**CHƯƠNG 1 : COMPUTER SECURITY CONCEPTS**

I – Giới thiệu

Những thông tin cần an toàn : Thông tin cá nhân, nhạy cảm (individuals store a lot of sensitive data online)

An toàn thông tin : the assurance ( sự đảm bảo ) of confidentiality ( bí mật ), integrity and availability of information.

II- Các đặc tính thông tin

Tính sẵn sàng ( availability )

Tính chính xác

Tính xác thực

Tính bí mật ( confidentiality )

Tính toàn vẹn ( integrity )

III – Tổ chức cần có nhiều lớp bảo mật

Physical security

Personal security

Operations security

Communications security

Network security

Information security

IV – NSTISSC security model ( mô hình bảo mật NSTISSC )

V – The security system life cycle

CIA triad

Accountability : tính chịu trách nhiệm ( hệ thống sẽ ghi lại toàn bộ hoạt động )

Non-repudiation : chống chối, chống khoái thác 🡪 xây dựng hệ thống đảm bảo người tham gia chịu trách nhiệm cho các hoạt động của mình

Authenticity : tính xác thực

Confidentiality : tính bí mật

Integrity : tính toàn vẹn

Availability : tính sẵn sàng

Thành phần :

Con người :

Hardware :

Software :

Procedure ( quy trình ) :

Network :

Data :

🡪 Có an toàn không ? dựa vào các tiêu chí về tính integrity, availability, confidentiality, authentication, accountability 🡪 mỗi yếu tố cần có minh chứng, được thể hiện ở chỗ nào ?

Có những hệ thống, phần cứng có thể được nhìn chỉ cần không gây hư hại.

Bài tập

Thư viện

Thành phần :

Con người : sinh viên, giáo viên, thủ thư

Hardware : bàn ghế, kệ, tủ, sách, máy tính, máy lạnh…

Software : phần mềm quản lý thông tin sách, mượn trả, nhập sách, tra cứu

Procedure ( quy trình ) :

1. Để đồ như túi, balo, áo khoác, nón,… ở ngoài thư viện
2. Check thẻ sinh viên để xác nhận danh tính
3. Nếu mượn sách thì cần tìm đến và lấy rồi đem ra xác nhận danh tính để mượn cho thủ thư. ( chưa biết vị trí thì có thể sử dụng hệ thống tra cứu sách )
4. Khi trả, cần đến và check thẻ sinh viên để xác nhận danh tính để trả.

Network : tường lửa, hệ thống nhắc nhở trả sách, giới thiệu sách mới, hệ thống tra cứu.

Data : lưu trữ thông tin sách, thông tin người mượn, nhật mượn trả, nhật kí nhập hàng.

🡪 Có an toàn không ? dựa vào các tiêu chí về tính integrity, availability, confidentiality, authentication, accountability 🡪 mỗi yếu tố cần có minh chứng, được thể hiện ở chỗ nào ?

Có những hệ thống, phần cứng có thể được nhìn chỉ cần không gây hư hại.

Phần tích :

Phần mềm tra cứu sách:

Tính toàn vẹn : đội hậu cần bảo trì định kì

Tính sẵn sàng : luôn trong trạng thái mở để người dùng sử dụng

Tính bí mật : không có phân quyền

Tính xác thực : cần được đăng nhập, xác nhận danh tính

Tính chịu trách nhiệm : lưu trữ hoạt động tra cứu

VI- Key terms

Attack :

Threats : mối đe doạ

Threat agent :

Vulnerability : dễ tổn thương = lỗ hỗng ( trong hệ thống thì là lỗ hỗng, cũng là lỗi )

Hacking :

Risk : rủi ro ( khi mối đe doạ bị khai thác thì sẽ gây ra rủi ro )

Subject :

Access :

Asset : tài sản số

Control, safeguard or countermeasure …. : các chính sách bảo mật, đối phó với tấn công, giải quyết lỗ hỗng, giảm rủi ro….

Exploit : khai thác ( khai thác điểm yếu )

Exposure : bung ra ( khi lỗ hỗng bị khai thác thì nó sẽ bung ra toàn bộ sự nguy hiểm )

…..

VII- Threat and the types of threat actions

Unauthorized

Deception liên quan đến intergrity

Disruption

Usurpation

VIII- Attacks

So sánh tấn công bị động ( pasive attack ) và tấn công chủ động ( Active Attack )

Tấn công bị động : khó phát hiện nhưng dễ dàng ngăn chặn. Có các phần mềm có thể giám sát để có thể phát hiện điều bất thường.

Tấn công chủ động : khó ngăn chặn, chỉ còn cách khôi phục

Mối liên quan : có thể kết hợp, hợp tác.

Attack surface : giảm thiểu để đảm bảo an toàn

Attack vector : sẽ có nhiều hướng tấn công vào đối tượng

Attack tree :