Mục Lục

1. **Trình bày các khái niệm "an toàn thông tin", "an ninh thông tin". Phân biệt hai khái niệm này.**

An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân [72/2013/NĐ-CP].

Phân biệt: An ninh thông tin đảm bảo thông trên mạng. ATTT đảm bảo an toàn trong hệ thống tập trung vào tính nguyên vẹn, bảo mật, khả dụng của thông tin

2. **Trình bày khái niệm, phân loại hiểm họa an toàn thông tin, cho ví dụ đối với từng loại.**

****Hiểm họa ATTT*** của HTTT là những khả năng tác động lên TT, HTTT dẫn tới sự thay đổi, hư hại, sao chép, sự ngăn chặn tiếp cận tới TT; tới sự phá huỷ hoặc sự ngừng trệ hoạt động của vật mang TT.

Ví dụ: virus, động đất, tấn công mạng,…

****Phân loại hiểm họa an toàn thông tin theo các tiêu chí khác nhau:***

-Theo bản chất xuất hiện

+Hiểm họa tự nhiên: thiên tai, mối mọt, ẩm mốc,...

+ Hiểm họa nhân tạo: phá hoại, thao tác sai,...

-Theo mức độ định trước

+Hiểm họa từ hành động vô ý: tải 1 tập tin có virus trên mạng về máy

+Hiểm họa từ hành động có chủ ý: Cố tình phát tán virus

-Theo nguồn trực tiếp sinh ra

+Nguồn sinh trực tiếp là con người

+ Nguồn sinh là các phần mềm hợp lệ

+ Nguồn sinh là các phần mềm trái phép: malware tấn công

-Theo vị trí của nguồn sinh ra

+Vùng 1: phạm vi cơ quan, đơn vị, tổ chức.

+Vùng 2:phạm vi tòa nhà.

+Vùng 3: phòng chờ lễ tân, trực ban

+Vùng 4: phòng họp, phòng làm việc của cán bộ, nhân viên

+Vùng 5: Những khu vực đặc biệt quan trọng của lãnh đạo.

+Vùng 6: Tủ chứa tài liệu, cơ sở dữ liệu

-Theo mức độ hoạt động của HTTT

+ Không phụ thuộc vào hoạt động của hệ thống

+ Chỉ xuất hiện khi hệ thống hoạt động

-Theo mức độ tác động lên HTTT

+ Hiểm họa thụ động, không làm thay đổi cấu trúc, nội dung của hệ thống

+ Hiểm họa tích cực, gây ra những thay đổi nhất định trong hệ thống

3. Phân biệt các khái niệm "điểm yếu" và "lỗ hổng". Cho ví dụ (có giải thích).

Điểm yếu là những chỗ trong hệ thống mà tại đó không có biện pháp kiểm soát hoặc biện pháp kiểm soát không có tác dụng (điểm yếu:có thể sẽ bị khai thác)

Lỗ hổng của HTTT là những khiếm khuyết trong chức năng, thành phần nào đó của HTTT mà có thể bị lợi dụng để gây hại cho hệ thống. (thực tế đã bị khai thác)

Ví dụ: Không có cơ chế ngăn chặn duyệt mật khẩu, không có UPS

Một lỗ hổng bị khai thác bởi nhiều hiểm họa khác nhau, lỗ hổng thực tế là đã bị khai thác.

4. Nêu và giải thích các nguyên tắc chung đảm bảo an toàn thông tin.

1. Nguyên tắc tính hệ thống

• Các yếu tố, các điều kiện và các nhân tố có quan hệ với nhau, có tương tác với nhau và có biến đổi theo thời gian

• Chống lại cả những kênh truy cập trái phép tiềm tàng (chưa biết)

2. Nguyên tắc tổng thể

• Các biện pháp phải thống nhất, đồng bộ

• Phải tổ chức phòng ngự nhiều lớp

. Nguyên tắc bảo vệ liên tục

• Đảm bảo ATTT là quá trình liên tục

• Xuyên suốt chu kỳ sống của hệ thống, từ thiết kế cho đến loại bỏ

4. Nguyên tắc đầy đủ hợp lý

• Không có an toàn tuyệt đối

• Biện pháp bảo vệ ít nhiều đến hoạt động của hệ thống

• Biện pháp bảo vệ thường tốn kém

• Chi phí cho việc bảo vệ không lớn hơn giá trị của hệ thống

• Mục tiêu của bảo vệ là đưa rủi ro về mức chấp nhận được

5. Nguyên tắc mềm dẻo hệ thống

• Phân hệ an toàn được thiết lập trong điều kiện có nhiều bất định

• Phải cho phép nâng cấp, cập nhật

6. Nguyên tắc đơn giản trong sử dụng

• Cơ chế bảo vệ không được gây khó khăn cho người dùng hợp lệ

7. Nguyên tắc công khai thuật toán và cơ chế bảo vệ

• Biết được thuật toán, cơ chế bảo vệ cũng không thể vượt qua được

• Chính tác giả cũng không thể vượt qua

• Không có nghĩa là phải công khai thuật toán và cơ chế bảo vệ

5. Nêu khái niệm "rò rỉ thông tin". Liệt kê các kênh rò rỉ thông tin.

Rò rỉ thông tin là việc thông tin mật bị phát tán một cách không kiểm soát ra ngoài phạm vi tổ chức hoặc ra ngoài nhóm người, mà trong đó thông tin được coi là an toàn.

Các kênh rò rỉ thông tin:

- Rò rỉ thông tin qua kênh tiêu chuẩn:

+ Thiết bị lưu trữ di động

+ Thư điện tử

+ Hội thoại

+ Diễn đàn

+ các giao thức, dịch vụ mạng khác (http)

+ giao tiếp thoại (trực tiếp, voip, phone)

+ photocopy, scanner, camera

- rò rỉ thông tin qua kênh kỹ thuật là việc phát tán (lan truyền) thông tin mật một cách không kiểm soát từ vật mang qua một môi trường vật lý nhất định đến thiết bị thu thông tin.

6. Trình bày khái niệm "định danh", "xác thực" và "phân quyền". Lấy ví dụ để phân biệt 3 tác vụ trên.

Định danh (identification) là việc gắn định danh (identificator) cho người dùng và kiểm tra sự tồn tại của định danh đó

Xác thực (authentication) là quá trình kiểm tra tính chân thực của danh tính được xác lập trong quá trình định danh

Cấp quyền (Authorization) là việc xác định một chủ thể (subject) đã được xác thực được phép thực hiện những thao tác nào lên những đối tượng (object) nào trong hệ thống

7. Trình bày khái niệm và phân loại "nhân tố xác thực". Cho ví dụ với mỗi loại nhân tố xác thực, chỉ ra ứng dụng của nhân tố xác thực đó.

Nhân tố xác thực (authentication factor) là thông tin sử dụng cho quá trình xác thực.

Có 3 loại nhân tố xác thực chính

–Cái người dùng biết

• Thường là mật khẩu:

• Ngoài ra: tr.lời cho 1 số câu hỏi riêng tư. Chủ yếu để khôi phục mật khẩu

• Ưu điểm: đơn giản, chi phí thấp

• Nhược điểm: Có thể bị lộ (đánh cắp), có thể bị quên

–Cái người dùng có

• Chìa khóa, giấy tờ tùy thân

• Thẻ từ, smartcard

• OTP token, Cryptographic token, khóa mật mã

• SIM điện thoại

• Ưu điểm: phù hợp cho xác thực đa nhân tố

• Nhược điểm: Chi phí cao, có thể bị mất, chiếm đoạt, làm giả

–Cái thuộc về bản thể người dùng

• Khuôn mặt, vân tay, bàn tay, võng mạc, giọng nói

• Ưu điểm: không bị sao chép, làm mất, đánh cắp

• Nhược điểm: Chi phí rất cao, có thể thay đổi theo thể trạng, không phù hợp cho xác thực qua mạng

Có 2 nhóm nhân tố xác thực khác

– Đặc điểm hành vi người dùng

• Chữ ký bàn phím

• Chữ ký viết tay (tốc độ và gia tốc)

• Ưu điểm: không bị sao chép, đánh cắp

• Nhược điểm: chi phí cao, không ổn định, có thể thay đổi theo thời gian, không phù hợp cho xác thực qua mạng

–Vị trí của người dùng

• Vị trí trên mặt đất (qua hệ thống định vị toàn cầu)

• Nhược điểm: Chi phí rất cao, làm lộ thông tin riêng tư người dùng

8. Trình bày khái niệm "mật khẩu". Hãy chỉ ra các hiểm họa an toàn đối với mật khẩu.

Mật khẩu là một lượng thông tin mật nào đó, mà chỉ có người dùng và hệ mật khẩu được biết, mà người dùng cần phải nhớ và đưa ra để đi qua thủ tục xác thực.

Hiểm họa an toàn đối với mật khẩu.

• Thông qua tìm kiếm, dò đoán.

• Nhìn trộm.

• Qua bàn giao định trước mật khẩu cho người khác.

• Đánh cắp CSDL của hệ mật khẩu.

• Chặn bắt các thông tin chứa mật khẩu

• Lưu giữ mật khẩu ở vị trídễ tiếp cận.

• Đưa vào các bẫy chương trình.

• Khai thác các lỗi ở giai đoạn thiết kế.

• Làm hỏng hệ mật khẩu

• Lựa chọn mật khẩu dễ nhớ và cũng dễ đoán.

• Ghi các mật khẩu khó nhớ và lưu ghi chép đó tại nơi dễ tiếp cận

• Đưa mật khẩu vào mà để cho người khác nhìn thấy được.

• Cho người khác mật khẩu một cách cố ý hoặc do nhầm lẫn.

• Hiểm họa an toàn khi truyền mật khẩu qua mạng

Chặn bắt và dùng lại thông tin.

Chặn bắt và khôi phục mật khẩu

Thay đổi thông tin với mục đích đánh lừa phía kiểm tra.

Kẻ xấu bắt chước hđộng của phía kiểm tra để đánh lừa người dùng

9. Hãy chỉ ra các yêu cầu an toàn đối với hệ mật khẩu. Giải thích ý nghĩa của các yêu cầu đó.

Yêu cầu đối với hệ mật khẩu

1. Xác định độ dài cực tiểu của MK: làm khó cho kẻ xấu muốn nhìn trộm hoặc tấn công bằng phương pháp "vét cạn"

2. Trong MK dùng các nhóm ký hiệu khác nhau: hạn chế phương pháp tấn công "vét cạn" của đối phương

3. Kiểm tra và loại bỏ MK theo từ điển: chống lại phương pháp đoán nhận MK theo từ điển của đối phương

4. Xác định độ dài cực đại thời gian MK: hạn chế tấn công theo kiểu "vét cạn", kể cả khi tiếp cận từ xa (chế độ off-line)

5. Xác định độ dài cực tiểu thời gian dùng MK: ngăn cản ý định người dùng đổi MK như cũ sau khi đến hạn đổi theo yêu cầu trên

6. Hạn chế số lượng các ý định đưa MK vào: hạn chế ý đồ tấn công lựa chọn tích cực của đối phương

7. Duy trì chế độ bắt buộc thay đổi MK người dùng: bảo đảm hiệu quả cho đòi hỏi hạn chế độ dài cực đại tác dụng MK

8. Dùng biện pháp dừng kéo dài khi có MK sai đưa vào: hạn chế phương pháp lựa chọn tích cực của đối phương

9. Cấm việc tự ngdùng chọn MK và sinh MK tự động hoá bằng thuật toán: chống lại việc đoán MK theo từ điển và chống lại tấn công "vét cạn" của đối phương

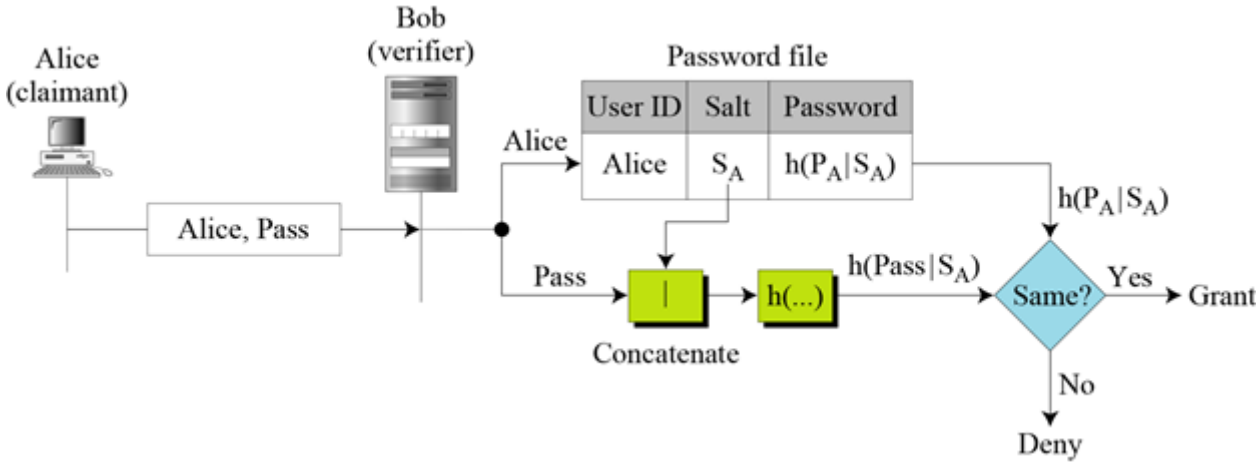
10.Bắt buộc đổi MK khi lần đầu tiên ghi nhận người dùng trong HT: ngăn cản các hành vi trái phép của nhà quản trị hthống có quyền tiếp cận hệ MK ở thời điểm bắt đầu ghi danh sách kiểm toán

11.Đưa ra sổ ghi lý lịch các MK: tăng cường khả năng an toàn của các MK kèm với các đòi hỏi khác

10. Trình bày các khái niệm "từ điển mật khẩu", "bảng băm mật khẩu" (precomputed hash table). Giải thích cách sử dụng các đối tượng nói trên.

Từ điển mật khẩu là danh sách tập hợp các mật khẩu thường được sử dụng nhất.

11. Cho sơ đồ giao thức xác thực sử dụng mật khẩu



Hãy trình bày hoạt động của giao thức (bao gồm cả pha khởi tạo). Giải thích quyết định cuối cùng của Bob. Hãy chỉ ra 2 khả năng tấn công lên giao thức đã cho.

Pha khởi tạo:

+ Salt: được tạo ngẫu nhiên với chiều dài bất kỳ, nhưng thường là 8 byte(64 bit) là đủ độ khó để cho attacker khó dò tìm được Salt.

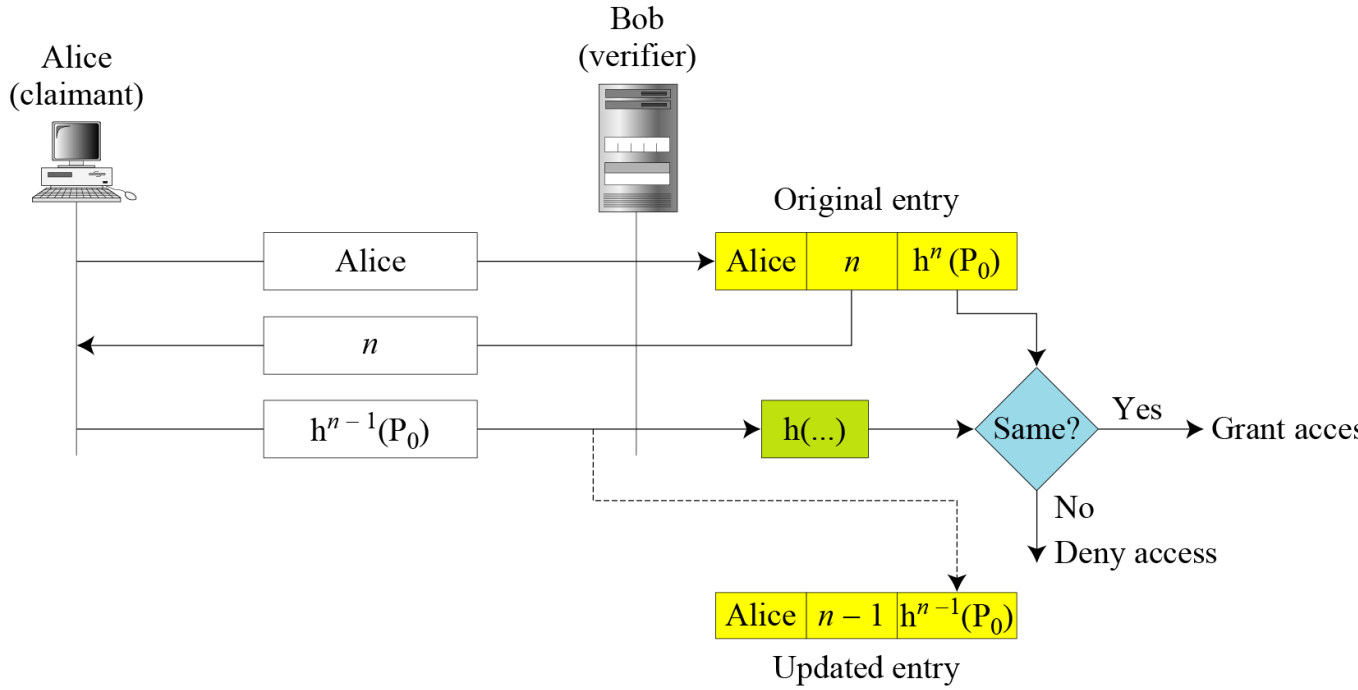
+ Password file lưu trữ: tên người dùng, Salt, Password đã được băm cùng với Salt

Đầu tiên Alice gửi thông tin bao gồm ID và Pass. Tìm xem ID có tồn tại hay không nếu có thì gửi lại Salt của ID dùng để băm (Pass người dùng nhập vào và Salt ID tìm được). So sánh 2 Pass nếu đúng thì xác thực thành công ngược lại thì không.

=>> 2 Khả năng tấn công lên giao thức.

Chặn bắt thông tin trong khi truyền tới Bob

12. Cho sơ đồ giao thức xác thực bằng mật khẩu một lần Lamport



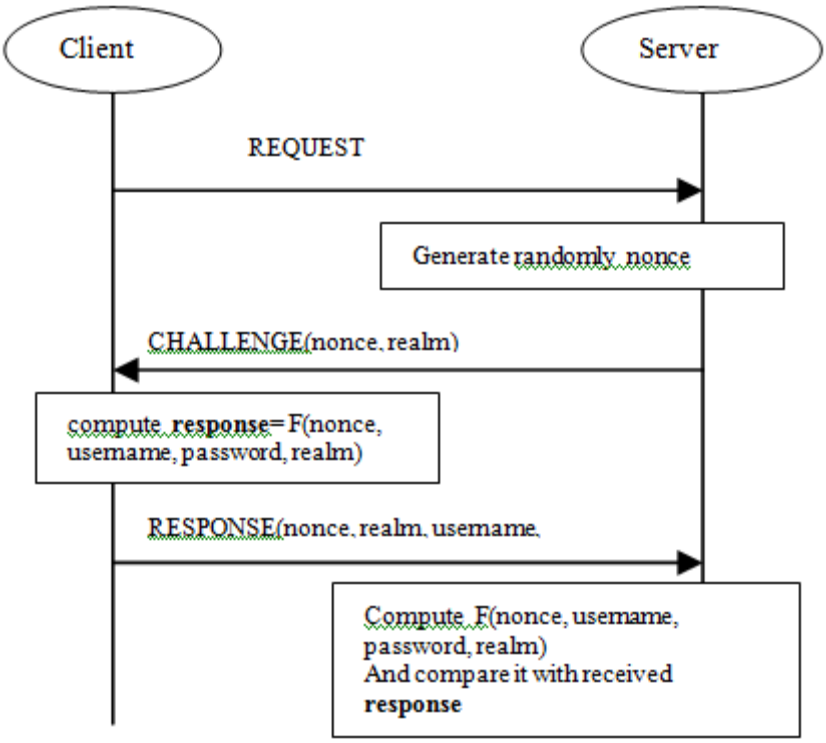
Hãy giải thích hoạt động của giao thức (bao gồm cả pha khởi tạo). Giải thích quyết định cuối cùng của Bob. Giải thích tấn công Man-In-The-Middle lên giao thức đã cho.

Khởi tạo: Trong database sẽ lưu trữ ID, n (number), Hash n lần Password (sau mỗi lần xác thực thành công thì n sẽ giảm đi 1)

Đầu tiên Alice yêu cầu xác thực. Bob sẽ tìm trong database để trả lại 1 giá trị (n-1) cho Alice. Alice Hash (n-1) lần Password rồi gửi cho Bob. Bob nhận được sẽ Hash thêm 1 lần nữa rồi dem so sánh với Hash n lần trong database nếu đúng thì cho phép truy cập ngược lại thì ko.

Sau mỗi lần đăng nhập thành công database sẽ update lại n thành (n -1) và Hash(P)

13. Cho sơ đồ giao thức xác thực bằng mã băm (Digest Authentication)



Hãy giải thích hoạt động của giao thức (bao gồm pha khởi tạo). Giải thích quyết định cuối cùng của Server. Hãy chỉ ra điểm yếu của giao thức đã cho.

1. Đầu tiên Client gửi 1 requires authentication lên Server
2. Server sẽ trả về nonve và realm cho client
3. Ở tại client sẽ tính toán response bằng cách dùng MD5

   HA1=MD5(username:realm:password)

   HA2=MD5(method:digestURI)

   response=MD5(HA1:nonce:HA2)
4. sau đó gửi username, password cùng với response lên Server.

…

14. Hãy giải thích các mô hình kiểm soát truy cập DAC, MAC và RBAC.

- Kiểm soát truy cập tùy chọn DAC:

Mô hình ít hạn chế nhất

Mọi đối tượng đều có một chủ sở hữu

Chủ sở hữu có toàn quyền điều khiển đối với đối tượng của họ

Chủ sở hữu có thể cấp quyền đối với đối tượng của mình cho một chủ thể khác.

Được sử dụng trên các hệ điều hành như Microsoft Windows và hầu hết các hệ điều hành Unix

Nhược điểm của DAC:

Phụ thuộc vào quyết đinh của người dùng để thiết lập cấp độ bảo mật phù hợp.

Quyền của chủ thể sẽ được thừa kế bởi các chương trình mà chủ thể thực thi

Trojan là một vấn đề đặc biệt của DAC

- Kiểm soát truy cập bắt buộc MAC:

Là mô hình điều khiển truy cập nghiêm ngặt nhất

Thường bắt gặp trong thiết lập quân đội

Hai thành phần: nhãn và cấp độ

Mô hình Mac cấp quyền bằng cách đối chiếu nhãn của đối tượng với nhãn chủ thể

Để xác định có mở file hay không:

So sánh nhãn của đối tượng với nhãn của chủ thể.

Chủ thể phải có cấp độ tương đương hoặc cao hơn: đối tượng được phép truy cập.

Hai mô hình thực thi của MAC

Mô hình dạng lưới

Mô hình Bell – Lapadula

Mô hình mạng lưới

Các chủ thể và đối tượng được gán một cấp bậc trong mạng lưới.

Nhiều mạng lưới có thể đạnh cạnh nhau

Mô hình Bell – LaPadula

Tương tự mô hình mạng lưới.

Các chủ thể không thể tạo một đối tượng mới hay thực hiện một số chúc năng nhất đinh đối với các đối tượng có thấp hơn.

- Kiểm soát truy cập dựa trên vai trò RBAC

Điều khiển truy cập RBAC dựa trên vai trò:

Còn gọi là điều khiển truy cập không tùy ý

Quyền truy cập dựa trên chức năng công việc

RBAC gán các quyền cho các vai trò cụ thể trong tổ chức.

Điều khiển truy cập dựa trên các quý tắc:

Tự động gán vai trò cho các chủ thể dựa trên một tập quy tắc do người giám sát quy định

Mỗi đối tượng tài nguyên chứa các thuộc tính truy cập dựa trên quy tắc.

Khi người dùng truy cập tới tài nguyên hệ thống sẽ kiểm tra các quy tắc của đối tượng để xác đinh quyền truy cập.

Thường sử dụng để quản lý truy cập ngườ dùng tới một hoặc nhiều hệ thống

15. Hãy phân biệt dạng thức sử dụng mật mã để đảm bảo tính bí mật thông tin là mã hóa dữ liệu lưu trữ, mã hóa đầu cuối và mã hóa kênh truyền. Lấy một ví dụ cho mỗi dạng thức.

Mã hóa dữ liệu lưu trữ

-Dữ liệu chủ yếu tồn tại ở dạng mã hóa

-Chỉ đc giải mã khi cần sử dụng

-Sau khi dùng xong, dữ liệu đc mã hóa trở lại

Ví dụ:

• Encryption File System

• Mã hóa email, điện mật

• Các ứng dụng mật mã khác: Office, PDF,...

• Hệ quản trị tập tin mật mã EFS

• Mã hóa ổ đĩa

• Mã hóa dữ liệu khi đồng bộ qua đám mây

Mã hóa đầu cuối

-Dữ liệu ở các điểm đầu cuối tồn tại ở dạng rõ

-Khi truyền đi, dữ liệu được mã hóa

-Ứng dụng truyền/nhận thực hiện mã hóa/giải mã một cách rõ ràng

Ví dụ: Mã thoại, các giao thức: HTTPS, SSH...

Mã hóa kênh truyền

-Dữ liệu ở các điểm đầu cuối tồn tại ở dạng rõ

-Khi truyền đi, dữ liệu được mã hóa

-Dữ liệu được mã hóa ở tầng mạng hoặc bởi gateway; ứng dụng truyền/nhận không tự mình mã hóa

Ví dụ: Các giao thức VPN:

Site-to-Site (Tunnel mode) VPN

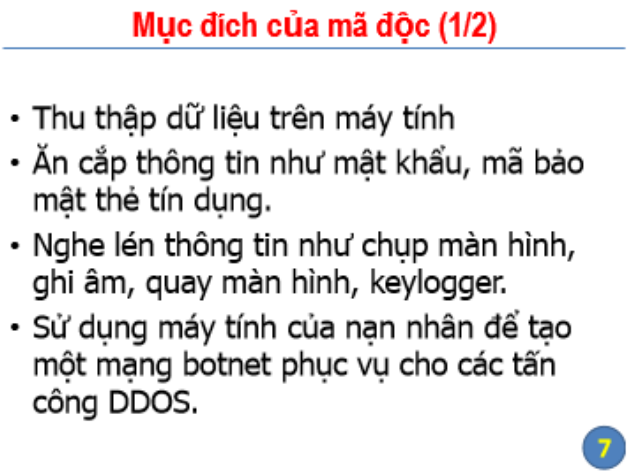
Point-to-Point(Transport mode) VPN

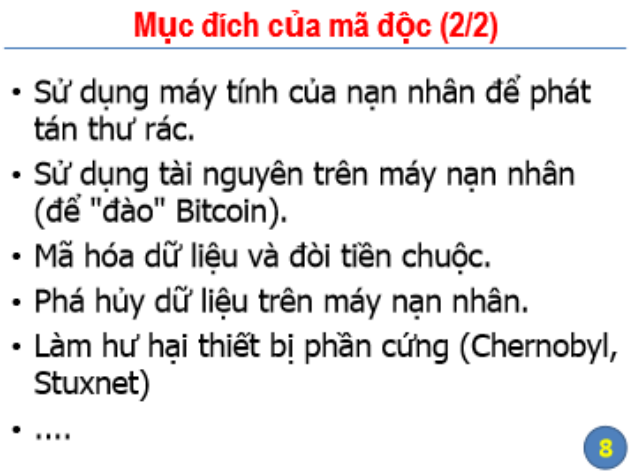
Point-to-Site (Remote Access) VPN

16. Hãy trình bày khái niệm và phân loại mã độc. Chỉ ra mục đích của người phát tán mã độc. Trình bày các con đường lây nhiễm mã độc. Trình bày các giải pháp phòng chống mã độc.

Mã độc *là* một khái niệm chung để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức. Thực hiện các hành vi chuộc lợi cá nhân, kinh tế, chính trị hoặc để thỏa mãn ý tưởng và sở thích của người viết.

Mục đích





Phân loại: tuỳ thuộc vào cơ chế, hình thức lây nhiễm và phương pháp phá hoại mà người ta phân mã độc thành nhiều loại khác nhau. Đặc điểm chung của mã độc là thực hiện các hành vi không hợp pháp nhưng không theo ý muốn của người sử dụng máy tính.

+ Mã độc cần có vật chủ: Logic bomb, Trojan, Backdoor, Exploit, Virus

+ Phần mềm độc lập: Worm, Zombie

+ Trong phần Viruses được chia ra làm 2 loại :

Vật chủ : boot sector, file thực thi, file văn bản

Kỹ thuật : đơn giản, đa hình, siêu đa hình, tàng hình

Con đường lây nhiễm mã độc:

- Cài đặt trực tiếp:

+Cho người khác mượn máy tính, điện thoại

+Rời máy tính, đthoai mà k khóa hệ thống

+ Máy bị nhiễm mã độc từ nhà sản xuất

- Phần mềm lậu, bẻ khóa

+Người bẻ khóa thường là thành viên của những nhóm hacker, cracker

+Phần mềm bẻ khóa thường bị nhúng mã độc để pvụ mục đích của tin tặc

+Khi sd những phần mềm như thé mã độc sẽ phát triển vào máy

- Qua thiết bị lưu trữ di động

+Khi cắm USB, thẻ nhớ,... vào máy bị nhiễm mã độc, chúng sẽ bị nhiễm

+Cắm USB, thẻ nhớ... đã bị nhiễm vào máy khác, mã độc có thể được kích hoạt và lây nhiễm vào máy đó

+Kích hoạt: tính năng autorun, hoạt động của người dùng

-Khai thác lỗi phần mềm

+Phần mềm: hệ điều hành, trình duyệt web, phần mềm chơi nhạc & video, game,…

+Nhiều phần mềm có lỗi

+Hacker tạo những đầu vào đặc biệt cho phần mềm trong đó có mã độc

+Khi phần mền xử lí đầu vào đặc biệt đó thì mã độc đc thực thi

Phương pháp phòng chống mã độc: phòng tránh và ngăn chặn mã độc không chỉ dựa vào các phần mềm diệt virus mà còn liên quan tới cả nhận thức của người dùng. Một số biện pháp phòng tránh mã độc:

+Luôn luôn cài đặt và sử dụng một phần mềm diệt virus chính hãng

+Xây dựng chính sách với các thiết bị PnP

+Đóng băng ổ đĩa

+Thiết lập quy tắc đối xử với các file:

+Truy cập web an toàn

+Cập nhật máy tính, phần mềm

+Nhờ chuyên gia can thiệp

17. Hãy trình bày về tấn công nghe lén trong mạng máy tính.

Đó là một kỹ thuật tấn công, thường được hacker dùng để dò tìm mật khẩu, đọc các thông tin trao đổi bằng các ứng dụng chat trên Internet.

18. Hãy trình bày về tấn công từ chối dịch vụ trong mạng máy tính.

Là tấn công nhằm phá vỡ tính khả dụng của thông tin, hệ thống thông tin

Phân loại

• Băng thông thấp

• Băng thông cao

–Đơn lẻ

–Phân tán

Băng thông thấp

• Ping of Death

• Teardrop

• +++

Băng thông cao (máy đơn)

• SYN flood

• Ping flood

• HTTP POST DoS

• +++

Các hình thức tấn công DoS:

SYN Floods: attacker liên tục gửi gói tin chứa cờ SYN cho target, và đến một lúc nào đó target sẽ k thể trả lời kịp những gói tin này dẫn tới tình trạng target bị crash hoặc treo.

Fin Floods: Tương tự như SYN floods nhưng attacker sẽ gửi các gói tin có chứa cờ FIN, đây là cờ kết thúc của một kết nối. Thực chất attacker ko thiết lập 1 kết nối nào do vậy victim sẽ drop gói tin này. Việc drop gói tin vẫn cần xử lý do vậy tốn 1 phần tài nguyên trên victim, Attacker gửi liên tục như vậy đồng thời gửi những gói tin có dung lượng lớn đến một lúc nào đó victim sẽ bị treo hoặc crash

Smurf: Là kiểu tấn công mà attacker sẽ giả mạo gói tin ICMP với địa chỉ nguồn là địa chỉ IP của victim và gửi tới địa chỉ broadcast của các mạng khác nhau, do vậy đồng loạt các máy trong mạng sẽ reply tới máy victim và làm máy victim bị treo

Fraggle: Tương tự như smurf nhưng gói tin ở đây là UDP

Ping of Death: Attacker gửi gói tin ICMP trong công cụ ping cho victim nhưng giả mạo địa chỉ nguồn chính là địa chỉ IP của victim do đó tạo thành một vòng lặp trong máy nạn nhân, đến khi máy nạn nhân bị treo

Teardrop: attacker gửi gói tin đã bị phân mảnh tới nạn nhận, nhưng máy nạn nhân k thể sắp xếp lại được thứ tự các gói tin và làm treo hệ thống, đây là một bug trong mạng TCP/IP

***Tấn công DDoS*:** đây là kiểu tấn công phân tán, attacker sẽ lợi dụng hàng loạt các máy tính bị điều khiển trong mạng botnet (thường là các máy tính bị dính malware) nghe lệnh attacker đồng thời tấn công một mục tiêu nào đó theo giờ đã lên lịch trước.

19. Hãy trình bày về tấn công kỹ nghệ xã hội trong mạng máy tính.

- Kỹ nghệ xã hội (social engineering)
  - là phương tiện thu thập thông tin cho một cuộc tấn công bằng cách dựa trên những điểm yếu của các cá nhân.
  - Không cần đến công nghệ
- Tấn công dùng kỹ nghệ xã hội có thể bao gồm
  - các phương pháp tâm lý
  - các phương pháp vật lý.

- Phương pháp tâm lý (psychology).
  - Tiếp cận về mặt tinh thần và cảm xúc hơn là về mặt vật chất.
  - Nhằm thuyết phục nạn nhân cung cấp thông tin hoặc thuyết phục họ hành động.
- Các phương pháp tâm lý thường được sử dụng
  - Thuyết phục (Persuasion)
  - Mạo danh (Impersonation)
  - Phishing (lừa đảo)
  - Thư rác (Spam)
  - Cảnh báo giả (Hoax)

- Những phương pháp thuyết phục cơ bản bao gồm
  - lấy lòng (tâng bốc hay giả vờ)
  - a dua (những người khác cũng đang làm vậy)
  - thân thiện
- Kẻ tấn công sẽ hỏi một vài thông tin nhỏ
  - Tập hợp thông tin từ vài nạn nhân khác nhau
- Đưa ra những yêu cầu đáng tin
- Kẻ tấn công có thể "tạo vỏ bọc" để có được thông tin
  - Trước khi nạn nhân bắt đầu cảm thấy nghi ngờ
- Kẻ tấn công có thể mỉm cười và yêu cầu sự giúp đỡ từ nạn nhân

- Mạo danh (impersonation)
  - tạo một nhân cách giả, rồi đóng vai đó đối với nạn nhân.
- Những vai phổ biến thường được mạo danh
  - Trợ lý hỗ trợ kỹ thuật
  - Công nhân sửa chữa
  - Bên thứ ba đáng tin cậy
  - Các cá nhân có quyền lực
    - nạn nhân có thể nói "không" với người có quyền lực.

Phishing (Lừa đảo)

- Gửi thư điện tử tự xưng là một nguồn hợp pháp
  - Thư điện tử có thể chứa logo và lý lẽ hợp pháp
- Cố gắng đánh lừa người dùng để họ cung cấp các thông tin riêng tư

Người dùng được yêu cầu

- trả lời e-mail
- cập nhật thông tin cá nhân trên một trang Web
  - Mật khẩu, mã số thẻ tín dụng, mã số chứng minh thư, số tài khoản ngân hàng, hoặc các thông tin khác.
  - Tuy nhiên, trang Web này chỉ là một địa chỉ mạo danh và được lập nên nhằm đánh cắp thông tin của người sử dụng.

- Những biến thể của Fishing
  - Pharming (nuôi cá)
    - Tự động chuyển hướng tới một website giả mạo
  - Spear phishing (xiên cá)
    - Gửi e-mail hoặc tin nhắn đến những người dùng xác định
  - Whaling (câu cá voi)
    - Nhắm vào những người giàu có
  - Vishing (lừa đảo bằng gọi điện thoại)
    - Kẻ tấn công gọi cho nạn nhân với nội dung tin nhắn từ phía "ngân hàng" và yêu cầu nạn nhân gọi lại vào một số điện thoại do hắn cung cấp
    - Nạn nhân sau đó gọi vào số điện thoại của kẻ tấn công và nhập các thông tin riêng tư

20. Thế nào là tấn công XSS? Phân loại tấn công XSS. Lấy ví dụ đoạn mã có lỗ hổng XSS; trình bày cơ chế khai thác lỗ hổng trong đoạn mã đó.

Lỗ hổng XSS(CROSS SITE SCRIPTING) *là* một lỗ hổng cho phép hacker chèn script vào tham số truy vấn HTTP và sau đó script này được thực thi trên máy người dùng.

* Phân loại : Stored XSS, Reflected XSS, DOM Based XSS…

Stored XSS: là dạng ấn công mà hacker chèn trực tiếp mã độc vào csdl của website. Dạng tấn công này xảy ra khi các dữ liệu được gửi lên server không được kiểm tra kỹ lưỡng mà lưu trực tiếp vào csdl. Khi người dùng truy cập vào trang web này thì những đoạn script độc sẽ được thực thi chung với quá trình load web.

Refkected XSS là dạng tấn công thường gặp nhất trong các loại XSS với. Reflected XSS, hacker không gửi dữ liệu động lại lên server nạn nhân, mà gửi trực tiếp link có chứa mã độc cho người dùng, khi người dùng click vào link này thì trang web sẽ được load chung vs đoạn script độc hại. Reflected XSS thường dùng để ăn cắp Cookie, Session..

Cơ chế tấn công XSS điển hình:

• Tạo URL chứa script và gửi cho nạn nhân

• Nạn nhân mở URL và script được thực thi

Ví dụ và giải thích:

Ta có một trang web mà người dùng có thể để lại những lời nhắn , bìn luận, Thay vì nhập vào lời nhắn bình thường, ta nhập vào đoạn mã sau:

Xin <script>alert(“XSS”)</script>chào!

Kết quả: xuất hiện 1 alert với nội dung *“XSS” với button OK.*

Vì các lời nhắn được lưu trữ trong database nên bất cứ người dùng nào khi truy cập vào trang web này sẽ thực thi đoạn mã trên. Thay vì một đoạn mã vô hại như trên, hacker có thể thay bằng các đoạn mã nguy hiểm khác nhằm gây hại đến người dùng.

21. Thế nào là tấn công SQL Injection? Phân loại tấn công SQL Injection. Lấy ví dụ đoạn mã có lỗ hổng SQL Injection; trình bày cơ chế khai thác lỗ hổng trong đoạn mã đó.

Lỗ hổng SQL Injection là lỗ hổng cho phép những kẻ tấn công lợi dụng lỗ hổng của việc ktra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị CSDL trả về để inject (tiêm vào) và thi hành các câu lệnh SQL một cách trái phép

Phân Loại :

Dựa trên kênh truy xuất dữ liệu

Inband or inline

Out-of-band

Dựa trên sự phàn hồi nhận được từ máy chủ

Error-based sql injections

Blind sql injection

Dựa trên dữ liệu đầu vào được xử lý(kiểu dữ liệu : string, number…)

Dựa thoe mức/ thứ tự bị inject

Dựa trên điểm bị inject

Cơ chế: Lợi dụng các truy vấn từ ứng dụng web tới CSDL (SQL) mà attacker có thể truyền vào các câu lệnh truy vấn của SQL bên trong dữ liệu đầu vào và khi webserver thực thi sẽ thực hiện đoạn truy vấn này với CSDL do đó attacker có thể chỉnh sửa dữ liệu (thêm, sửa, xoá, ...) hoặc bypass việc xác thực user

Ví dụ và giải thích: một đoạn PHP k-ểm tra login như sau

```
<?php
        $username = $_POST[‘user’]
        $passwd = $_POST[‘passwd’]
        $sql = “SELECT ID FROM users WHERE username=’ ” + $username +”’ AND password = ‘”+ $password + “‘””
        $result = mysqli_query ($sql)
if ($result) // Xác thực thành công
else // xác thực thất bại
?>
```

Khi ngdùng nhập username và password rồi gửi lên cho web server, web server sẽ kiểm tra trong cơ sở dữ liệu có bản ghi nào trùng với điều kiện username và password đó không. Nếu có sẽ xác thực thành công còn k xác thực thất bại.

Lợi dụng điều này mà attacker sẽ truyền vào nội dung để vượt qua xác thực như sau

Username: anyuser’ OR 1=1; --- comment

Password: anypassword

Câu truy vấn mà web server sẽ thực hiện là

SELECT ID FROM users WHERE username=’anyuser’ OR 1=1; --- comment AND password=anypassword

Ta thấy sau “--” là comment do vậy câu lệnh chỉ còn là

SELECT ID FROM users WHERE username=’anyuser’ OR 1=1;

Với câu lệnh này ta sẽ luôn trả về được tất cả các bản ghi bởi vì điều kiện 1 bằng 1 luôn đó

Do đó attacker sẽ vượt qua được việc xác thực.

22. Thế nào là lỗ hổng tràn bộ đệm? Phân loại lỗ hổng tràn bộ đệm. Lấy ví dụ đoạn mã có lỗ hổng tràn bộ đệm; trình bày cơ chế khai thác lỗ hổng trong đoạn mã đó.

Khái niệm : Lỗ hổng tràn bộ đệm là lỗ hổng cho phép dữ liệu xử lý thường là dữ liệu đầu vào, dài hơn giới hạn của vùng đệm được cấp phát để chứa nào

Phân loại :

Tràn bộ đệm trên Stack : biến cục bộ

Tràn bộ đệm trên Heap : cấp phát động

Ví dụ

Ta có ví dụ một chương trình C như sau

```
#include “stdio.h”
int main()
{
        int cookie;
        char buf[16];
        printf (“&buf: %p, &cookie: %p\n”, buf, &cookie);
        gets(buf);
        if (cookie == 0x41424344)
        {
                printf(“You Win”);
```

```
    }
}
```

Chương trình trên sẽ nhận một chuỗi từ bộ nhập chuẩn (stdin) từ hàm gets

Nếu biến cookie là 41424344 thì nó sẽ in ra dòng chữ ‘You Win’. Giả sử cookie đóng vai trò là dữ liệu quan trọng. Và mục đích của ta là in ra được dòng chữ này. Để làm được ta phải gán biến cookie bằng giá trị 41424344

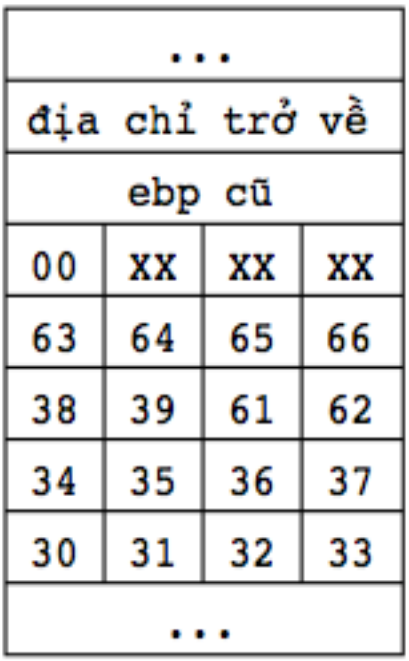
Ta thấy hàm gets không kiểm tra kích thước vùng nhớ dùng để chứa dữ liệu nhập cho nên sẽ xảy ra tràn bộ đẹp nếu như nhập dữ liệu dài hơn kích thước của bộ đệm.

Vì biến cookie được khai báo trước do vậy biến cookie nằm ở địa chỉ cao hơn biến buf, và do đó nằm sau buf trong bộ nhớ.

Nếu ta nhập 6 kí tự “abcdef” thì trạng thái bộ nhớ sẽ như sau

<table>
<tr><td colspan="4">...</td></tr>
<tr><td colspan="4">địa chỉ trở về</td></tr>
<tr><td colspan="4">ebp cũ</td></tr>
<tr><td colspan="4">cookie</td></tr>
<tr><td>XX</td><td>XX</td><td>XX</td><td>XX</td></tr>
<tr><td>XX</td><td>XX</td><td>XX</td><td>XX</td></tr>
<tr><td>65</td><td>66</td><td>00</td><td>XX</td></tr>
<tr><td>61</td><td>62</td><td>63</td><td>64</td></tr>
<tr><td colspan="4">...</td></tr>
</table>

Nếu ta nhập 16 kí tự “0123456789abcdef” thì trạng thái bộ nhớ sẽ như sau



ở đây biến cookie đã bị ghi đè, để biến Cookie có giá trị 41424344 thì các ô nhớ của biến cookie phải có giá trị lần lượt là 44,43, 42, 41 theo như quy ước kết thúc nhỏ của bộ xử lý intel x86. Đối chiếu với bảng mã ASCII thì đây là các kí tự ABCD

Sau khi ta nhập đoạn dữ liệu sau gồm 16 chữ a và theo sau là DCBA thì ta sẽ được dòng chữ You Win

aaaaaaaaaaaaaaaaDCBA

Khái niệm “quản lý an toàn thông tin”. Tại sao cần có tiêu chuẩn về quản lý an toàn thông tin? Giải thích chu trình PDCA theo tiêu chuẩn ISO 27001.

23. Quản lý an toàn thông tin là tác động lên hệ thống thông tin nhằm đưa hệ thống đó về trạng thái được đảm bảo tính bí mật, tính toàn vẹn và tính khả dụng.

Tại sao cần có tiêu chuẩn về quản lý an toàn thông tin

Trong quá trình quản lý an toàn thông tin chúng ta sẽ gặp phải những câu hỏi như:

Cần những biện pháp tác động nào

Tác động như thế nào

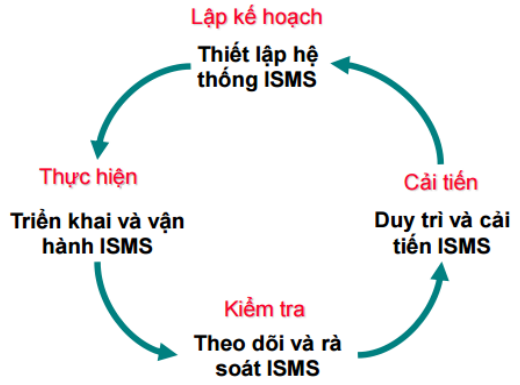
Bao nhiêu là đủ

Kiểm chứng kết quả ra sao

....

Để giải quyết những vấn đề này một cách hiệu quả nhất chúng ta cần áp dụng các tiêu chuẩn về quản lý an toàn thông tin

Chu trình PDCA theo tiêu chuẩn iso 27001



Mô hình gồm có 4 bước

B1: Lập kế hoạch

Thiết lập ISMS

Xác định phạm vi của ISMS

Đề ra một chính sách ISMS

Xác định một phương pháp đánh giá rủi ro của tổ chức

Nhận diện các rủi ro

Phân tích và đánh giá các rủi ro

B2: Thực hiện

Triển khai và vận hành ISMS

Thiết lập kế hoạch xử lý rủi ro

Thực hiện kế hoạch xử lý rủi ro

Thực hiện các công cụ kiểm soát được chọn để đáp ứng các mục tiêu kiểm soát

Quy định cách đo lường sự hiệu quả của các công cụ kiểm soát được chọn

…

B3 : Theo dõi và rà sát

Theo dõi và rà soát ISMS

Thực hiện các thủ tục theo dõi, soát xét và các công cụ kiểm soát khác

Rà soát định kỳ hiệu quả của ISMS

Đo lường hiệu quả của các công cụ kiểm soát

Xem xét định kỳ các đánh giá rủi ro

Định kỳ đánh giá nội bộ ISMS

…

B4 : Cải tiến

Duy trì và cải tiến ISMS

Thực hiện các cải tiến đã được xác định

Thực hiện các hành động khắc phục và phòng ngừa thích hợp

Thông tin về các hoạt động và cải tiến với tất cả các bên liên quan

Bảo đảm các cải tiến đạt được mục tiêu đề ra

Tiếp tục vòng lặp cho đến khi hệ thống thông tin được quản lý 1 cách an toàn.

24. Hãy giải thích vai trò của pháp luật trong an toàn thông tin. Hãy chỉ ra các tội danh trong lĩnh vực Công nghệ thông tin được quy định trong Bộ luật hình sự 2015 và cho biết khung hình phạt cao nhất đối với từng tội danh.

Vai trò của pháp luật trong an toàn thông tin :

Vai trò của bên tấn công quá lớn?

Nhà cung cấp vì lợi nhuận mà sử dụng sản phẩm, công nghệ không đảm bảo an toàn

Những hiểm họa mà không thể loại trừ bằng biện pháp kỹ thuật

Tổ chức , cá nhân coi nhẹ việc bảo vệ hệ thống thông tin

Xây dựng hành lang pháp lý để bảo vệ quyền, lợi ích hợp pháp của cá nhân , tổ chức, xã hội và nhà nước trong lĩnh vực thông tin

Các tội danh trong lĩnh vực công nghệ thông tin được quy định trong bộ luật hình sự 2015

Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật

Khởi điểm: ... để sử dụng trái pháp luật

Phạt tiền: 20 tr – 1 tỉ

Phạt tù: đến 7 năm

Bổ sung: phạt tiền, cấm hành nghề

Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử

Khởi điểm: thu lợi bất chính hoặc gây hại 50 tr, lây nhiễm 50 máy

Phạt tiền: 50 tr – 500 tr

Phạt tù: đến 12 năm

Bổ sung: phạt tiền, cấm hành nghề

Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử

Phạt tiền : từ 20tr – 25tr

Phạt tù : từ 5 năm đến 20 năm

Bổ sung : cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 1 đến 5 năm

Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông

Khởi điểm: phạm tội có tổ chức, thu lợi bất chính từ 5 tr ...

Phạt tiền : 20tr – 200tr

Phạt tù : 2 năm – 7 năm

Bổ sung: cấm đảm nhiệm chức vụ, cấm hành nghề

Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác

Khởi điểm : thu lợi bất chính trên 500tr , xâm nhập vào cơ sở hạ tầng thông tin quốc gia, hệ thống thông tin phục vụ quốc phòng an ninh

Phạt tiền : 300tr- 1 tỉ

Phạt tù : 7 năm – 12 năm

Bổ sung: cấm đảm nhận chức vụ, cấm hành nghề

Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản

Khởi điểm: chiếm đoạt tài sản từ 5tr trở lên, gây hậu quả nghiêm trọng

Phạt tiền 20tr – 100 tr

Phạt tù : 20 năm

Bổ sung : tịch thu 1 phần hoặc toàn bộ tài sản, cấm đảm nhiệm chức vụ...

Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng

Khởi điểm : thu lợi bất chình từ 200tr , công khai 200 tài khoản trở lên

Phạt tiền:200tr – 500 tr

Phạt tù : 2 năm – 7 năm

Bổ sung: cấm đảm nhiệm chức vụ, cấm hành nghề

Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông

Khởi điểm : thu lợi bất chính từ 500tr trở lên

Phạt tiền: 1tỉ - 1tỉ 500tr

Phạt tù : 2 năm – 5 năm

Bổ sung: cấm đảm nhiệm chức vụ, hành nghề, tịch thu tài sản

25. Hãy cho biết tại sao cần xem xét vấn đề đạo đức trong an toàn thông tin. Hãy nêu ra một số vấn đề đạo đức mà người làm an toàn thông tin có thể gặp phải.

Tại sao cần xem xét vấn đề đạo đức trong attt

Đạo đức phải là công cụ để giải quyết vấn đề trong những trường hợp mà luật pháp không thể phát huy tác dụng. đạo đức trong ATTT là sự bổ sung, phối hợp và không mâu thuẫn với các quy định có tính pháp lí. Vấn đề này hướng tới mục tiêu hướng dẫn các tổ chức, cá nhân hành nghề cung cấp dịch vụ an toàn thông tin a một cách chính trực, trọng danh dự và tin cậy. Các chương trình đào tạo về CNTT, bao gồm đào tạo chuyên gia ATTT, thường tập trung vào kiến thức và kỹ năng kỹ thuật. Người học được truyền thụ kiến thức, kỹ năng để thực hiện công việc, nhưng lại ít được cảnh báo về khả năng, về kịch bản các kiến thức, kỹ năng đó bị lạm dụng. Trên thực tế, nhiều người làm CNTT hành động với suy nghĩ của một hacker (mũ đen): tất cả những gì có thể làm đều là những thứ được phép làm. Và nhiều người thậm chí không nhận thấy sự tồn tại vấn đề đạo đức trong công việc của họ.

Đó là những vấn đề đạo đức nào?

1. Giúp đỡ những người có tinh thần học hỏi

Người làm ATTT không được phép từ chối chia sẻ với người khác những kiến thức trong lĩnh vực CNTT và bảo vệ thông tin. Những kiến thức này phải được truyền đạt một cách không vụ lợi cho tất cả những ai có mong muốn học hỏi.

2. Tránh những điều có hại

Trong công việc của mình, người làm ATTT cần phải tránh việc gây hại cho đối tượng được bảo vệ (thiệt hại từ tác dụng phụ), trừ trường hợp việc gây hại là cần thiết để ngăn chặn một thiệt hại lớn hơn. Cần tránh gây hại cho những bên không liên quan, cho dù việc gây hại đó giúp tránh được thiệt hại cho đối tượng được bảo vệ.

3. Không phát tán những thông tin nguy hiểm

Người làm ATTT không được cung cấp cho bất kỳ ai thông tin về các điểm yếu mà có thể bị khai thác (ngoại trừ việc cung cấp thông tin cho chủ sở hữu hoặc nhà phát triển hệ thống chứa điểm yếu nhằm mục đích loại trừ điểm yếu đó). Không được cung cấp cho bất kỳ ai những chương trình độc hại hoặc chương trình đa mục đích, nếu như có căn cứ để cho rằng người được cung cấp sẽ sử dụng chương trình một cách ác ý.

4. Sử dụng có chừng mực

Khi có được quyền truy cập tới hệ thống hoặc thông tin về hệ thống, người làm ATTT chỉ được sử dụng quyền truy cập/thông tin đó để thực hiện việc bảo vệ, ngăn chặn các mối nguy hại và tăng cường mức an toàn, mà không được sử dụng quyền truy cập/thông tin đó cho bất kỳ mục đích nào khác, kể cả mục đích vô hại. Khi thực hiện xong nhiệm vụ, quyền truy cập cần được đóng lại, còn thông tin thì cần phải được xóa bỏ.

5. Giữ bí mật

Người làm ATTT cần phải giữ bí mật mọi thông tin được tiếp cận trong quá trình cung cấp dịch vụ bảo vệ, nếu thông tin đó là bí mật thương mại, bí mật đời tư, bí mật nghề nghiệp hay bất kỳ dạng thông tin mật nào khác, dù cho có hay không có thỏa thuận về việc giữ bí mật các thông tin.

Những quy tắc đạo đức trên đây không chỉ là nỗ lực ban đầu trong việc văn bản hóa chuẩn mực đạo đức nghề nghiệp cho những người làm trong lĩnh vực bảo vệ thông tin, mà chúng cần được quy định chính thức cho các tổ chức ứng cứu sự cố máy tính, giám sát an toàn mạng, cung cấp dịch vụ ATTT. Đó là một trong những yếu tố đảm bảo rằng thành viên của đội sẽ thực hiện chức năng của mình một cách vô tư, công bằng.

Trong số những vấn đề đạo đức mà người làm ATTT phải đối mặt trước hết phải kể đến các vấn đề liên quan đến tính riêng tư. Ví dụ:

Nếu bạn có khả năng đọc được email cá nhân của các người dùng khác trong mạng thì bạn có đọc chúng không?

Liệu có ổn không, nếu bạn đọc email của nhân viên để đảm bảo rằng thông tin nhạy cảm của công ty không bị tiết lộ? Liệu có ổn không nếu bạn đọc đọc email của nhân viên để đảm bảo rằng nhân viên không vi phạm các quy định của công ty (ví dụ, quy định không được phép sử dụng hệ thống email của công ty vào mục đích cá nhân). Và nếu bạn quyết định đọc email của nhân viên thì bạn có thông báo cho họ biết hay không? Nếu có thì thông báo trước hay sau khi đọc chúng?

Liệu có cần phải giám sát tất cả hành động truy cập web của người dùng trong mạng hay không? Có cần ghi vào log tất cả những website mà người dùng truy cập không? Việc không giám sát các truy cập như thế có phải là một sự tắc trách không, khi mà bạn biết rằng việc giám sát có thể giúp ngăn ngừa

ai đó truy cập nội dung khiêu dâm trong giờ làm việc nhưng đồng thời cũng tạo ra một môi trường làm việc kém thân thiện?

Liệu có ổn không nếu cài đặt key logger trên các máy tính trong mạng để ghi lại tất cả thao tác gõ bàn phím của người dùng? Câu trả lời có khác không nếu đối tượng được cài đặt là phần mềm chụp ảnh màn hình, cho phép người quản lý theo dõi tất cả những gì hiện trên màn hình người dùng? Và nếu bạn quyết định giám sát người dùng bằng một trong hai hình thức trên thì bạn có thông báo trước cho người dùng hay không?

Liệu có ổn không nếu bạn đọc các file tài liệu hoặc xem các file hình ảnh mà người dùng lưu trên máy của họ hoặc trong thư mục của họ trên file server?