Họ tên: Nguyễn Huỳnh Minh Tiến

MSSV: 18110377

**BÀI KIỂM TRA GIỮA KỲ LẦN 1**

**MÔN: AN TOÀN THÔNG TIN**

**Câu 1. Trình bày những nguyên tắc, giải pháp để đảm bảo an toàn thông tin trong một hệ thống CNTT.**

Để đảm bảo an toàn thông tin trong một hệ thống CNTT, cần phải đảm bảo nguyên tắc C-I-A sau:

* C-I-A
  + Confidentiality (tính bảo mật): tránh lộ thông tin đến những đối tượng không được xác thực hoặc để lọt vào các hệ thống khác, tức là thông tin chỉ được phép truy cập bởi những đối tượng (người, chương trình máy tính…) được cấp phép.
    - Giải pháp: dùng Xác thực, yêu cầu đối tượng cung cấp credential (cặp username + password hay đặc điểm về sinh trắc để xác thực.
    - VD: Khi thanh toán đơn hàng online trên các sàn thương mại điện tử (Tiki, Lazada,…) qua tài khoản Ví điện tử Momo hoặc qua Internet Banking, số thẻ tín dụng (hoặc thông tin tài khoản) được gửi từ người mua hàng đến người bán, và từ người bán đến nhà cung cấp dịch vụ thẻ tín dụng. Để bảo mật, hệ thống sẽ mã hóa số thẻ trong suốt quá trình truyền tin… Nếu một bên không được xác thực (ví dụ như hacker…) lấy số thẻ này bằng bất kì cách nào, thì tính bí mật không còn nữa.
  + Integrity (tính toàn vẹn): thông tin chỉ được chỉnh sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi, đồng thời phải xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy.
    - => Dùng Checksum
    - VD: để làm mất tình toàn vện, người ta có thể: Chặn đứng và thay đổi gói tin được gửi qua mạng, chỉnh sửa trái phép các file được lưu trữ trên máy tính…
  + Availability (tính sẵn sàng) => Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.
    - Giải pháp: Load Balancing, Clustering, Redudancy, Failover…
    - VD: để phá vỡ tính sẵn sàng, hacker có thể tiến hành tấn công từ chối dịch vụ (Máy của hacker sẽ gửi hàng loạt các gói tin có các MAC nguồn giả tạo đến switch làm bộ nhớ lưu trữ MAC address table của switch nhanh chóng bị đầy khiến switch không thể hoạt động bình thường được nữa).

Ngoài ra, cần phải lưu ý đảm bảo các vấn đề về phần cứng cũng như về nguồn điện.

Các giải pháp:

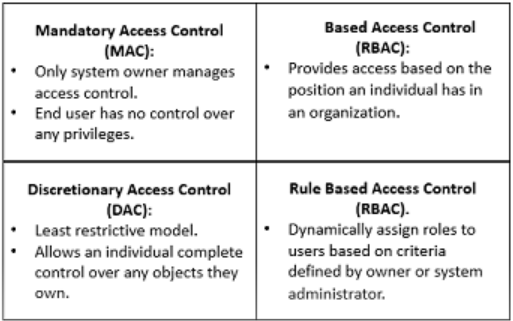
* Governance (Quản trị)
  + Policy: Đặc ra các quy định để bắt buộc các nhân viên tuân theo.
  + Audit: theo dõi những thay đổi trong hệ thống
  + Awareness: mở các khóa training cho nhân viên trong công ty về các vần đề bảo mật trong hệ thống CNTT công ty
* A-A-A:
  + Authentication (xác thực/chứng thực): Xác định “Bạn là ai?”
  + Authorization: “Bạn có quyền gì?”
  + Accounting/Auditing: Lưu lại lịch sử log
* Non-repudiation (chống chối bỏ/chống chối thác): => Dùng chữ ký số

**Câu 2. Trình bày các giải pháp bảo mật phần mềm (Software Security)**

* Phân tích hệ thống, bao gồm các vấn đề về bảo mật, trước khi tiến hành code.
* Kiểm tra dữ liệu đầu vào, đặc biệt là các dữ liệu người dùng nhập vào để tránh việc chèn mã độc nhằm tấn công hệ thống (SQL Injection…).
* Connectivity (kết nối): chỉ mở những port cần thiết sử dụng, để tránh trường hợp hacker lợi dụng tấn công. Giảm thiếu tối đa các thiết bị kết nối, để tránh việc kẻ tấn công có thể có nhiều cơ hội và thiết bị để có thể tấn công vào đó.
* Hệ điều hành: thường xuyên cập nhật các bản vá của Hệ điều hành, nhằm đảm bảo hệ thống luôn trong tình trạng cập nhật mới nhất.
* Familiarity (Quen thuộc): Không đặt các tên người dùng, mật khẩu mặc định, thường dùng, dễ đoán (VD: admin, user, username,…).
* Quy trình phát triển phần mềm: quá trình thiết kế, xây dựng và thử nghiệm phần mềm cần phải xem xét đến các vấn đề bảo mật, thêm phần testing về bảo mật trước khi release sản phẩm.
* Rà soát, quét các lỗ hổng bảo mật trước khi release phần mềm.
* Coding: luôn cập nhật các kỹ thuật code mới nhất, các phương pháp phòng tránh hacking.
* People: hướng dẫn người dùng cách sử dụng phần mềm, nhắc nhở đổi tài khoản đăng nhập, các lỗi thường gặp có thể dẫn đến bị đánh mất thông tin,…

**Câu 3. Trình bày về vấn đề** **Authentication và** **Access Control trong ATTT**

* Authentication
  + Xác thực thông tin chứng thực của người dùng (trả lời cho câu hỏi “Who are you?”)
  + Factors (các nhân tố chứng thực):
    - Account: user + password. Mỗi tài khoản cần phải có strong password, mật khẩu phải đặt theo quy tắc định trước (độ dài mật khẩu, chứa các kí tự đặc biệt,..). Ngoài ra, cần phải có quy định về số lần nhập sai mật khẩu, thời hạn hiệu lực của mật khẩu,…
    - Phân loại: Single-factor Authentication, Two-factor Authentication, Muilti-factor Authentication.
  + Để phá vỡ tính chứng thực, người ta có thể dùng các cách tấn công như:
    - Brute force, truy cập vào CSDL chứa thông tin đăng nhập,…
    - Key logger: theo dõi các ký tự bàn phím mà người dùng nhập vào
    - Sniffer: bắt gói tin chứa thông tin đăng nhập
    - Social Engeneering: tạo trang web giả mạo (giả web ngân hàng, giả giao diện Google, Facebook,…), chèn các đoạn quảng cáo chứa liên kết để tải các chương trình có mã độc vào máy người dùng,..
  + Để xác thực, dùng các phương pháp:
    - Something you know: mật khẩu, mã PIN,…
    - Something you have: số điện thoại, email, mã số trên thẻ ATM, địa chỉ MAC,…
    - Something you are: vân tay, móng mắt, gương mặt, tiếng nói,…
    - Địa chỉ GPS, thời gian truy cập hệ thống, mạng truy cập
* Access Control: Các tính năng bảo mật kiểm soát cách người dùng và hệ thống giao tiếp và tương tác với nhau.
  + Gồm Authentication (who you are?) và Authorization (What rights/permissions do you have?)
  + Các mô hình Access Control: xác định cách gán quyền.
    - Mandatory Access Control (MAC): mô hình chỉ cung cấp cho chủ sở hữu và quản lý giám sát các điều khiển truy cập
    - Role Based Access Control (RBAC): Cung cấp kiểm soát truy nhập vị trí của một cá nhân trong một tổ chức.
    - Discretionary Access Control (DAC): cho phép một cá nhân hoàn toàn kiểm soát bất kỳ đối tượng mà họ sở hữu cùng với các chương trình liên kết với các đối tượng.
    - Rule Based Access Control (RBAC): Kiểm soát truy cập dựa trên quy tắc sẽ tự động gán vai trò cho người dùng dựa trên các tiêu chí được xác định bởi người quản lý hoặc quản trị viên hệ thống.
    - Attribute-based access control: Xác định quyền thể hiện điều kiện về thuộc tính của cả tài nguyên và chủ đề.



* + Thực thi Access Control: có thể dùng các cách sau:
    - Access Control List
    - Group policy
    - Hạn chế tài khoản
      * Giới hạn thời gian trong ngày: giới hạn thời gian trong ngày người dùng có thể đăng nhập vào hệ thống
      * Hạn chế tài khoản hết hạn: quá trình thiết lập tài khoản của người dùng hết hạn
  + Các khái niệm:
    - Access (Permisson): Luồng thông tin giữa subject và object
      * Read
      * Write
      * Execute
    - Subject: Một thực thể đang hoạt động yêu cầu quyền truy cập vào một đối tượng hoặc dữ liệu trong một đối tượng
      * User\_Id
      * Program\_Id
      * Process\_Id
    - Object: Một thực thể thụ động có chứa thông tin
      * File
      * Folder
      * Data …
    - Nguyên lý bảo mật: CIA

**Câu 4. Trình bày về các giải pháp bảo vệ dữ liệu (Data security)**

Các giải pháp có thể dùng để bảo vệ dữ liệu:

* Khám phá và phân loại dữ liệu:
  + Khai phá dữ liệu rồi phân loại chúng thành: dữ liệu tối mật, dữ liệu mật, dữ liệu thông thường, dữ liệu công khai, dữ liệu chưa phân loại,…
  + Dùng để dễ dàng xác định tập các dữ liệu quan trọng cần được bảo vệ trong hệ thống. Nếu dữ liệu được chỉnh sửa, việc phân loại có thể phải tiến hành lại. Mỗi người dùng sẽ được cấp phép truy cập vào từng mức độ bảo mật của dữ liệu, hạn chế được việc truy cập các dữ liệu không được phép.
* Tường lửa:
  + Tường lửa loại trừ lưu lượng truy cập không mong muốn vào mạng. Ngoài ra, ta chỉ có thể mở một số cổng nhất định, điều này làm cho attacker ít chỗ cơ động để truy cập hoặc tải xuống dữ liệu. Tùy thuộc vào chính sách tường lửa của tổ chức, tường lửa có thể hoàn toàn không cho phép một số lưu lượng truy cập hoặc tất cả lưu lượng truy cập hoặc nó có thể thực hiện xác minh trên một số hoặc tất cả lưu lượng truy cập.
* Sao lưu và phục hồi:
  + Giúp khôi phục lại dữ liệu trong trường hợp dữ liệu bị xóa hoặc bị phá hủy. Tất cả dữ liệu quan trọng nên được sao lưu định kỳ để khi có lỗi xảy ra ở máy chủ, dữ liệu vô ý bị người dùng xóa, hoặc bị tấn công từ các phần mềm độc hại… thì có thể khôi phục dữ liệu nhanh chóng, không mất mác dữ liệu.
* Antivirus:
  + Để chống các phần mềm chứa mã độc, các phần mềm key logger… thu thập, chỉnh sửa, phá hủy dữ liệu quan trọng, kịp thời ngăn chặn các mối nguy hại ngay khi có pahanf mềm được tải về…
* Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)
  + IDS là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn, xác định các hoạt động nguy hại, lưu giữ các thông tin này. Sau đó kết hợp với tường lửa để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên.
  + Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.
* Thông tin bảo mật và quản lý sự kiện (SIEM):
  + Phân tích thời gian thực các bản ghi bảo mật được ghi lại bởi các thiết bị mạng, máy chủ và các ứng dụng phần mềm. SIEM rất quan trọng cho các cuộc điều tra bảo mật dữ liệu.
* Ngăn mất dữ liệu (DLP):
  + Giám sát máy trạm, máy chủ và mạng để đảm bảo rằng dữ liệu nhạy cảm không bị xóa, loại bỏ, di chuyển hoặc sao chép, ngoài ra cũng giám sát những người đang sử dụng và truyền dữ liệu để phát hiện việc sử dụng trái phép.
* Access Control:
  + Các tệp nhạy cảm chỉ nên được truy cập bởi người có thẩm quyền. Quyền của người dùng phải được cấp theo đúng nguyên tắc Quyền tối thiểu, đồng thời dùng ACL để xác định ai có thể truy cập tài nguyên nào và ở cấp độ nào.
* Giải pháp bảo mật đám mây
* Auditing:
  + Theo dõi những thay đổi trong hệ thống. Ví dụ: bất kỳ tài khoản nào vượt quá số lần đăng nhập không thành công tối đa sẽ tự động được báo cáo cho quản trị viên bảo mật thông tin để điều tra.
* Mã hóa Dữ liệu:
  + Những dữ liệu quan trọng (mã thẻ tín dụng, mật khẩu,…) nên được mã hóa để phòng chống các cuộc tấn công của hackers nhằm đánh cắp dữ liệu quan trọng. Ví dụ: nếu không có mã hóa Lớp Cổng Bảo mật (SSL), các giao dịch thẻ tín dụng tại các trang web phổ biến sẽ rất bất tiện hoặc không an toàn.
* Bảo mật vật lý:
  + VD: đặt mật khẩu cho BIOS để ngăn chặn kẻ tấn công khởi động vào hệ điều hành. Đảm bảo nguồn điện luôn ổn định, có nguồn phát điện dự phòng cho các sự cố cúp điện bất ngờ.