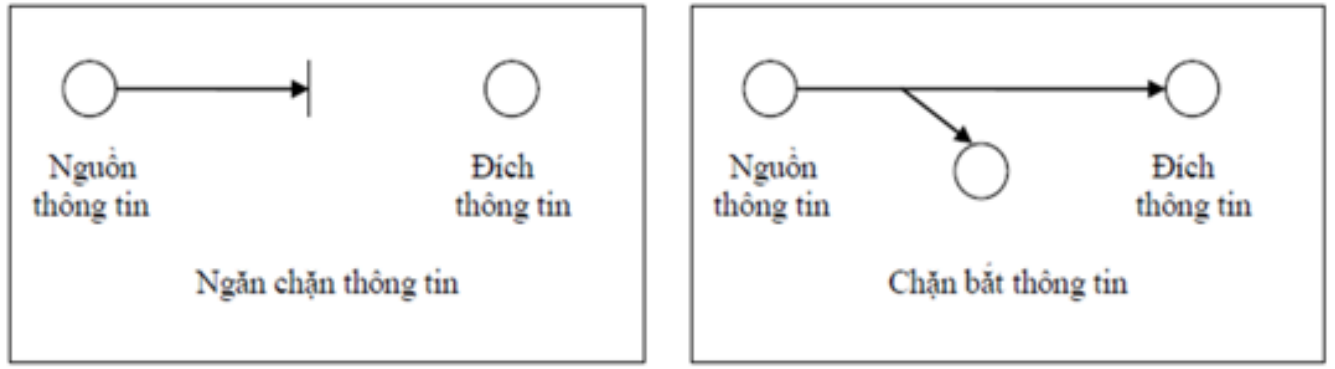






Các loại hình tấn công (tiếp)

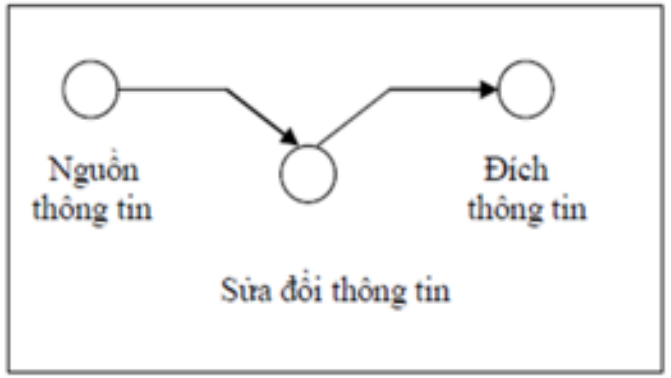
- **Tấn công ngăn chặn thông tin (interruption)**
  - Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- **Tấn công chặn bắt thông tin (interception)**
  - Kẻ tấn công có thể truy nhập tới tài nguyên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

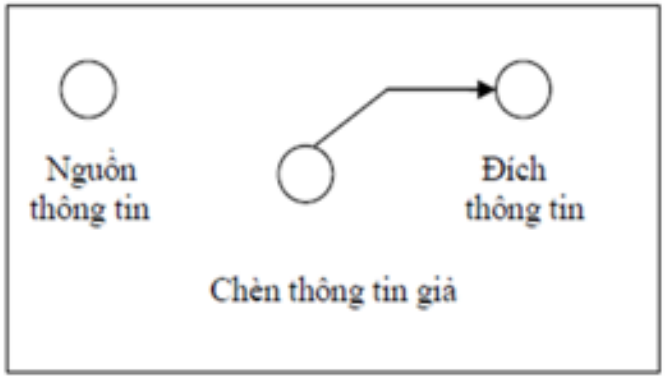


ı thông tin

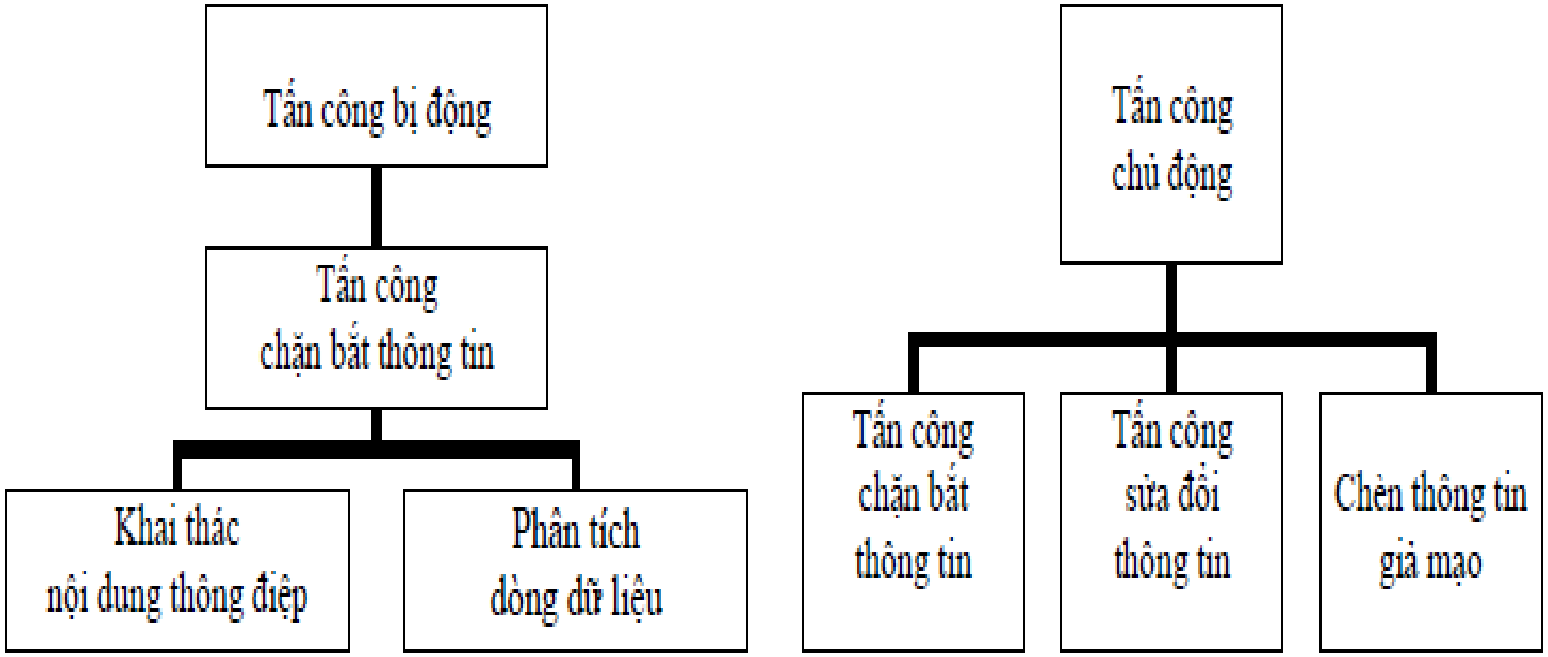
Các loại hình tấn công (tiếp)

- **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.





Tấn công bị động và chủ động



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).

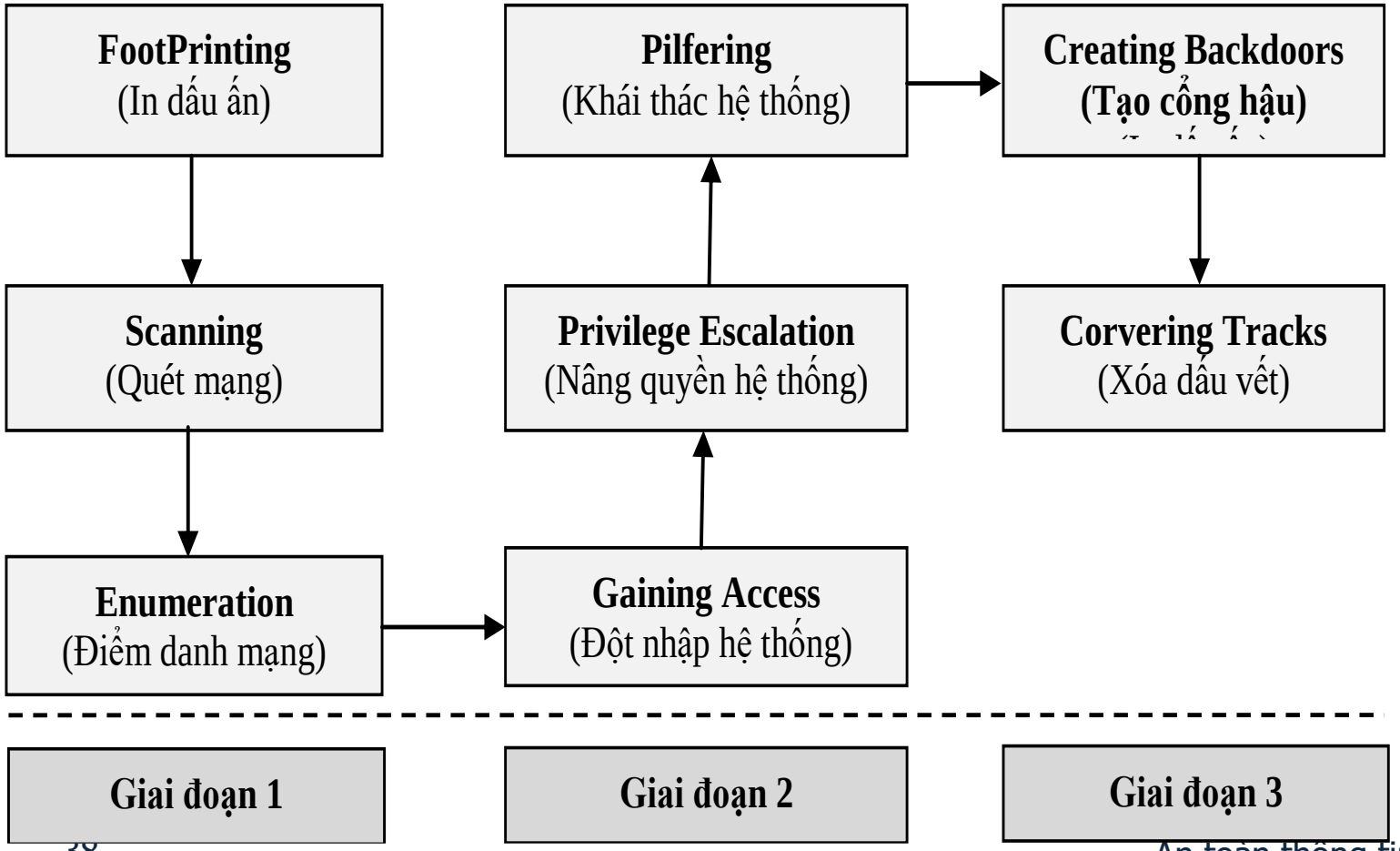
Tấn công chủ động (active attacks)

- 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.

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**

Các bước tấn công mạng



Một số kỹ thuật tấn công mạng

1) Tấn công thăm dò.
2) Tấn công sử dụng mã độc.
3) Tấn công xâm nhập.
4) Tấn công từ chối dịch vụ.
5) Tấn công sử dụng kỹ nghệ xã hội

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.

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.

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).

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.

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.

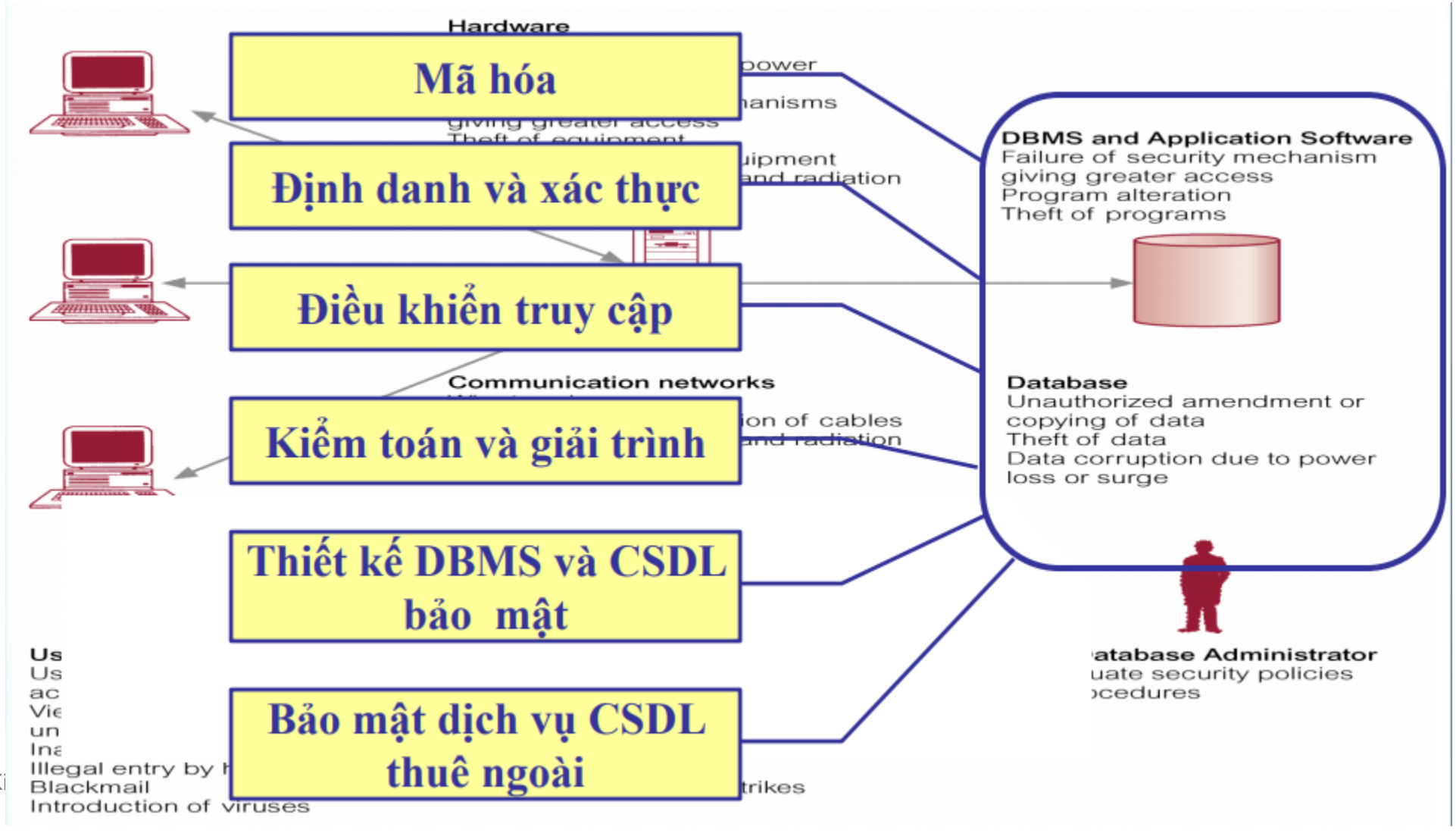
Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

- 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.

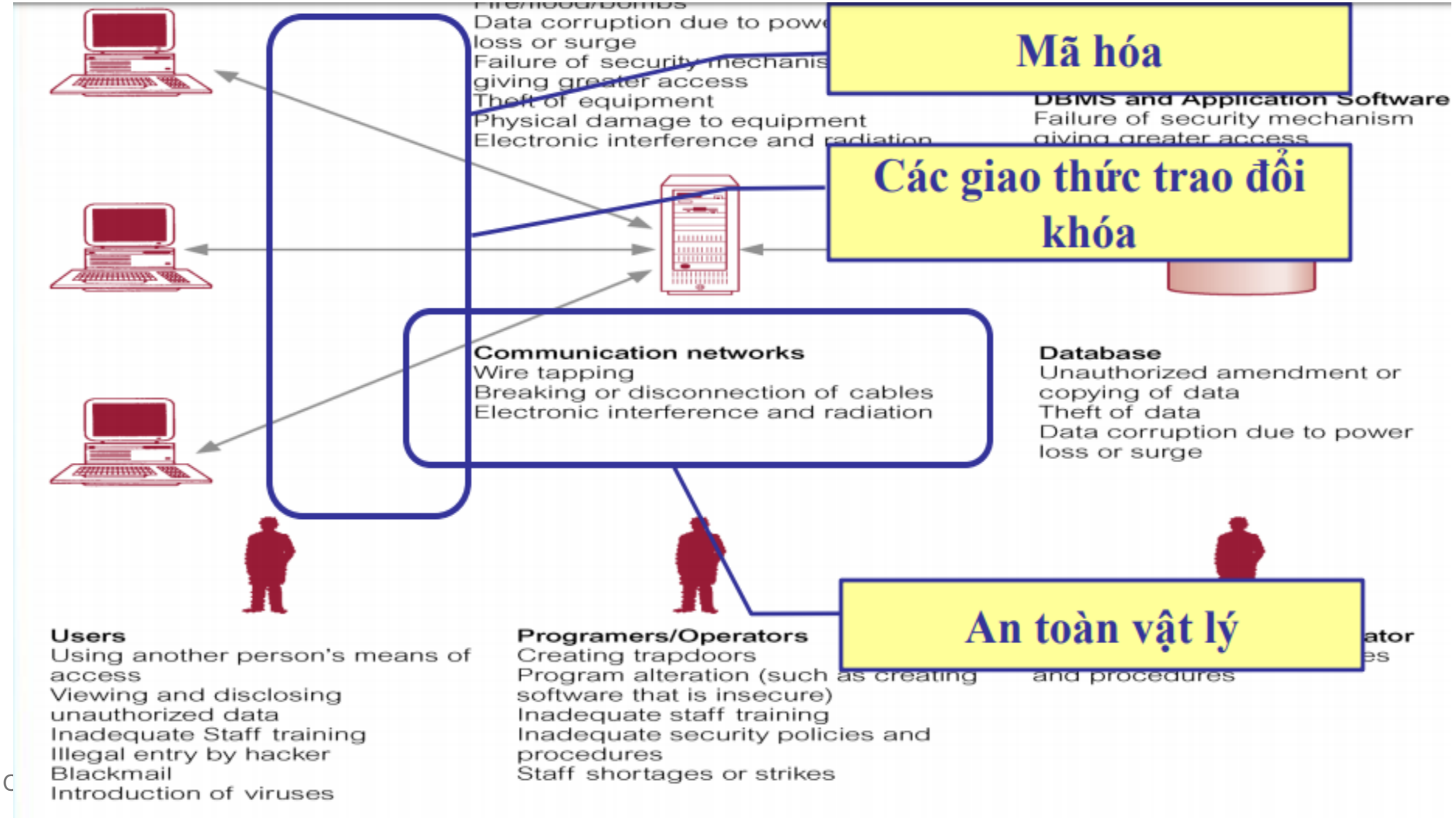
Các thành phần cần bảo vệ trong một HTTT

- Phần cứng
- Mạng
- Cơ sở dữ liệu (CSDL)
- Hệ quản trị CSDL (database management system - DMBS), các ứng dụng
- Người dùng
- Người lập trình hệ thống
- Người quản trị CSDL

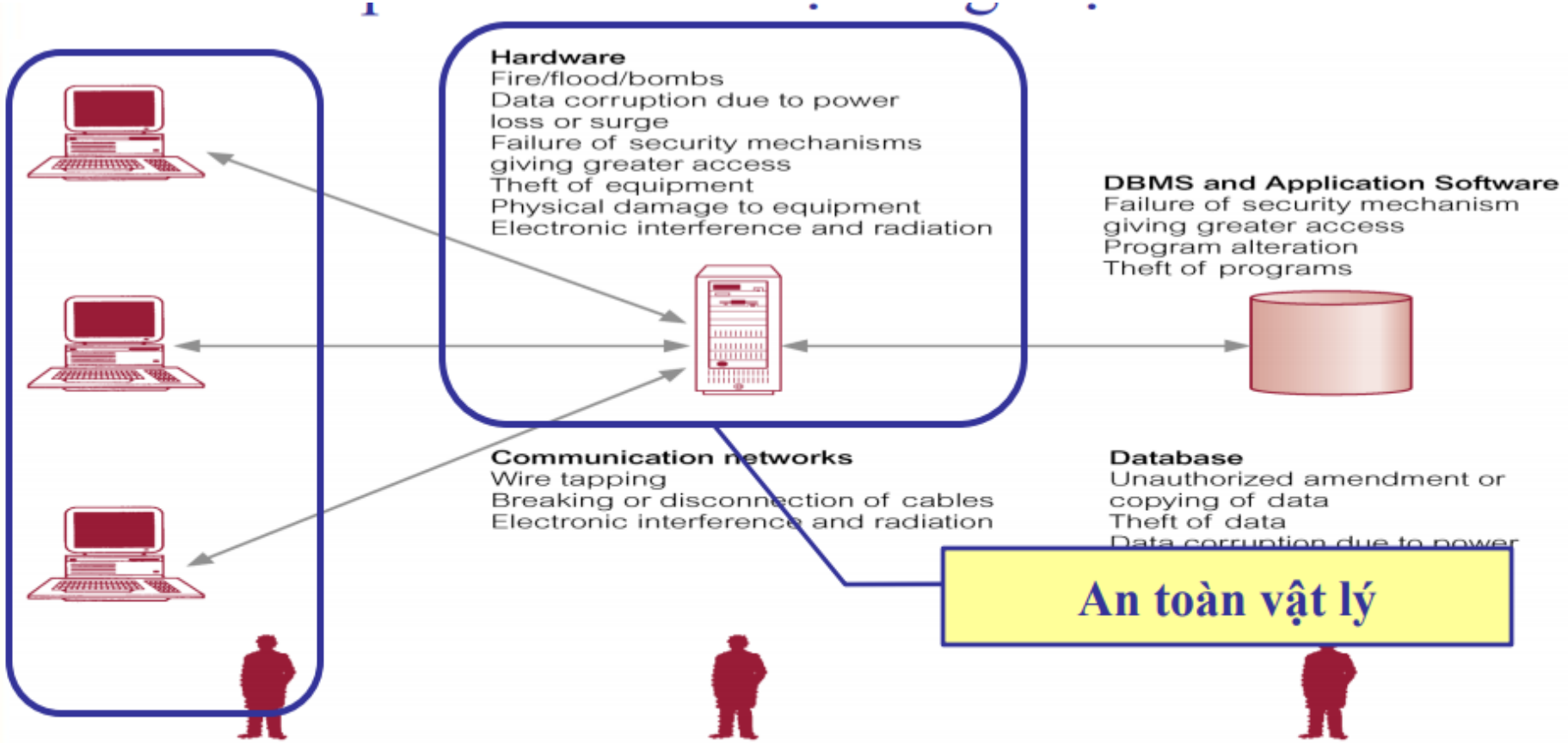
Các thành phần cần bảo vệ trong một HTTT



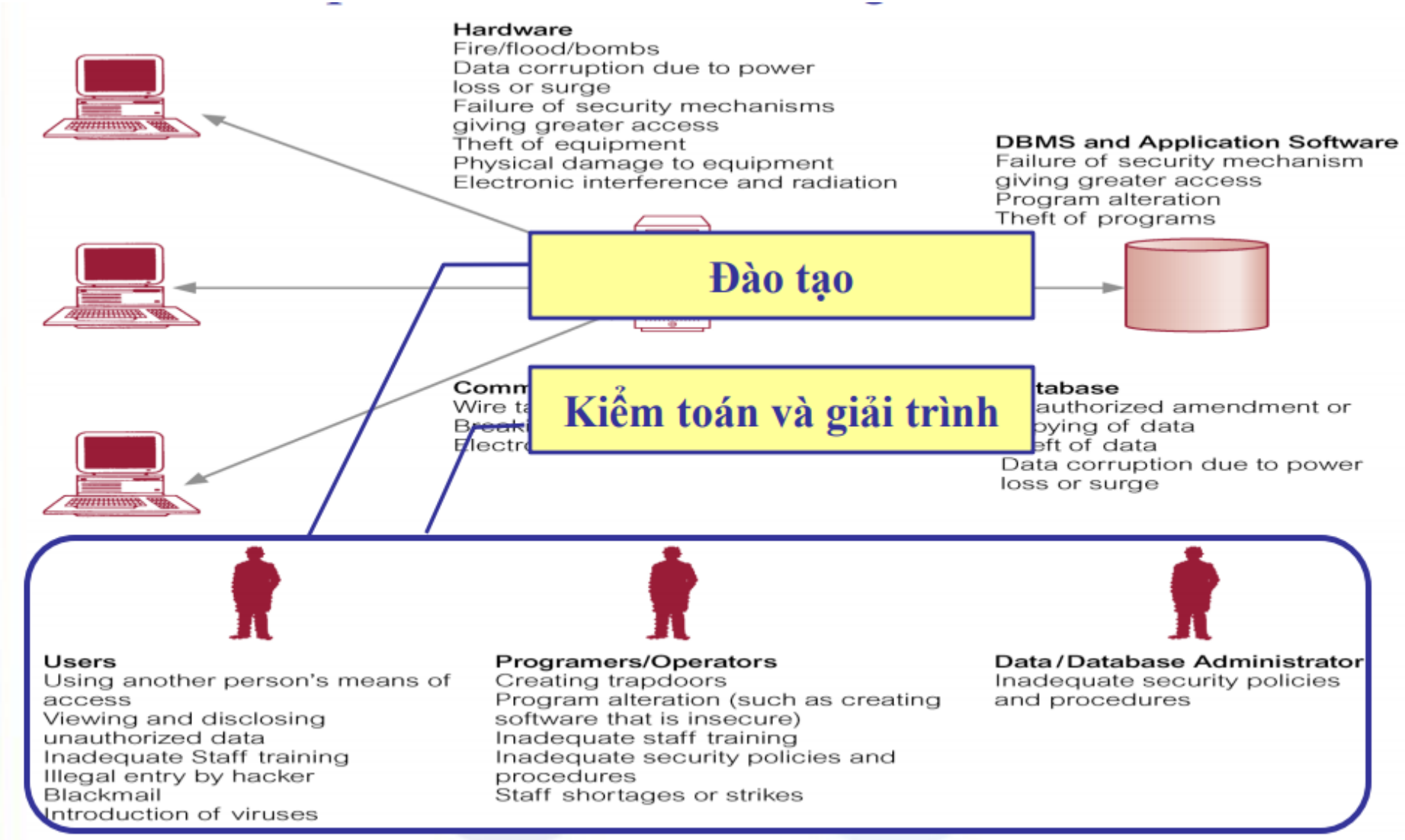
Các thành phần cần bảo vệ trong một HTTT

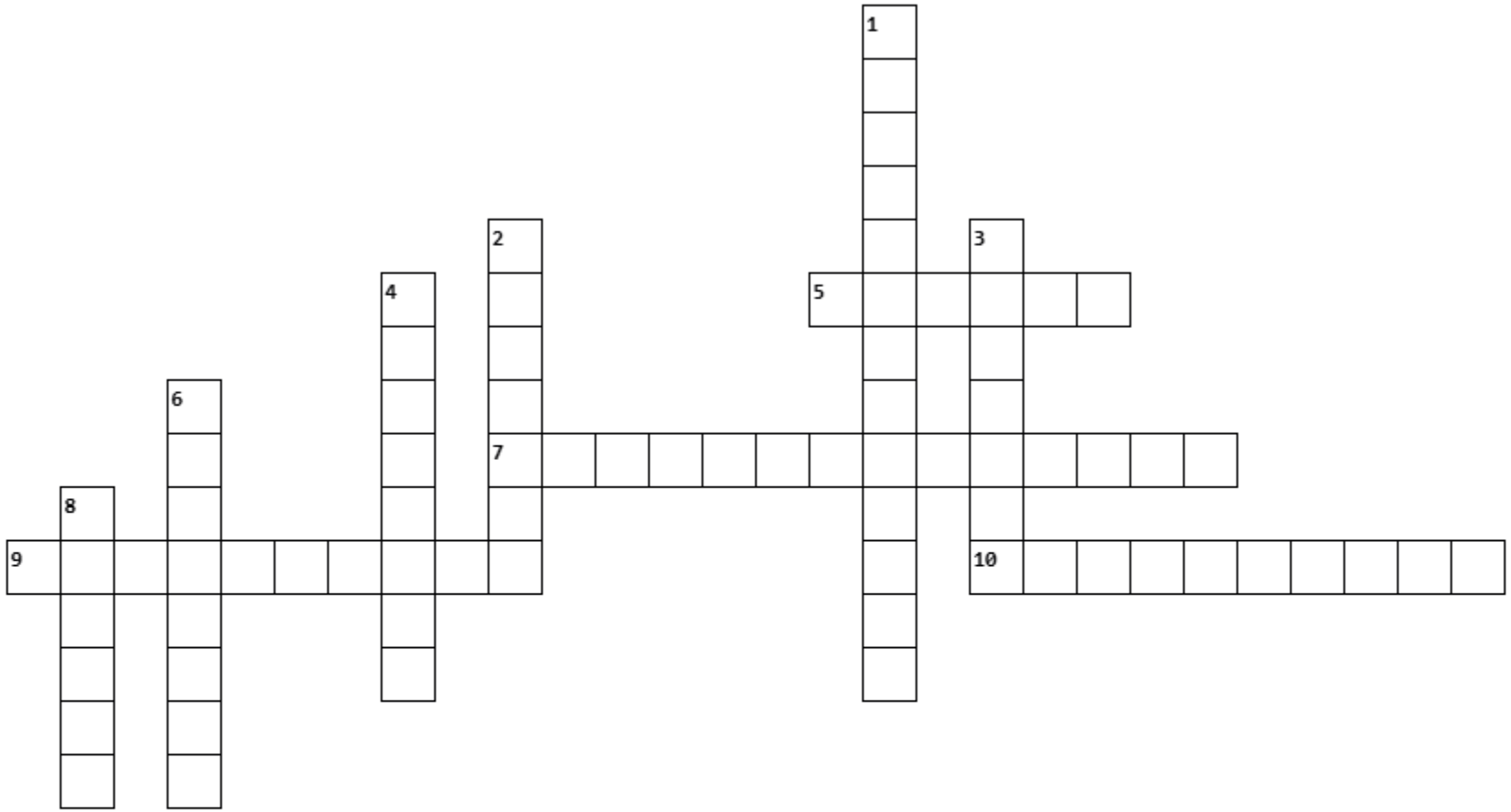


Các thành phần cần bảo vệ trong một HTTT



Các thành phần cần bảo vệ trong một HTTT





Across

5. Unauthorized access to data or systems

7. Verifying the identity of a user or device

9. Type of malware that demands payment to restore access

10. Process of converting data into a secure format

Down

1. Weakness in a system that can be exploited

2. Software that secretly monitors user activity

3. Software designed to harm or exploit systems

4. Protects a network from unauthorized access

6. Fraudulent attempt to obtain sensitive information

8. Copy of data made for recovery purposes

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.

Xu hướng tấn công HTTT (tiếp)

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.

Xu hướng tấn công HTTT (tiếp)

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.

Xu hướng tấn công HTTT (tiếp)

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.

Xu hướng tấn công HTTT (tiếp)

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.

Mã độc và các phòng chống mã độc

Mã độc là gì?

- 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.

Mã độc và các 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...
- 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.

Mã độc và các phòng chống mã độc

Một số loại mã độc

- Trojan: đặc tính phá hoại máy tính, thực hiện các hành vi phá hoại như: xoá file, làm đổ vỡ các chương trình thông thường, ngăn chặn người dùng kết nối internet...
- **Worm**: Giống trojan về hành vi phá hoại, tuy nhiên nó có thể tự nhân bản để thực hiện lây nhiễm qua nhiều 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.
- **Adware**: phần mềm quảng cáo, hỗ trợ quảng cáo, là các phần mềm tự động tải, pop up, hiển thị hình ảnh và các thông tin quảng cáo để ép người dùng đọc, xem các thông tin quảng cáo. Các phần mềm này không có tính phá hoại nhưng nó làm ảnh hưởng tới hiệu năng của thiết bị và gây khó chịu cho người dùng.

Mã độc và các phòng chống mã độc

Một số loại mã độc

- **Ransomware**: 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.
- **Virus:** là phần mềm có khả năng lây nhiễm trong cùng một hệ thống máy tính hoặc từ máy tính này sang máy tính khác dưới nhiều hình thức khác nhau. Quá trình lây lan được thực hiện qua hành vi lây file. Ngoài ra, virus cũng có thể thực hiện các hành vi phá hoại, lấy cắp thông tin...
- **Rootkit**: là một kỹ thuật cho phép phần mềm có khả năng che giấu danh tính của bản thân nó trong hệ thống, các phần mềm antivirus từ đó nó có thể hỗ trợ các module khác tấn công, khai thác hệ thống.

Mã độc và các 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

Mã độc và các phòng chống mã độc

Một số biện pháp phòng chống

- **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.

Mã độc và các phòng chống mã độc

Một số biện pháp phòng chống

- **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.

CÂU HỎI VÀ BÀI TẬP (tiếp)

- 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 hàng, 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.

CÂU HỎI VÀ BÀI TẬP (tiếp)

- 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

Bài 3: Chính sách bảo mật thông tin

Thuật ngữ	Giải thích

Chính sách bảo mật thông tin

- (Non-Disclosure Agreement) của một doanh nghiệp
- **Mục đích của NDA**

1. **Bảo vệ thông tin nhạy cảm**: NDA giúp bảo vệ thông tin bí mật và nhạy cảm của doanh nghiệp, như bí quyết kinh doanh, dữ liệu khách hàng, và công nghệ.
2. **Xây dựng lòng tin**: Thỏa thuận này tạo điều kiện thuận lợi cho sự hợp tác giữa các bên bằng cách thiết lập một môi trường an toàn để chia sẻ thông tin.
3. **Ngăn chặn rò rỉ thông tin**: NDA giúp giảm thiểu nguy cơ thông tin bị rò rỉ ra ngoài doanh nghiệp hoặc bị sử dụng sai mục đích.

Chính sách bảo mật thông tin

- (Non-Disclosure Agreement) của một doanh nghiệp
- **Mục đích của NDA**

1. **Bảo vệ thông tin nhạy cảm**: NDA giúp bảo vệ thông tin bí mật và nhạy cảm của doanh nghiệp, như bí quyết kinh doanh, dữ liệu khách hàng, và công nghệ.
2. **Xây dựng lòng tin**: Thỏa thuận này tạo điều kiện thuận lợi cho sự hợp tác giữa các bên bằng cách thiết lập một môi trường an toàn để chia sẻ thông tin.
3. **Ngăn chặn rò rỉ thông tin**: NDA giúp giảm thiểu nguy cơ thông tin bị rò rỉ ra ngoài doanh nghiệp hoặc bị sử dụng sai mục đích.

Chính sách bảo mật thông tin

- **Cách dùng**
- **Ký kết trước khi chia sẻ thông tin**: Các bên cần ký kết NDA trước khi bắt đầu bất kỳ cuộc thảo luận nào liên quan đến thông tin nhạy cảm.
- **Áp dụng cho nhiều tình huống**: NDA có thể được sử dụng trong nhiều bối cảnh, bao gồm hợp tác kinh doanh, tuyển dụng nhân viên, hoặc khi làm việc với nhà cung cấp.
- **Nội dung cần có trong tài liệu NDA**

1. **Định nghĩa thông tin bí mật**: Rõ ràng mô tả các loại thông tin được coi là bí mật.
2. **Nghĩa vụ bảo mật**: Cam kết của các bên trong việc giữ bí mật và không tiết lộ thông tin cho bên thứ ba.
3. **Thời gian hiệu lực**: Thời gian mà NDA có hiệu lực, cũng như thời gian bảo mật thông tin sau khi thỏa thuận kết thúc.
4. **Các ngoại lệ**: Các trường hợp mà thông tin có thể được tiết lộ mà không vi phạm NDA, như thông tin công khai hoặc thông tin đã biết trước.
5. **Hình thức giải quyết tranh chấp**: Các phương thức giải quyết tranh chấp nếu có vi phạm thỏa thuận.

Chính sách bảo mật thông tin

- **Ví dụ NDA của VPBank**

CỘNG HOA XA HỘI CHU NGHIA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
--------oOo--------

THOA THUẬN BẢO MẬT THÔNG TIN

THOA THUẬN BẢO MẬT THONG TIN NAY ("Thỏa Thuận") được lập vào ngày ..... tháng ... năm ....

BỞI VA GIỮA:

(1) **NGAN HANG THƯƠNG MẠI CỔ PHẦN VIỆT NAM THỊNH VƯỢNG (VPBANK)**, một ngân hàng thương mại cổ phần được thành lập và tồn tại hợp pháp theo pháp luật nước Cộng hoa Xã hội Chủ nghĩa Việt Nam, có trụ sở chính đăng ký tại số 89 Láng Hạ, Đống Đa, Hà Nội.
Người đại diện: **Nguyễn Thị Thu Thủy**.
Chức vụ: Giám đốc TT Dịch vụ Nội Bộ- Khối Vận Hành.
Theo Văn bản ủy quyền số 56/2019/UQ-GĐKVH ngày 26/02/2019 của GĐ Khối Vận hành

Và

(2) **CONG TY** ....., một công ty được thành lập và tồn tại hợp pháp theo pháp luật ....., giấy Chứng nhận đăng ký doanh nghiệp số.....do.....cấp ngày.....tháng.....năm..... có địa chỉ trụ sở chính tại .....
Người đại diện: ..... Chức vụ: .....

XET RĂNG

Các Bên đồng ý ký kết Thỏa Thuận này cho mục đích bảo mật đối với các thông tin mà Bên Cung Cấp Thông Tin tiết lộ cho Bên Nhận Thông Tin phục vụ cho các mục đích bao gồm nhưng không giới hạn: tham gia đấu thầu/nhận thầu/báo giá/chào giá/ký kết hợp đồng và thực hiện các giao dịch khác trong quá trình Bên Nhận Thông Tin cung cấp hàng hóa và dịch vụ cho Bên Cung Cấp Thông Tin (sau đây gọi tắt là *"Mục Đích Kinh Doanh"*). Theo đó, các Bên sẽ cung cấp và tiếp nhận, bảo mật thông tin cho Mục Đích Kinh Doanh trên cơ sở các điều khoản và điều kiện dưới đây:

ĐIỀU 1. Định nghĩa

1.1. **"Thông Tin Mật"**: có nghĩa là tất cả thông tin do Bên Cung Cấp Thông Tin trực tiếp hoặc gián tiếp cung cấp cho Bên Nhận Thông Tin dưới bất kỳ hình thức nào mà gắn với bất kỳ kiến thức, chương trình máy tính, công nghệ, bí mật và kế hoạch kinh doanh, thông tin khách hàng, phân tích, đánh giá, dữ liệu, bài học, tài liệu khác được chuẩn bị bằng văn bản, lời nói hay dữ liệu điện tử, ngoại trừ các thông tin sau:

- Thông tin đã trở nên công khai (công khai trên website của Bên Cung Cấp Thông Tin hoặc Bên Cung Cấp Thông Tin sẵn sàng công bố trên phạm vi rộng mà không có bất kỳ hạn chế hoặc ảnh hưởng nào đến hoạt động kinh doanh của Bên Cung Cấp Thông Tin) trước thời điểm được tiết lộ, cung cấp cho Bên Nhận Thông Tin;
- Thông tin được Bên Nhận Thông Tin xây dựng, phát triển và có được một cách hợp pháp với điều kiện là Bên Nhận Thông Tin chứng minh được rằng việc xây dựng và phát triển này được thực hiện bởi hay nhân danh Bên Nhận Thông Tin mà không sử dụng hay tham khảo bất cứ Thông Tin Mật nào được tiết lộ, cung cấp;
- Thông tin được tiết lộ cho Bên Nhận Thông Tin bởi một Bên thứ ba có quyền hợp pháp tiết lộ thông tin.

1.2. **"Đại Diện"**: bao gồm nhưng không giới hạn các lãnh đạo, cộng sự, cán bộ, nhân viên, cộng tác viên của Bên Nhận Thông Tin có quyền hạn được biết hay tiếp cận các Thông Tin Mật.

1.3. **"Bên Cung Cấp Thông Tin"**: là bên sở hữu và/hoặc cung cấp các Thông Tin Mật. Trong Thỏa Thuận này, Bên Cung Cấp Thông Tin được hiểu là VPBank.

1.4. **"Bên Nhận Thông Tin"**: là bên tiếp nhận Thông Tin Mật. Trong phạm vi Thoả thuận này Bên Nhận Thông Tin được hiểu là chính bên đó hoặc bất kỳ người Đại Diện nào của bên đó.

1.5. **"Các Bên"**/ **"Bên"**: Tùy từng trường hợp được hiểu là "Bên Cung Cấp Thông Tin" và/hoặc "Bên Nhận Thông Tin".

ĐIỀU 2. Cam kết bảo mật thông tin

2.1. Trên cơ sở các Thông Tin Mật được cung cấp, Bên Nhận Thông Tin cam kết tuyệt đối sẽ không cung cấp Thông Tin Mật cho bất cứ Bên thứ ba nào trừ khi có sự chấp thuận trước bằng văn bản của Bên Cung Cấp Thông Tin.

2.2. Bên Nhận Thông Tin phải đảm bảo Thông Tin Mật chỉ được tiết lộ cho Đại Diện của Bên Nhận Thông Tin. Bên Nhận Thông Tin cũng sẽ thông báo với Đại Diện của mình về các điều khoản của Thoả thuận này và tiến hành các thủ tục cần thiết để đảm bảo rằng những người này đồng ý tuân thủ và chịu sự ràng buộc của Thoả thuận này.

2.3. Tùy theo yêu cầu của Bên Cung Cấp Thông Tin, Bên Nhận Thông Tin phải trả lại hay hủy bỏ ngay lập tức tất cả các văn bản và/hoặc tài liệu thuộc Thông Tin Mật, bao gồm cả bản gốc hay bản sao bằng văn bản hay trong hệ thống máy tính hay dưới bất kỳ hình thức điện tử nào khác và cam kết không có bất kỳ bản gốc hay bản sao nào của các Thông Tin Mật đó được lưu lại.

2.4. Bên Nhận Thông Tin cam kết thiết lập, thực hiện và duy trì các điều kiện, thủ tục cần thiết nhằm đảm bảo rằng các Thông Tin Mật không bị tiết lộ, sử dụng hoặc sao chép cho bất cứ mục đích nào khác ngoài Mục Đích Kinh Doanh. Nếu Bên Nhận Thông Tin nhận thấy có bất cứ hay tiềm tàng bất cứ vi phạm nào đối với bản Thoả thuận này, Bên Nhận Thông Tin sẽ thông báo ngay lập tức cho Bên Cung Cấp Thông Tin và sẽ nỗ lực hợp tác tốt nhất với Bên Cung Cấp Thông Tin nhằm tìm kiếm các giải pháp thích hợp để khắc phục, xử lý vi phạm.

2.5. Trong trường hợp Bên Nhận Thông Tin buộc phải tiết lộ các Thông Tin Mật theo yêu cầu bằng văn bản của cơ quan nhà nước có thẩm quyền: (i) Bên Nhận Thông tin sẽ gửi ngay cho Bên Cung Cấp Thông Tin một văn bản thông báo để Bên Cung Cấp Thông Tin có thể thực hiện các hành động thích hợp hoặc các biện pháp bảo vệ phù hợp khác và (ii) Bên Nhận Thông Tin có trách nhiệm thực hiện theo đúng các yêu cầu và biện pháp khắc phục do Bên Cung Cấp Thông Tin đưa ra. Trong trường hợp không có được các biện pháp bảo vệ này, Bên Nhận Thông Tin cam kết sẽ chỉ cung cấp phần thông tin đúng theo yêu cầu của cơ quan nhà nước có thẩm quyền và theo cách thức phù hợp để vẫn có thể bảo vệ được tính chất mật của Thông Tin Mật.

2.6. Tất cả các tài liệu dưới bất kỳ hình thức nào có chứa Thông Tin Mật được Bên Cung Cấp Thông Tin cung cấp là và sẽ được duy trì là tài sản của Bên Cung Cấp Thông Tin. Tất cả quyền sở hữu trí tuệ của các Thông Tin Mật thuộc về Bên Cung Cấp Thông Tin, trừ khi có quy định khác giữa Các Bên bằng văn bản.

2.7. Bên Nhận Thông Tin cam kết sẽ bảo đảm và giữ cho Bên Cung Cấp Thông Tin không bị ảnh hưởng bởi và sẽ bồi thường thiệt hại cho Bên Cung Cấp Thông Tin liên quan đến các khiếu kiện, khiếu nại, tranh chấp, bất đồng phát sinh từ việc đại diện ký kết Thỏa Thuận không đúng thẩm quyền hay phát sinh từ việc vi phạm các cam kết bảo mật của mình theo Thỏa Thuận này và các văn bản liên quan được ký kết giữa Các Bên.

2.8. Bên Cung Cấp Thông Tin sẽ không chịu trách nhiệm cho bất kỳ thiệt hại trực tiếp hay gián tiếp nào phát sinh từ việc Bên Nhận Thông Tin sử dụng bất cứ phần nào của Thông Tin Mật cho Mục Đích Kinh Doanh, trừ trường hợp các Bên có thỏa thuận khác

ĐIỀU 3. Chấm dứt Thỏa Thuận

3.1. Thoả Thuận có hiệu lực kể từ ngày ký kết Thoả thuận này và chấm dứt khi các Bên ký kết văn bản thỏa thuận chấm dứt. Các sửa đổi, bổ sung điều kiện và điều khoản trong Thỏa Thuận này sẽ chỉ có hiệu lực khi được Các Bên thỏa thuận và đồng ý bằng văn bản.

3.2. Khi hai Bên tiến hành chấm dứt thỏa thuận này,Bên Nhận Thông Tin vẫn có trách nhiệm bảo mật thông tin theo quy định tại Thoả Thuận này trừ khi có văn bản đồng ý miễn trách nhiệm của Bên Cung Cấp Thông Tin.

3.3 Trong suốt thời hạn của Thoả Thuận này cũng như trong thời gian sau khi chấm dứt Thỏa Thuận, Bên Nhận Thông Tin sẽ không được trực tiếp hay gián tiếp sử dụng, áp dụng, thương mại hóa hoặc khai thác các Thông Tin Mật hoặc sử dụng Thông Tin Mật để tham gia bất kỳ chương trình nghiên cứu, phối hợp, liên doanh, dự án, hợp tác nào nhằm mục đích thu lợi nhuận thương mại hoặc bất kỳ mục đích nào khác với bất kỳ Bên thứ ba nào trong bất kỳ lĩnh vực nào có hay không có liên quan đến nghiên cứu Thông Tin Mật trừ khi có sự chấp thuận trước bằng văn bản của Bên Cung Cấp Thông Tin.

ĐIỀU 4. Luật áp dụng và Thẩm quyền giải quyết tranh chấp

Thoả Thuận này chịu sự điều chỉnh và được giải thích theo pháp luật nước CHXHCN Việt Nam. Bất cứ tranh chấp nào phát sinh hay liên quan đến Thoả Thuận này sẽ được các Bên giải quyết trước hết bằng thương lượng trên tinh thần hợp tác và tôn trọng lẫn nhau. Trường hợp không giải quyết được hoặc không muốn giải quyết bằng thương lượng, Các Bên có quyền khởi kiện ra Tòa án nhân dân có thẩm quyền để giải quyết theo quy định của pháp luật.

Thoả Thuận này được lập thành hai (2) bản gốc có hiệu lực pháp lý như nhau. Mỗi Bên giữ một (1) bản gốc để thực hiện. Không Bên nào được chuyển giao các quyền và trách nhiệm của mình cho bất cứ Bên thứ ba nào khác mà không có sự đồng ý bằng văn bản của Bên kia.

ĐẠI DIỆN VPBANK	**ĐẠI DIỆN CONG TY ...**
(Ký, ghi rõ họ tên, đóng dấu)	*(Ký, ghi rõ họ tên, đóng dấu)*

Chính sách bảo mật thông tin

- **1. Chính sách bảo mật thông tin**
- **Mục tiêu**: Xác định mục tiêu bảo vệ thông tin nhạy cảm và quy định cách thức xử lý, lưu trữ, và chia sẻ thông tin.
- **Định nghĩa thông tin nhạy cảm**: Rõ ràng xác định các loại thông tin được coi là nhạy cảm, như mã nguồn, dữ liệu khách hàng, và thông tin tài chính.
- **2. Chính sách truy cập và kiểm soát**
- **Quyền truy cập**: Định rõ ai được phép truy cập thông tin nào và trong những hoàn cảnh nào.
- **Xác thực người dùng**: Sử dụng phương pháp xác thực hai yếu tố (2FA) và mật khẩu mạnh để bảo vệ tài khoản.
- **3. Chính sách về mã hóa**
- **Mã hóa dữ liệu**: Quy định việc mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải.
- **Sử dụng giao thức bảo mật**: Áp dụng các giao thức bảo mật như HTTPS và SSL cho các ứng dụng web.
- **4. Chính sách sao lưu và khôi phục**
- **Sao lưu định kỳ**: Thiết lập quy trình sao lưu dữ liệu định kỳ để đảm bảo khôi phục dữ liệu trong trường hợp mất mát.
- **Kế hoạch khôi phục thảm họa**: Xây dựng kế hoạch khôi phục thông tin và hệ thống sau sự cố.
- **5. Chính sách đào tạo nhân viên**
- **Đào tạo bảo mật**: Tổ chức các khóa đào tạo về nhận thức bảo mật cho nhân viên để nâng cao ý thức về bảo mật thông tin.
- **Chính sách báo cáo sự cố**: Khuyến khích nhân viên báo cáo các sự cố bảo mật ngay lập tức.
- **6. Chính sách kiểm tra và đánh giá**
- **Kiểm tra bảo mật định kỳ**: Thực hiện kiểm tra bảo mật thường xuyên để phát hiện lỗ hổng và cải thiện hệ thống bảo mật.
- **Đánh giá rủi ro**: Thực hiện đánh giá rủi ro định kỳ để xác định các mối đe dọa tiềm tàng và biện pháp khắc phục.
- **7. Chính sách chia sẻ và xử lý thông tin**
- **Chia sẻ thông tin**: Định rõ quy trình và quy định về việc chia sẻ thông tin với bên thứ ba.
- **Xử lý dữ liệu**: Quy định cách thức thu thập, xử lý và xóa bỏ thông tin cá nhân.