Bảo mật là j?

Nói chung bảo mật là “ trách nhiệm hoặc trạng thái an toàn để tránh khỏi những mối đe dọa. Nói cách khác , bảo vệ chống lại kẻ thù từ những người sẽ làm gây hại, cố ý hay nói cách khác là mục tiêu. Vs dụ, an ninh quốc gia là 1 hệ thống nhiều lớp để bảo vệ chủ quyền của 1 quốc gia , tải sản ,tài nguyên, con người của quốc gia đó. Để đạt được 1 mức bảo mật thích hợp cho môt hệ thống cần nhiều mặt. Một tổ chức thành công nên có nhiều lớp bảo mật để đảm bảo việc hoạt động của nó:

National security: an ninh quốc gia

protection against adversaries: bảo vệ chống lại kẻ thù

sovereignty: chủ quyền

resources: tài nguyên

assets: tài sản

appropriate :phù hợp,thích hợp

an ninh vật lý:để bảo vệ 1 các cá thể vật lý, các đối tượng hoặc các khu vực từ truy cập trái phép và lạm dụng

unauthorized access:truy cập trái phép

misuse: lạm dụng

an ninh nhân sự: để bảo vệ các cá nhân hoặc các nhóm người. Người được phép truy cập vào tổ chức và các hoạt động của nó

individual : cá nhân

authorized: có quyền

ogannization: tổ chức

operation: hoạt động

an ninh hoạt động:để bảo vệ các chi tiết của 1 hoạt động cụ thể hoặc chuỗi các hoạt động

particular : đặc thù, cụ thể

an ninh truyền thông, bảo vệ phương tiện truyền thông, công nghệ và nội dung

Communications security: bảo vệ thông tin liên lạc

communications media: phương tiện truyền thông

an ninh mạng, để bảo vệ các thành phần mạng,sự kết nối và các nội dung

components: thành phần

an ninh thông tin, để bảo vệ tính bí mật, tính toan vẹn và sẵn có của tài sản thông tin trong lưu trữ, xử lý hoặc truyền tải. nó đạt được thông qua việc áp dụng các chính sách,giáo dục, dào tạo và nhận thức và công nghệ

confidentiality:bảo mật,bí mật

integrity:tính toàn vẹn

transmission: truyền tải

achieve: đạt được

awareness: nhận thức

Ủy ban về Hệ thống An ninh Quốc gia (CNSS) định nghĩa an toàn thông tin như việc bảo vệ thông tin và các yếu tố quan trọng của nó, bao gồm các hệ thống và phần cứng sử dụng, lưu trữ và truyền tải thông tin đó. Hình 1-3 cho thấy an ninh thông tin bao gồm các lĩnh vực rộng lớn của quản lý an ninh thông tin, bảo mật máy tính và dữ liệu, và bảo mật mạng. Mô hình thông tin CNSS bảo mật phát triển từ một khái niệm được phát triển bởi ngành bảo mật máy tính được gọi là C.I.A. Tam giác. C.I.A. tam giác đã là tiêu chuẩn công nghiệp cho bảo mật máy tính kể từ khi phát triển máy tính lớn. Nó dựa trên ba các đặc điểm của thông tin mang lại giá trị cho tổ chức: bảo mật, tính toàn vẹn và tính sẵn có. Tính bảo mật của ba đặc điểm này của thông tin ngày nay vẫn quan trọng như trước đây, nhưng C.I.A. mô hình tam giác không còn tương thích môi trường thay đổi liên tục. Các mối đe dọa đối với tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin đã phát triển thành một tập hợp các sự kiện, bao gồm thiệt hại vô tình hoặc cố ý, phá hủy, trộm cắp, sửa đổi ngoài ý muốn hoặc trái phép, hoặc lạm dụng khác từ con người hoặc mối đe dọa phi nhân loại. Môi trường mới này với nhiều mối đe dọa liên tục phát triển đã đã thúc đẩy sự phát triển của một mô hình mạnh mẽ hơn nhằm giải quyết các vấn đề phức tạp của môi trường an toàn thông tin hiện nay.

Committee: ủy ban

Defines: định nghĩa

critical elements: yếu tố quan trọng

industry standard: tiêu chuẩn công nghiệp

based: dựa trên

characteristics: đặc trưng đặc điểm

adequately addresses: tương thích

the constantly changing environment: môi trường thay đổi liên tục

accidental: vô tình

intentional: cố ý

a more robust:mạnh mẽ hơn

unintended:ngoài ý muốn

unintended:ko được phép

Quyền truy cập: Khả năng sử dụng, thao tác, sửa đổi hoặc ảnh hưởng đến chủ thể hoặc đối tượng khác. Người dùng được ủy quyền có quyền truy cập hợp pháp vào hệ thống, trong khi tin tặc có quyền truy cập bất hợp pháp vào một hệ thống. Kiểm soát truy cập quy định điều này khả năng.

Manipulate: thao tác

Tài sản: Tài nguyên tổ chức đang được bảo vệ. Một tài sản có thể logic, chẳng hạn như trang Web, thông tin hoặc dữ liệu; hoặc một tài sản có thể là vật chất, chẳng hạn như một người, hệ thống máy tính hoặc đối tượng hữu hình khác. Tài sản và đặc biệt là tài sản thông tin, là trọng tâm của các nỗ lực bảo mật; họ là những gì những nỗ lực đang cố gắng để bảo vệ.

Tấn công:các hoạt dộng vô ý hay cố ý có thể gây ra thiệt hại hoặc làm tổn hại thồn tin/ các hệ thống hỗ trợ thông tin đó. Các cuộc tấn công có thể chủ động hay bị động, cố ý hay vô ý, trực tiếp hay gián tiếp. Người nào tình cờ đọc thông tin nhạy cảm không nhằm mục đích sử dụng của mình là một cách thụ động tấn công.

sensitive information: thông tin nhạy cảm

Một hacker cố gắng đột nhập vào một hệ thống thông tin là một cuộc tấn công có chủ đích. Một sét đánh gây ra hỏa hoạn trong một tòa nhà là một cuộc tấn công không cố ý. Trực tiếp tấn công là việc hacker sử dụng máy tính cá nhân để đột nhập vào một hệ thống. Gián tiếp tấn công là một tin tặc xâm nhập một hệ thống và sử dụng nó để tấn công các hệ thống khác, ví dụ, như một phần của mạng botnet (tiếng lóng của mạng rô-bốt). Nhóm bị xâm phạm này máy tính, chạy phần mềm do kẻ tấn công lựa chọn, có thể hoạt động độc lập hoặc dưới sự kiểm soát trực tiếp của kẻ tấn công để tấn công hệ thống và đánh cắp thông tin người dùng hoặc tiến hành tấn công từ chối dịch vụ tấn công. Các cuộc tấn công trực tiếp bắt nguồn từ mối đe dọa chính nó. Các cuộc tấn công gián tiếp bắt nguồn từ một hệ thống hoặc tài nguyên bị xâm phạm đang bị trục trặc hoặc hoạt động dưới sự kiểm soát của một mối đe dọa.

break into: đột nhập vào…

denial-of-service attacks: sự từ chối của dịnh vụ tấn công

originate: bắt nguồn

malfunctioning: trục trặc

Kiểm soát, bảo vệ hoặc biện pháp đối phó: Cơ chế bảo mật, chính sách hoặc thủ tục có thể chống lại thành công các cuộc tấn công, giảm thiểu rủi ro, giải quyết các lỗ hổng mặt khác cải thiện an ninh trong một tổ chức.

Countermeasure: biện pháp đối phó

Mechanisms: cơ chế

reduce risk: giảm rủi ro

vulnerabilities: lỗ hổng

Khai thác: Một kỹ thuật được sử dụng để thỏa hiệp một hệ thống. Thuật ngữ này có thể là một động từ hoặc một danh từ. Các tác nhân đe dọa có thể cố gắng khai thác một hệ thống hoặc thông tin khác bằng cách sử dụng nó bất hợp pháp cho các mục đích cá nhân của họ. Hoặc, một khai thác có thể là một tài liệu quá trình để tận dụng một lỗ hổng hoặc phơi bày, thường là trong phần mềm, đó là vốn có trong phần mềm hoặc do kẻ tấn công tạo ra. Khai thác sử dụng các công cụ phần mềm hiện có hoặc các thành phần phần mềm tùy chỉnh.

+ phơi nhiễm (exposure ) : tình trạng hoặc trạng thái bị phơi nhiễm . Trong bảo mật thông tin , sự phơi nhiễm tồn tại khi có 1 lỗ hổng mà kẻ tấn công biết đến hiện nay.

+ Mất mát (Loss) : Một trường hợp duy nhất của một tài sản thông tin bị thiệt hại hoặc sửa đổi hoặc tiết lộ ngoài ý muốn hoặc trái phép . Khi thông tin của một tổ chức bị đánh cắp , nó đã bị tổn thất

+ Bảo vật hồ sơ hoặc bảo mật tư thế : Toàn bộ các biện pháp kiểm soát và bảo mật , bao gồm chính sách , giáo dục , đào tạo và nhận thức và công nghệ , mà một tổ chức thực hiện (hoặc không thực hiện ) để bảo vệ tài sản . Các thuật ngữ này đôi khi được sử dụng để thay thế cho thuật ngữ chương trình bảo mật , mặc dù chương trình bảo mật bao gồm các khía cạnh quản lý về bảo mật , bao gồm kế hoạch, nhân sự , và chương trình cấp dưới

Exposure : phơi nhiễm

Condition : tình trạng

Single instance : trường hợp duy nhất

suffering damage ; bị thiệt hại , chịu thiệt hại

disclosure : tiết lộ

stolen : ăn cắp

entire : toàn bộ

implements : thực hiện

comprises : bao gồm

aspects : các khía cạnh

subordinate : cấp dưới

+ Rủi ro (Risk) : Khả năng xảy ra điều gì đó không mong muốn . Các tổ chức phải giảm thiếu rủi ro để phù hợp với mong muốn rủi ro của họ - Số lượng và bản chất của rủi ro mà tổ chức sẵn sàng chấp nhất .

+ Chủ thể và đối tượng (subject and objects ) : Một máy tính có thể là đối tượng của một cuộc tấn công – một tác nhân được sử dụng để thực hiện cuộc tấn công - hoặc đối tượng của một cuộc tấn công – thực thể mục tiêu , hình 1-4 cho thấy . Một máy tính có thể là chủ thể vừa là đối tượng của một cuộc tấn công , ví dụ khi nó bị xâm nhập bởi một cuộc tấn công (đối tượng ) , và nó sử dụng để tấn công các hệ thống khác .

Probability : khả năng

will happen : sẽ xảy ra

to match : bằng , phù hợp

quantity : số lượng

nature : bản chất

entity : thực thể

weaknesses : điểm yếu

+ Mối đe dọa ( threat) : Một loại đối tượng , người, hoặc thực thể khác để gây nguy hiểm cho tài sản . Các mối đe dọa luôn hiện hữu và có thể có mục đích hoặc vô hướng . Ví dụ , Hacker cố tình đe dọa các hệ thống thông tin không được bảo vệ , khi những cơn bão nghiêm trọng vô tình đe dọa các hệ thống và nội dung của chúng

+Tác nhân đe dạo (threat agents) : Trường hợp cụ thể hoặc 1 thành phần của 1 mối đe dọa. Ví dụ tất cả hacker trong thế giới hiện nay đều là mối đe dọa tập thể , Trong khi kevin Mitnick , người bị kết án xâm nhập vào hệ thống điện thoại , là một tác nhân đe dọa cụ thể . Tương tự như vậy , set đánh , mưa đá hoặc lốc xoáy là tác nhân đe dọa là một phần của mối đe dọa của các cơn bão

+ Lỗ hổng bảo mật (vulnerability) : là điểm yếu hoặc lỗi hệ thống hoặc cơ chế bảo mật khiến nó bị tấn công hoặc phá hoại . 1 số ví dụ về lỗ hổng bảo mật là lỗ hổng trong gói phần mềm , cổng hệ thống không được bảo vệ và cửa không khóa . Một số lỗ hổng nổi tiếng đã được kiểm tra, ghi lại , và công khai , Những lỗ hổng khác vẫn còn tiềm ẩn ( hoặc chưa được khám phá )

Câu 1:

An toàn thông tin gồm những lĩnh vực nào?

Management of information sercurity, computer &data sercurity and network sercurity

Câu 2:

Tại sao mô hình tam giác CIA ko còn giải quyết thỏa đáng trong môi trường thay dổi lien tục

The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats

Câu 3

What is security? What is information security?

security is “the quality or state of being secure to be free from danger.”

Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission

Câu 4

How many fundamental characteristics does information have? What are they?

3 fundamental characteristics: confidentality, integrity and availability

Câu 5

Since when has the C.I.A triangle been industry standard for computer security? What is it based on?

The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability

Câu 6

What should a successful organization have to protect its operation?

Physical security, Personnel security, Operations security, Communications security, Network security, Information security.

Câu 7

What is attack? What types of attack are mentioned in the passages?

Attack: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it.

intentional attack, unintentional attack, direct attack, indirect attack

câu 8

What is vulnerability? Give some examples of vulnerabilities.

Vulnerability: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage

Ms17010,log4j,sql injection

2.2

1 false

2 true

3 false

4 NI

5 true

6 true

7true

8false