**Phần 1 – Tổng quan về an toàn an ninh thông tin**

**Bài 1: tổng quan về an ninh mạng**

**Khái niệm cơ bản về an toàn an ninh thông tin**

**Tại sao an toàn an ninh thông tin là quan trọng?**

**-** Đảm bảo hệ thống hoạt động đúng đắn để chúng ta nhận được kết quả mong đợi

- Chúng ta hoàn toàn không muốn hệ thống bị đánh cắp dữ liệu hay bị hư hại, những kẻ xấu có thể truy cập được vào những dữ liệu nhạy cảm và kiếm tiền, trục lợi từ các thông tin này.

**Mô hình CIA**

**-** Sau khi đã hiểu về tầm quan trọng của an toàn an ninh thông tin, chúng ta cần phải định nghĩa được một cách bao quát vè các mục tiêu an toàn an ninh thông tin trong hệ thống

- Các mục tiêu này có thể được phát biểu theo những mô hình khác nhau, mà trong đó CIA là mô hình phổ biến và nổi tiếng nhất.

- Mô hình này đề cập đến mục tiêu về tính bí mật (confidetiality), toàn vẹn (integrrity) và sẵn sàng (availability).

**Tấn công an toàn an ninh thông tin**

**Rủi ro an toàn an ninh thông tin**

**-** Độ rủi ro an toàn an ninh thông tin là đại lượng đánh giá khả năng xảy ra sự cố gây mất an toàn an ninh thông tin cho hệ thống và các hậu quả của nó.

- Trong phần lớn các trường hợp, sự cố là do các hành vi cố ý tấn công của đối phương, trong khi phần ít các trường hợp còn lại là do thiên tai, lỗi vô ý của người dùng hay hỏng hóc ngẫu nhiên của hệ thống

- Các yếu tố ảnh hưởng đến độ rủi ro an toàn an ninh thông tin gồm các mối đe dọa, lỗ hổng và tấn công bảo mật

**Lỗ hổng và tấn công bảo mật**

**-** Lỗ hổng là các điểm yếu của hệ thống mà kẻ xấu có thể lợi dụng khai thác để thực hiện các hành vi tấn công gây mất an toàn an ninh cho hệ thống 🡪 Khi lỗ hổng xuất hiện độ rủi ro an toàn thông tin của hệ thống tăng lên

- Lỗ hổng không chỉ xuất hiện trong phần cứng, phần mềm mà ngay ở khâu phân tích, thiết kế hệ thống cũng như quá trình vận hành của người dùng.

**Xây dựng giải pháp an toàn an ninh thông tin**

**Các nguyên tắc an toàn bảo mật**

**Đánh giá rủi ro an toàn an ninh thông tin**

**-** Là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin

- Đánh giá rủi ro là bước tiên quyết để tổ chức có thể xác định được mức độ an toàn của hệ thống công nghệ thông tin, từ đó đưa ra những giải pháp quản lý giám sát rủi ro

- Đánh giá rủi ro bao gồm nhiều công đoạn với những tác vụ phức tạp, từ xác định và đánh giá tầm quan trọng của tài nguyên, nhận diện nguy cơ cho tới tìm kiếm lỗ hổng an toàn bảo mật hệ thống

**Kiểm thử xâm nhập**

**-** Quá trình tìm kiếm lỗ hổng hệ thống được thực hiện theo phương pháp luận là đóng vai trò kẻ tấn công để tìm cách gây hại cho hệ thống, hay còn gọi là kiểm thử xâm nhập

- Đây là công tác được thực hiện ngay từ giai đoạn phát triển hệ thống và được thực hiện thường xuyên trong khi vận hành hệ thống

**--------------- --------------- --------------- --------------- --------------- --------------- --------------- --------------- --------------- --------------- --------------- ---------------**

**Phần 2: an toàn an ninh trong mạng TCP/IP**

**Bài 2: an toàn bảo mật giữa các giao thức của Internet**

**Các vấn đề an toàn bảo mật của TCP/IP**

**Kiến trúc hạ tầng internet**

**Chồng giao thức TCP/IP**

**-** Mỗi hệ thống được xây dựng theo mô hình phân tầng, mà OSI và TCP/IP là 2 mô hình phôe biến.

- Nếu như OSI có vai trò như một mô hình kiểu mẫu để tham chiếu thìTCP/IP chính là mô hình được sử dụng để triển khai mạng internet.

- Với kiến trúc đó, mạng internet hoạt động dưới sự điều khiển của một loạt các giao thức truyền thông được sắp đặt thành cấu trúc chồng giao thức TCP/IP

**Giao thức IP**

**-** Trong chồng giao thức TCP/IP, giao thức IP nằm trên tầng liên mạng và đóng vai trò là giao thức kết nối liên mạng trong internet. Tất cả máy tính và thiết bị mạng internet đều được gán địa chỉ IP và trao đổi dữ liệu đóng gói tin IP.

**Vấn đề xác thực trong giao thức IP:**

- Dữ liệu trao đổi giữa các máy tính trong mạng internet được đóng gói theo giao thức IP với thông số địa chỉ gửi và nhận.

- Là một giao thức có vai trò đặc biệt quan trọng trong mạng internet nhưng giao thức IP không sử dụng bất cứ cơ chế an toàn bảo mật nào, dẫn tới thông tin trong toàn bộ gói tin IP đều không được đảm bảo an toàn.

**Giao thức TCP:**

**-** Giao thức TCP, một trong hai giao thức trên tầng giao vận trong chồng giao thức TCP/IP có chức năng điều khiển truyền giữa liệu giữa các ứng dụng mạng cần sự tin cậy.

- Giao thức TCP/IP cung cấp các cơ chế để cố gắng truyền dữ liệu tới được ứng dụng đích và ben gửi biết dữ liệu này có được truyền đi thành công hay không.

**Các vấn đề an toàn bảo mật của giao thức TCP:**

**Tấn công do thám mạng:**

**-** Là các hành vi lợi dụng hoạt động của các giao thức để thu thập thông tin hoạt động của các máy tính trong mạng, bao gồm trạng thái kết nối, các dịch vụ đang cung cấp, hệ điều hành và các phần mềm dịch vụ được cài đặt.