Câu 1: Trình bày tới các khái niệm về tính bí mật, tính sẵn sàng và tính an toàn trong ATTT?

Câu 2: Trình bày 1 số kiểu tấn công mạng?

- Tấn công quét mạng
- Tấn công từ chối dịch vụ
- Tấn công mã độc
- Tấn công kỹ nghệ XH

Câu 3: Trình bày và phân tích các giải pháp bảo đảm ATTT?

Câu 4: Trình bày tổng quan về thực trạng ATTT trên tg và tại VN?

Bài làm:

Câu 1:

- Tính bí mật (Confidentiality): Bảo vệ dữ liệu ko bị lộ ra ngoài 1 cách trái phép

VD: Trong hệ thống quản lý sinh viên, 1 ~~hs~~ sinh viên đc phép xem thông tin kết quả học tập của mình nhưng ko đc phép xem kết quả học tập của sinh viên ≠

- Tính sẵn sàng (Availability): Đảm bảo dữ liệu luôn ở sẵn sàng khi những ng dùng hoặc ứng dụng đc ủy quyền ~~truy cập~~ yêu cầu

VD: Trong hệ thống quản lý sinh viên, cần đảm bảo rằng sinh viên có thể truy cập vào thông tin kết quả học tập của mình bất cứ lúc nào

- Tính toàn vẹn (Integrity): Chỉ những ng dùng đc ủy quyền mới đc phép chỉnh sửa dữ liệu

VD: Trong hệ thống quản lý sinh viên, ko để cho phép sinh viên được phép tự thay đổi thông tin kết quả học tập của mình

- Tính an toàn: Là 1 k/n rộng, bao gồm việc bảo vệ thông tin khỏi mọi hình thức truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại hủy trái phép. Nói cách khác, tính an toàn là cấu thành từ tính bảo mật, tính toàn vẹn và tính sẵn sàng

Câu 2:

- Tấn công quét mạng: Là 1 hoạt động tìm tắc dùng các công cụ chuyên biệt để khám phá và xác định các lỗ hổng bảo mật trong 1 hệ thống mạng hoặc máy tính.
- Tấn công từ chối dịch vụ: Là tên gọi chung của biến tấn công làm cho 1 hệ thống nào đó bị quá tải ở thể cung cấp dịch vụ, gây ra gián đoạn hoạt động hoặc làm cho hệ thống ngừng hoạt động
- Tấn công mã độc: Mã độc là ñ chương trình khi đc khởi chạy có khả năng phá hủy hệ thống, bao gồm Virus, sâu (Worm) và Trojan, ...

+ Tấn công 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 kỹ nghệ xH: Là 1 nhóm p² đc sử dụng để đánh lừa ng sử dụng tiết lộ các thông tin bí mật

+ Là p tấn công phi kỹ thuật, dựa trên sự thiếu hiểu biết của ng dùng để lừa gạt họ cung cấp các thông tin nhạy cảm như password hay các thông tin quan trọng

Câu 3

- Các biện pháp công nghệ (Technology): Bao hàm tất cả các biện pháp phần cứng, các phần mềm, phần sụn cũng như các kỹ thuật công nghệ liên quan được sử

dụng nhằm đảm bảo các yêu cầu an toàn của thông tin trong các trạng thái của nó

- Các biện pháp về chính sách và tổ chức (Policy & Practices): Đưa ra các chính sách, quy định, phương thức thực thi

+ Thực tế cho thấy, ATTT ko chỉ đơn thuần là vấn đề ứng dụng công nghệ, kỹ thuật. Hệ thống chính sách và kiến trúc tổ chức đóng 1 vai trò hữu hiệu trong việc đảm bảo an toàn thông tin

- Các biện pháp về đào tạo, tập huấn, nâng cao nhận thức (Education, Training & Awareness):

+ Các biện pháp công nghệ hay các biện pháp về tổ chức thích hợp phải dựa trên các biện pháp đào tạo, tập huấn và tăng cường nhận thức để có thể triển khai đảm bảo an toàn thông tin từ nhiều hướng ≠ nhau

+ Các nhà nghiên cứu và các kỹ sư cũng cần phải hiểu rõ các nguyên lý an toàn thông tin, thì mới mong các sản phẩm và hệ thống do họ làm ra đáp ứng đc các nhu cầu về an toàn thông tin của cuộc sống hiện tại đặt ra

- Biện pháp hợp tác quốc tế:

+ Hợp tác với các quốc gia có kinh nghiệm, kế thừa những thành tựu khoa học của các quốc gia đi trc trong vấn đề đảm bảo ATTT

+ Xây dựng các quy chế phối hợp với các cơ quan tổ chức quốc tế trong ứng phó các sự cố về ATTT

Câu 4:

⊛ Thực trạng ATTT trên t/g:

- Các mối đe dọa chủ yếu:
  + Tấn công mạng: Ransomware, phising, DDoS...
  + Rò rỉ dữ liệu. vi phạm dữ liệu cá nhân, thông tin doanh nghiệp
  + Các cuộc tấn công vào cơ sở hạ tầng quan trọng
- Xu hướng tấn công:
  + Tần suất tấn công ngày càng tăng
  + Các cuộc tấn công trở nên tinh vi và phức tạp hơn
  + Mục tiêu tấn công đa dạng hơn
- Tác động:
  + Thiệt hại kinh tế lớn
  + Mất niềm tin của khách hàng
  + Ảnh hưởng đến an ninh quốc gia

⊛ Thực trạng ATTT tại VN:

- Tình hình chung:
  + VN là 1 trong n quốc gia có tốc độ tăng trưởng về số lượng cuộc tấn công mạng
  + Các loại hình tấn công phổ biến: lừa đảo trực tuyến, đánh cắp thông tin cá nhân, tấn công vào các cơ quan nhà nc và doanh nghiệp
- Nguyên nhân: + Nhận thức về ATTT còn hạn chế
  + Cơ sở hạ tầng CNTT chưa đồng bộ
  + Thiếu nguồn lực và nhân lực chuyên môn
- Tác động: + Ả/h đến quá trình chuyển đổi số
  + Gây thiệt hại kinh tế lớn
  + Mất lòng tin ng dùng