TRƯỜNG ĐẠI HỌC KỸ THUẬT – CÔNG NGHỆ CẦN THƠ

AN TOÀN CÁC HỆ THỐNG THÔNG TIN

ThS. Nguyễn Văn Kha

dzokha1010@gmail.com

MỤC TIÊU HỌC TẬP

Kiến thức

- Định nghĩa về khái niệm liên quan đến an ninh HTTT.
- Nhận thức và phân biệt được các mối đe doạ đến an ninh HTTT.
- Phân tích, phát hiện và khắc phục các lỗ hổng bảo mật cơ bản.
- Hiểu về chữ ký số, chứng thực số và các cách xác thực bảo mật.
- Hiểu và ứng dụng xây dựng một HTTT an toàn và hiệu quả.

MỤC TIÊU HỌC TẬP

Kỹ năng

- Trình bày được nguyên lý để thiết lập một hệ thống an toàn.
- Xác định được các nguy cơ, lỗ hổng trong an ninh thông tin.
- Có khả năng đánh giá độ tin cậy, lỗ hổng bảo mật, xây dựng các chính sách bảo mật đề ra các giải pháp an toàn HTTT.

Tư tưởng

- Có tinh thần hợp tác tốt, thái độ nghiêm túc trong học tập, nghiên cứu, làm việc nhóm, tích cực tham gia cá hoạt động trên lớp, thảo luận nhóm.

ĐÁNH GIÁ KẾT THÚC MÔN

Hình thức		Chuẩn đầu ra	Thời điểm	Trọng số
Đánh giá quá trình	Chuyên cần và tham gia các hoạt động trên lớp	Có mặt đầy đủ, nghiêm túc, tích cực thảo luận	Mỗi buổi học	10 %
	Báo cáo nhóm	K3.1, K3.2, K3.4, K6.1, S3.1, S3.2, C1.1	Sau kết thúc chương 5	10 %
	Kiểm tra giữa kỳ	K3.1, K3.2, K3.4, S5.1	Kết thúc Chương 3	20 %
Thi cuối kỳ		K3.1, K3.2, K3.3, K3.4, K6.1, S3.1, S3.2, S5.1	Cuối kỳ	60 %

TÀI LIỆU THAM KHẢO

- Nguyễn Khanh Văn (2019), Giáo trình Cơ sở an toàn thông tin, NXB Bách khoa Hà Nội, Hà Nội.
- Lê Văn Phùng (2018), An toàn thông tin, NXB Thông tin và Truyền thông, Hà Nội.

Chương 1
TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1. Các khái niệm cơ bản

1.2. Các mối đe doạ đến an ninh HTTT

1.3. Phương pháp tiếp cận và các vai trò trong an ninh thông tin

1.3. Quản lý an ninh thông tin

1.4. Các thành phần trong một HTTT.

1.1 Các khái niệm cơ bản
1.1.1. Security

“Bảo mật” thường được dịch từ tiếng Anh “Security”.

“Cybersecurity" được dịch là "an ninh mạng"

"Information Safety" dịch là "an toàn thông tin"

Thống nhất sử dụng thuật ngữ trong bài giảng này là “**an ninh**” thay cho “bảo mật” và “an toàn” khi dịch từ “**Security**”.

1.1 Các khái niệm cơ bản
1.1.1. Security

An ninh (Security) là sự bảo vệ. Mục tiêu chính của an ninh là bảo vệ khỏi kẻ thù, những kẻ muốn gây hại, dù cố ý hay vô tình.

- Ví dụ, an ninh quốc gia là một hệ thống nhiều tầng bảo vệ chủ quyền, người dân, tài nguyên và lãnh thổ của quốc gia.
- Tương tự, an ninh một tổ chức phải có nhiều tầng bảo mật để bảo vệ con người, hoạt động, cơ sở hạ tầng vật lý, chức năng, thông tin liên lạc và thông tin của mình.

1.1 Các khái niệm cơ bản
1.1.2. Information

Thông tin (Information) là dữ liệu đã được đưa vào một bối cảnh/ngữ cảnh có ý nghĩa và hữu ích.

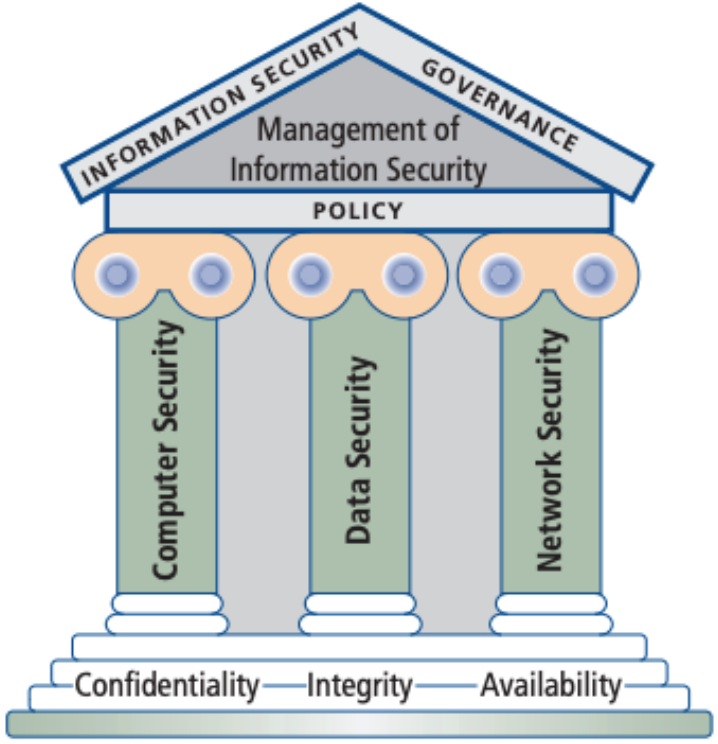
Thông tin là dữ liệu đã được xử lý thành một dạng có ý nghĩa đối với người nhận và có giá trị thực tế hoặc được nhận thức trong việc ra quyết định hiện tại hoặc tương lai.

- Ví dụ, dữ liệu liên quan đến doanh số bán hàng của nhiều nhân viên bán hàng, có thể được kết hợp để cung cấp thông tin liên quan đến tổng doanh số bán hàng.

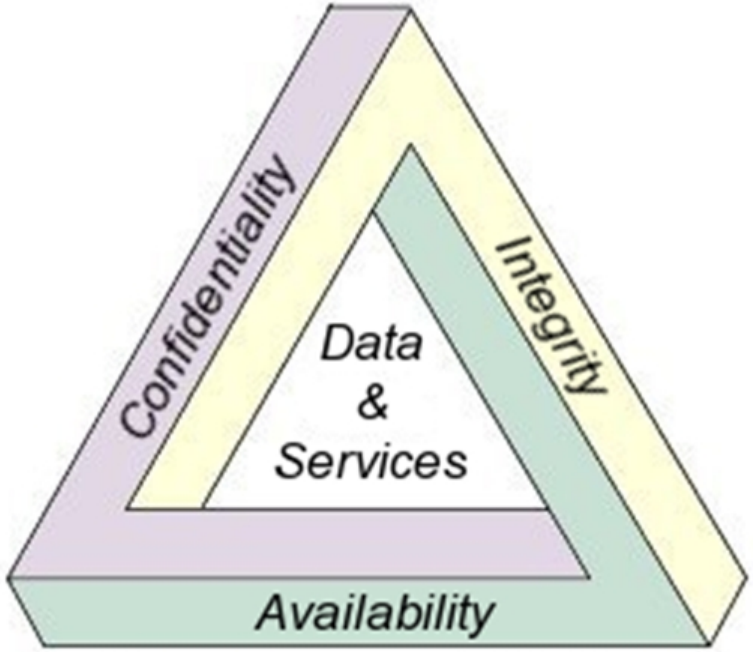
1.1 Các khái niệm cơ bản
1.1.3. Information Security

- An ninh thông tin (Information Security) là bảo vệ thông tin và các thành phần quan trọng của thông tin, bao gồm các hệ thống và phần cứng sử dụng, lưu trữ và truyền thông tin.

- An ninh thông tin bao gồm các lĩnh vực rộng lớn về quản lý an ninh máy tinh, an ninh dữ liệu và an ninh mạng.



1.1 Các khái niệm cơ bản
1.1.4. Bộ ba C.I.A và các đặt tính của thông tin



- **Tính bảo mật (Confidentiality)**
- **Tính toàn vẹn (Integrity)**
- **Tính khả dụng (Availability)**
- Độ chính xác (Accuracy)
- Xác thực (Authenticity)
- Hữu ích (Utility)
- Quyền sở hữu (Possession)

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
a) Cybersecurity

An ninh mạng (Cybersecurity) là hành động bảo vệ hệ thống, mạng và chương trình từ tấn công kỹ thuật số. An ninh mạng bảo vệ con người, xã hội, tổ chức và quốc gia khỏi các rủi ro trên không gian mạng.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
b) Cyberspace

Không gian mạng (Cyberspace) có thể được coi là các dịch vụ cơ sở hạ tầng của Internet cung cấp thông tin cho người dùng thông qua hệ thống thiết bị và phần mềm của nó.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
c) Cyberattack

Tấn công mạng (Cyberattack) là cố ý khai thác không gian mạng, khai thác trái phép thông tin và hệ thống thông tin.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
d) Hacker

- White Hat: còn được gọi là Hacker đạo đức hoặc một chuyên gia bảo mật máy tính.
- Black Hat: hay còn gọi là Cracker, được định nghĩa là những kẻ chuyên đột nhập vào máy tính của người khác một cách bất hợp pháp
- Gray Hat: xâm nhập vào hệ thống máy tính với mục đích duy nhất là thông báo cho quản trị viên, sau đó đề nghị sửa lỗi với một khoản phí
- Blue Hat: người được công ty thuê để tìm lỗi và lỗ hổng hoặc nguy cơ bị tấn công trong các sản phẩm công nghệ trước khi chúng được phát hành.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
e) Cracker

- Người mới học nghề (Novice): bẻ khóa để tinh nghịch và vui chơi
- Sinh viên (Student): quan tâm sâu sắc đến máy tính và lập trình
- Người thích khám phá (Tourist): xâm nhập hệ thống chỉ để thử thách và sau đó đăng xuất
- Kẻ háo danh (Crasher): đưa các hệ thống dừng hoạt động, để lại biệt danh tạo dấu ấn với các nạn nhân
- Tên trộm (Thief): là tội phạm thực sự, thường đột nhập vào hệ thống máy tính để thu lợi.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
f) Payload

Tải trọng (Payload) là phần dữ liệu được truyền tải, không bao gồm tiêu đề ‘Header’ và siêu dữ liệu ‘Metadata’. Payload thường là văn bản, âm thanh, mã thực thi độc hại được thiết kế. Tiêu đề và siêu dữ liệu chỉ truyền tải kèm theo để hỗ trợ cho việc phân phối Payload.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware

- Phần mềm độc hại (Malware - Malicious Software) được định nghĩa là bất kỳ mã nào được thêm vào hoặc thay đổi hoặc xóa khỏi hệ thống phần mềm nhằm cố ý gây hại hoặc phá hủy chức năng của hệ thống, là phần mềm được thiết kế với mục đích xấu chứa các tính năng hoặc có khả năng gây hại trực tiếp hoặc gián tiếp cho người dùng hoặc hệ thống máy tính người dùng.
- Malware được phân loại dựa trên cách thức hoạt động của nó. Bao gồm: Virus, Worm, Trojan Hourse, Spyware, Adware, RootKit, Ransomware, Logic/Time Bomb, Bot/Botnet.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

Virus máy tính là một chương trình máy tính sửa đổi các chương trình và ứng dụng khác, bao gồm cả bản sao của chính nó. Tức là, nó biểu hiện ký sinh trên các phần mềm và ứng dụng khác, nó tồn tại dưới dạng thực thi và lây nhiễm bằng cách ký sinh trên các tập tin văn bản, tập tin đa phương tiện hoặc gói tin mạng.

- Virus đơn giản
- Virus được mã hóa
- Virus đa hình
- Virus biến hình

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

Sâu máy tính (Worm) là phần mềm độc hại tự sao chép và vận hành, có thể lan truyền trên mạng bằng cách khai thác lỗ hổng trong các hệ thống khác nhau, có thể là lỗ hổng trong hệ điều hành hoặc phần mềm được cài đặt. Nó chứa đựng những thói quen có hại nhưng có thể được sử dụng để mở các kênh truyền thông hoạt động như những người vận chuyển tích cực.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

- **Trojan Horse** được biết đến với cái tên Trojan, là phần mềm độc hại thường được ngụy trang thành phần mềm hợp pháp. Trojan không thể tự sao chép, không giống như Virus và Worm. Tội phạm mạng sử dụng Trojan để cố gắng truy cập vào hệ thống của người dùng. Người dùng thường bị lừa bởi các kỹ thuật xã hội trong việc tải xuống và thực thi trên hệ thống của họ.
- Ngoài Trojan là phần mềm được tải xuống và cài đặt trên máy tính của người dùng, còn có một loại Trojan phần cứng được gọi là mã độc phần cứng (Hardware Trojan - HT). Trojan phần cứng được định nghĩa là sự sửa đổi có chủ đích, độc hại đối với thiết kế mạch dẫn đến hành vi không mong muốn khi mạch được triển khai.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

Phần mềm gián điệp (Spyware) là một loại phần mềm độc hại lây nhiễm vào máy tính hoặc thiết bị di động và thu thập thông tin về người dùng, bao gồm các Website đã truy cập, những thứ tải xuống, tài khoản và mật khẩu, thông tin thanh toán và Email người dùng được gửi và nhận. Spyware hoạt động lặng lẽ trong nền, duy trì sự hiện diện bí mật, thu thập thông tin hoặc giám sát các hoạt động của người dùng để kích hoạt các hoạt động độc hại liên quan đến máy tính và cách người dùng sử dụng nó

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

Adware (Advertising Supported Software) là phần mềm quảng cáo, tự động phát, hiển thị hoặc tải xuống (thường là không mong muốn) quảng cáo khi người dùng trực tuyến duyệt qua các Website hoặc ứng dụng được cài đặt trên máy tính và thiết bị di động. Hầu hết Adware được thiết kế để phục vụ như các công cụ tạo doanh thu cho các nhà quảng cáo. Một số Adware có thể được đóng gói với Spyware, điều này rất nguy hiểm vì nó có thể theo dõi hoạt động của người dùng và đánh cắp thông tin người dùng

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

RootKit là một phần mềm máy tính bí mật được thiết kế để cung cấp quyền truy cập đặc quyền liên tục vào máy tính trong khi chủ động che giấu sự hiện diện của nó. Những công cụ này là các phần mềm rất tiên tiến và phức tạp được viết để ẩn trong các quy trình hợp pháp trên một máy tính bị nhiễm và thâm nhập sâu vào hệ thống rất khó để gỡ bỏ. Chúng được thiết kế với khả năng kiểm soát hoàn toàn hệ thống và giành được các đặc quyền cao nhất có thể trên máy bị thâm nhập.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

Ransomware là một dạng mã độc hoặc phần mềm độc hại lây nhiễm vào máy tính và lây lan nhanh chóng để mã hóa dữ liệu hoặc khóa máy tính. Phần mềm độc hại này làm cho dữ liệu không thể truy cập được đối với người dùng và những kẻ tấn công yêu cầu thanh toán từ người dùng để các tập tin của họ được giải mã và có thể truy cập được. Việc thanh toán thường được yêu cầu bằng tiền kỹ thuật số (Bitcoin) hoặc các loại tiền tệ khác.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

- **Bom Logic (Logic Bomb)** là một phần mềm độc hại được kích hoạt khi đáp ứng điều kiện Logic, chẳng hạn như sau khi một số giao dịch được xử lý sẽ được kích hoạt hoặc được kích hoạt vào một ngày cụ thể. Phần mềm độc hại như Worm thường chứa Bom Logic, hoạt.
- **Bom hẹn giờ (Time Bomb)** là một loại Bom Logic sử dụng ngày và giờ làm điều kiện kích hoạt. Bom hẹn giờ trong hệ thống thông tin tương tự như là quả bom hẹn giờ vật lý, Bom hẹn giờ được kích hoạt nó sẻ phát nổ ngay sau đó, dẫn đến một số hiệu ứng gây thiệt hại như là từ chối dịch vụ, làm hư hỏng và rò rỉ thông tin.

1.1 Các khái niệm cơ bản
1.1.5. Các khái niệm liên quan khác
g) Malware (tt)

- **Bot** là phần mềm được thiết kế để thực hiện các hành động cụ thể. Một số Bot được sử dụng cho các mục đích hợp pháp như lập trình Video và lập trình các chức năng tương tác phục vụ cộng đồng trực tuyến. Các Bot độc hại được thiết kế để tạo thành Botnet.
- **Botnet** được định nghĩa là một mạng gồm các máy tính (Zombie/Bot) được điều khiển bởi kẻ tấn công hoặc Botmaster. Bot lây nhiễm và điều khiển máy tính được kết nối khác, do đó hình thành một mạng lưới các máy tính bị thâm nhập có tên là Botnet.

1.2. Các mối đe doạ đến an ninh HTTT

1.2.1. Tấn công bằng Malware

1.2.2. Tống tiền thông tin

1.2.3. Gián điệp hoặc xâm nhập

1.2.4. Lỗi hoặc sai sót do con người

1.2.5. Lỗi hoặc sự cố phần cứng

1.2.6. Lỗi hoặc sự cố phần mềm

1.2.7. Sự lỗi thời của công nghệ

1.2.8. Sai lệch về chất lượng dịch vụ

1.2.9. Tấn công phá huỷ/phá hoại

1.2.10. Trộm

1.2.11. Sự xâm phạm đến SHTT

1.2.12. Sức mạnh của thiên nhiên

1.2. Các mối đe doạ đến an ninh HTTT
1.2.1. Tấn công bằng phần mềm độc hại

Tấn công bằng phần mềm độc hại là một loại tấn công mạng trong đó phần mềm độc hại được cài đặt vào máy tính của người dùng mà không có bất kỳ sự đồng ý nào của người dùng.

- Backdoor,
- Drive-by Download,
- Buffer Overflow,
- DoS/DDoS

1.2. Các mối đe doạ đến an ninh HTTT
1.2.2. Tống tiền thông tin

- Tống tiền thông tin, còn được gọi là tống tiền qua mạng, là hành vi phổ biến trong việc đánh cắp số thẻ tín dụng.
- Ví dụ: đánh cắp hàng trăm nghìn số thẻ tín dụng; đột nhập vào hệ thống của công ty và thay đổi mật khẩu cùng mã truy cập; phần mềm tống tiền WannaCry

1.2. Các mối đe doạ đến an ninh HTTT
1.2.3. Gián điệp hoặc xâm nhập

- Gián điệp hoặc xâm nhập là các hoạt động, bao gồm cả điện tử và con người, có thể vi phạm tính bảo mật của thông tin. Khi ai đó không được phép truy cập vào thông tin mà tổ chức đang cố gắng bảo vệ, hành vi đó được coi là gián điệp hoặc xâm nhập.
- Sau khi kẻ tấn công truy cập vào hệ thống, bước tiếp theo là tăng cường quyền hạn (leo thang đặc quyền). Thay vì chỉ có quyền sử dụng cơ bản, kẻ tấn công cần có quyền quản trị hoặc quyền "gốc". Những đặc quyền này cho phép truy cập, sửa đổi hệ thống, xem mọi thông tin, và ẩn dấu vết bằng cách thay đổi nhật ký hệ thống.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.3. Gián điệp hoặc xâm nhập (tt)

Tấn công mật khẩu thuộc loại gián điệp hoặc xâm nhập, tấn công mật khẩu là khi kẻ tấn công cố gắng đoán hoặc bẻ khóa mật khẩu để truy cập vào hệ thống. Có một số phương pháp để thực hiện việc này:

- Tấn công bằng vũ lực (Brute Force Attack)
- Tấn công từ điển (Dictionary Attack)
- Tấn công bằng bảng cầu vồng (Rainbow Table Attack)
- Kỹ nghệ xã hội (Social Engineering Attack)

1.2. Các mối đe doạ đến an ninh HTTT
1.2.4. Lỗi hoặc sai sót do con người

Các hành vi xảy ra mà không có chủ ý xấu hoặc mục đích xấu hoặc do người dùng được ủy quyền vô tình. Khi mọi người sử dụng thông tin, hệ thống thông tin, lỗi có thể xảy ra. Các lỗi tương tự cũng xảy ra khi mọi người không tuân theo các chính sách đã được thiết lập. Thiếu kinh nghiệm, đào tạo không đầy đủ, và giả định không chính xác là một số nguyên nhân có thể dẫn đến lỗi hoặc sai sót do con người.

Ví dụ: Vào năm 2017, một nhân viên gỡ lỗi sự cố với hệ thống thanh toán của Amazon Web Services (AWS) đã khiến nhiều máy chủ ngừng hoạt động hơn mức dự kiến, khiến một số trang Web lớn bị sập.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.4. Lỗi hoặc sai sót do con người (tt)

Kỹ nghệ xã hội (kỹ nghệ xã hội) mô tả kiểu tấn công sử dụng các hình thức thao túng hành vi của con người thay vì tập trung khai thác các lỗ hổng bảo mật của máy móc, thiết bị. Qua đó, kẻ tấn công có thể đạt được các mục đích của mình như xâm nhập vào hệ thống, truy cập thông tin quan trọng,… mà không cần phải thực hiện những kỹ thuật tấn công quá phức tạp.

- Thoả hiệp Email doanh nghiệp
- Gian lận phí ứng trước
- Lừa đảo (Phishing)

1.2. Các mối đe doạ đến an ninh HTTT
1.2.5. Lỗi hoặc sự cố phần cứng

Lỗi hoặc sự cố phần cứng xảy ra khi nhà sản xuất cung cấp thiết bị có lỗi, dù đã biết hoặc chưa biết. Những lỗi này có thể khiến hệ thống hoạt động không như mong đợi, dẫn đến dịch vụ không đáng tin cậy hoặc thiếu tính khả dụng.

- Ví dụ: Lỗi chia dấu phẩy động (FDIV) trên chip Pentium đã gây ra một cuộc khủng hoảng về hình ảnh cho Intel, buộc họ phải thu hồi chip và chịu thiệt hại hơn 475 triệu đô la.
- Phần cứng máy tính thường xuyên bị lỗi nhất là ổ cứng, hiện có thời gian trung bình giữa các lần lỗi (MTBF) khoảng 500.000 giờ

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm

Một lượng lớn mã máy tính được viết, gỡ lỗi, xuất bản và bán trước khi tất cả lỗi của chúng được phát hiện và khắc phục. Đôi khi, sự kết hợp của một số phần mềm và phần cứng nhất định sẽ tiết lộ những lỗi mới, hoặc tình huống chưa được kiểm tra. Đôi khi những lỗi này không phải là lỗi mà là các lối tắt cố ý do lập trình viên để lại vì lý do lành tính hoặc ác tính. Nhìn chung, những lối tắt này, gọi là "cửa bẩy" có thể bỏ qua kiểm tra bảo mật và chúng có thể gây ra các vi phạm an ninh nghiêm trọng.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm (tt)

OWASP Top 10 đề xuất 10 lỗ hổng Website nghiêm trọng năm 2017

1) Injection
2) Broken Authentication
3) Sensitive Data Exposure
4) XML External Entities (XXE)
5) Broken Access Control
6) Security Misconfiguration
7) Cross-Site Scripting (XSS)
8) Insecure Deserialization
9) Using Components with Known Vulnerabilities
10) Insufficient Logging & Monitoring

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(1) Injection

Các lỗi Injection như SQL Injection, NoSQL Injection, OS command Injection và LDAP Injection xảy ra khi dữ liệu không đáng tin cậy được gửi đến trình thông dịch như một phần của lệnh hoặc truy vấn. Dữ liệu của kẻ tấn công có thể đánh lừa trình thông dịch thực hiện các lệnh ngoài ý muốn hoặc truy cập dữ liệu mà không có sự cho phép thích hợp.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(2) Broken Authentication

Các chức năng liên quan đến xác thực và quản lý phiên thường được triển khai không chính xác, cho phép kẻ tấn công thỏa hiệp mật khẩu, khóa, mã thông báo phiên hoặc khai thác các lỗi triển khai khác để chiếm định danh của người dùng tạm thời hoặc vĩnh viễn.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(3) Sensitive Data Exposure

Nhiều ứng dụng Web và API không bảo vệ đúng cách dữ liệu nhạy cảm, chẳng hạn như thông tin tài chính, chăm sóc sức khỏe, tài khoản người dùng. Những kẻ tấn công có thể đánh cắp hoặc sửa đổi dữ liệu được bảo vệ yếu kém đó để thực hiện các hành vi như gian lận thẻ tín dụng, đánh cắp danh tính hoặc các tội phạm khác. Dữ liệu nhạy cảm có thể bị xâm phạm nếu không áp dụng các biện pháp bảo vệ, chẳng hạn như mã hóa trong lưu trữ hoặc trong quá trình truy xuất yêu cầu có các biện pháp phòng ngừa đặc biệt.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(4) XML External Entities (XXE)

Nhiều bộ xử lý XML cũ hoặc được cấu hình kém sẽ xử lý các tham chiếu thực thể bên ngoài trong các tài liệu XML. Các thực thể bên ngoài có thể được sử dụng để tiết lộ các tệp nội bộ bằng trình xử lý tập tin URI, chia sẻ tập tin nội bộ, quét cổng nội bộ, thực thi mã từ xa và tấn công từ chối dịch vụ

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(5) Broken Access Control

Các hạn chế về những gì người dùng đã xác thực được phép truy cập thường không được thực thi đúng cách. Những kẻ tấn công có thể khai thác các lỗ hổng này để giành quyền truy cập vào các chức năng hoặc dữ liệu trái phép, chẳng hạn như truy cập tài khoản người dùng, xem các tập tin nhạy cảm, sửa đổi dữ liệu của người dùng, thay đổi quyền truy cập,...

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(6) Security Misconfiguration

Sai sót trong cấu hình bảo mật là một vấn đề thường thấy. Đây thường là kết quả của cấu hình mặc định không an toàn, cấu hình không đầy đủ hoặc phân tán, lưu trữ đám mây mở, tiêu đề HTTP được định cấu hình sai và thông báo lỗi chứa thông tin nhạy cảm. Tất cả các Hệ điều hành, Framework, thư viện và ứng dụng cần phải được định cấu hình an toàn và được cập nhật kịp thời.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(7) Cross-Site Scripting (XSS)

Lỗi XSS xảy ra khi một ứng dụng hoặc dữ liệu không tin cậy trong Website không được xác thực hoặc thoát đúng cách hoặc cập nhật nội dung Website với dữ liệu do người dùng cung cấp bằng cách sử dụng API trình duyệt có thể tạo HTML hoặc JavaScript. Lỗi XSS cho phép những kẻ tấn công thực thi các tập lệnh trong trình duyệt của nạn nhân, có thể chiếm quyền điều khiển phiên của người dùng, phá hoại các Website hoặc chuyển hướng người dùng đến các Website độc hại.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(8) Insecure Deserialization

Giải mã không an toàn thường dẫn đến việc thực thi mã từ xa. Ngay cả khi lỗi giải mã không dẫn đến việc thực thi mã từ xa, chúng có thể được sử dụng để thực hiện các cuộc tấn công, bao gồm cả tấn công phát lại, tấn công chèn gói tin và tấn công leo thang đặc quyền.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(9) Using Components with Known Vulnerabilities

Các thành phần như thư viện, framework và mô-đun phần mềm chạy với các đặc quyền giống như các ứng dụng. Nếu một thành phần có lỗ hổng dễ bị khai thác, một cuộc tấn công vào lỗ hổng có thể tạo điều kiện cho việc mất dữ liệu nghiêm trọng hoặc chiếm quyền điều khiển máy chủ. Các ứng dụng và API sử dụng các thành phần có lỗ hổng bảo mật đã biết có thể làm suy yếu khả năng bảo vệ của ứng dụng và kích hoạt các cuộc tấn công và mối đe dọa khác nhau.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.6. Lỗi hoặc sự cố phần mềm
(10) Insufficient Logging & Monitoring

Cùng với việc tích hợp không đầy đủ hoặc không hiệu quả đối với các phản ứng sự cố, cho phép kẻ tấn công tận dụng để xâm nhập hệ thống, duy trì và tận dụng tài nguyên để tấn công sang nhiều hệ thống khác, giả mạo, trích xuất hoặc phá hủy dữ liệu. Hầu hết các nghiên cứu về vi phạm đều cho thấy thời gian để phát hiện vi phạm là hơn 200 ngày, thường được phát hiện bởi các tổ chức bên ngoài hơn là các quy trình hoặc giám sát nội bộ.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.7. Sự lỗi thời của công nghệ

- Cơ sở hạ tầng lỗi thời hoặc lạc hậu có thể dẫn đến các hệ thống không đáng tin cậy
- Khi công nghệ trở nên lỗi thời, có nguy cơ mất tính toàn vẹn của dữ liệu do các cuộc tấn công.
- Ví dụ, trường hợp lỗi thời công nghệ đáng kể nhất trong những năm gần đây là Windows, phát triển từ XP, Vista, Windows 7, 8,10.11.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.8. Sai lệch về chất lượng dịch vụ

- Sự sai lệch về chất lượng dịch vụ có thể là sự bất thường về nguồn điện, hỏng kết nối Internet, nguồn điện và truyền thông có thể ảnh hưởng đáng kể đến khả năng cung cấp thông tin và hệ thống.
- Sự suy giảm dịch vụ này là một dạng gián đoạn, ảnh hướng đến khả dụng của hệ thống thông tin.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.8. Sai lệch về chất lượng dịch vụ

- Sự sai lệch về chất lượng dịch vụ có thể là sự bất thường về nguồn điện, hỏng kết nối Internet, nguồn điện và truyền thông có thể ảnh hưởng đáng kể đến khả năng cung cấp thông tin và hệ thống.
- Sự suy giảm dịch vụ này là một dạng gián đoạn, ảnh hướng đến khả dụng của hệ thống thông tin.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.9. Tấn công phá huỷ hoặc phá hoại

Liên quan đến hành vi phá hoại có chủ ý nhằm làm hỏng hệ thống máy tính hoặc doanh nghiệp, hoặc làm tổn hại tài sản và hình ảnh của tổ chức. Các hành vi này có thể từ sự phá vặt vãnh của nhân viên đến hành vi phá hoại có tổ chức nhằm vào tổ chức. Dù không gây thiệt hại tài chính, việc tấn công vào hình ảnh của tổ chức là rất nghiêm trọng.

- Ví dụ, các nhà hoạt động tham gia vào một hành vi được gọi là doxing để định vị hoặc đánh cắp hồ sơ cá nhân và bí mật, sau đó công khai chúng để làm bẽ mặt các đối thủ chính trị.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.10. Trộm

- Trộm thường bao gồm nhiều hình thức tấn công như tấn công bằng phần mềm, gián điệp hoặc xâm phạm, tống tiền thông tin và xâm phạm quyền sở hữu trí tuệ.
- Khi thông tin điện tử bị đánh cắp, hành vi này không phải lúc nào cũng dễ dàng nhận ra. Nếu kẻ trộm thông minh và che giấu dấu vết kỹ lưỡng, tội phạm có thể không bị phát hiện.
- Điều đáng lo ngại hơn cả việc mất dữ liệu là khả năng người dùng đã lưu thông tin tài khoản trên thiết bị di động, cho phép kẻ trộm sử dụng quyền truy cập hợp pháp để xâm nhập vào tài khoản doanh nghiệp hoặc cá nhân của nạn nhân.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.11. Sự xâm phạm đến Sở hữu trí tuệ

- Sở hữu trí tuệ bao gồm bí mật thương mại, bản quyền, nhãn hiệu, bằng sáng chế và bản quyền.
- Việc chiếm dụng sở hữu trí tuệ trái phép cấu thành mối đe dọa đối với an ninh thông tin. ví dụ, khi nhân viên lấy một ý tưởng mà họ phát triển tại nơi làm việc và sử dụng nó để kiếm tiền cho chính mình.
- Vi phạm sở hữu trí tuệ phổ biến nhất là vi phạm bản quyền phần mềm.

1.2. Các mối đe doạ đến an ninh HTTT
1.2.12. Sức mạnh của thiên nhiên

Các lực lượng của thiên nhiên, có thể gây ra một số mối đe dọa nguy hiểm nhất vì chúng thường xảy ra mà không có cảnh báo trước và nằm ngoài tầm kiểm soát của con người. Những mối đe dọa này, bao gồm các sự kiện như hỏa hoạn, lũ lụt, động đất, lở đất, lở bùn, bão gió, bão cát, bùng phát năng lượng mặt trời và sét cũng như phun trào núi lửa và sự xâm nhập của côn trùng, không chỉ có thể phá vỡ cuộc sống của con người mà còn cả việc lưu trữ, truyền tải và sử dụng thông tin.

1.3. Phương pháp tiếp cận và các vai trò trong an ninh thông tin

1.3.1. Các phương pháp tiếp cận

- An ninh thông tin có thể bắt đầu từ các quản trị viên hệ thống nhằm cải thiện tính bảo mật của hệ thống của họ bằng cách làm việc cùng nhau (tiếp cận từ dưới lên).
- An ninh thông tin bắt đầu từ nhà quản lý cấp cao, những người ban hành chính sách, thủ tục và quy trình, chỉ định các mục tiêu và kết quả mong đợi, và xác định trách nhiệm giải trình cho từng hành động bắt buộc (tiếp cận từ trên xuống).

1.3. Phương pháp tiếp cận và các vai trò trong an ninh thông tin

1.3.2. Cân bằng giữa an ninh thông tin và quyền truy cập

- Để thuận tiện cho sử dụng, người dùng luôn muốn càng nhiều quyền truy cập càng tốt; nhưng để đảm bảo an ninh thông tin cho hệ thống, các biện pháp bảo vệ lại cố gắng duy trì tối thiểu quyền truy cập.
- Để đạt được sự cân bằng, nghĩa là, để vận hành một hệ thống thông tin thỏa mãn cả người dùng và các chuyên gia đảm bảo an toàn thông tin, cấp độ an toàn cần phải thiết lập truy cập hợp lý, nhưng vẫn bảo vệ chống lại các mối đe dọa.

1.3. Phương pháp tiếp cận và các vai trò trong an ninh thông tin
1.3.3. Chuyên gia an ninh

Quản lý cấp cao

- Giám đốc thông tin (CIO)
- Giám đốc an ninh thông tin (CISO)

Nhóm dự án an ninh thông tin

- Người phụ trách dự án
- Trưởng nhóm
- Người phát triển chính sách bảo mật
- Chuyên gia đánh giá rủi ro
- Chuyên gia bảo mật
- Quản trị viên hệ thống
- Người dùng cuối

1.3. Phương pháp tiếp cận và các vai trò trong an ninh thông tin
1.3.4. Trách nhiệm dữ liệu

- **Chủ sở hữu dữ liệu**: Họ xác định mức độ phân loại dữ liệu và điều chỉnh khi cần thiết dựa theo yêu cầu của thay đổi tổ chức.
- **Người giám hộ dữ liệu**: chịu trách nhiệm về thông tin và các hệ thống xử lý, truyền và lưu trữ thông tin đó, thường là các CISO hoặc quản trị viên hệ thống.
- **Người ủy thác dữ liệu**: giám sát việc quản lý một tập hợp thông tin cụ thể và phối hợp với người giám hộ dữ liệu để lưu trữ, bảo vệ và sử dụng thông tin đó.
- **Người dùng dữ liệu**: Mọi người trong tổ chức đều chịu trách nhiệm về bảo mật dữ liệu

1.3. Phương pháp tiếp cận và các vai trò trong an ninh thông tin
1.3.5. Cộng đồng lợi ích

- **Chuyên gia an ninh thông tin**: chịu trách nhiệm bảo vệ hệ thống và dữ liệu của tổ chức khỏi các cuộc tấn công.
- **Chuyên gia công nghệ thông tin**: Họ chú trọng vào chi phí, hiệu quả hoạt động, sự dễ dùng và tốc độ phản hồi của hệ thống.
- **Chuyên gia tổ chức**: bao gồm quản lý, nhân sự, kế toán và nhân viên pháp lý,...

1.4. Quản lý an ninh thông tin

Quản lý an ninh thông tin (InfoSec) với 6 chữ P

- **Planning**: chiến lược InfoSec phải được phát triển từ chiến lược phát triển, chiến lược kinh doanh và chiến lược CNTT.
- **Policy:** Chính sách InfoSec cho doanh nghiệp (EISP); CS an ninh cụ thể theo vấn đề (ISSP); CS an ninh cụ thể cho HT (SysSP).
- **Program:** Các hoạt động InfoSec được quản lý riêng biệt như các thực thể độc lập được gọi là "Program".
- **Protection:** hoạt động quản lý rủi ro, các cơ chế, công nghệ.
- **People:** nhân viên an ninh, an ninh của nhân viên.
- **Project:** Quản lý dự án bao gồm việc xác định và kiểm soát các nguồn lực, điều chỉnh quy trình để đạt được tiến độ.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin

- Lập kế hoạch chiến lược đặt ra định hướng dài hạn mà tổ chức và từng bộ phận cấu thành của nó phải thực hiện. Lập kế hoạch chiến lược phải hướng dẫn các nỗ lực của tổ chức và tập trung nguồn lực vào các mục tiêu cụ thể, được xác định rõ ràng.
- Kế hoạch chiến lược tổng thể được mở rộng từ chiến lược tổ chức thành các kế hoạch cho các bộ phận chính. Sau đó, mỗi cấp độ của mỗi bộ phận sẽ chuyển các mục tiêu kế hoạch đó thành các mục tiêu cụ thể hơn cho cấp độ bên dưới

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
a) Lãnh đạo an ninh thông tin

Lãnh đạo nhóm an ninh thông tin giám sát và quản lý tất cả các cấu trúc và quy trình tổ chức bảo vệ thông tin. Sau đó, quản trị an ninh thông tin áp dụng các nguyên tắc và cấu trúc quản lý này vào chức năng an ninh thông tin.

Lãnh đạo phải tham gia vào một loạt các hoạt động cốt lõi để hướng dẫn việc phát triển và triển khai chương trình quản trị InfoSec

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
a) Lãnh đạo an ninh thông tin (tt)

Các hoat động cốt lõi trong an ninh thông tin cần lãnh đao tham gia:

- Tiến hành đánh giá InfoSec hàng năm, kết quả đánh giá mà CEO phải xem xét cùng nhân viên và sau đó báo cáo lên hội đồng quản trị.
- Tiến hành đánh giá rủi ro định kỳ đối với tài sản thông tin như một phần của chương trình quản lý rủi ro.
- Triển khai các chính sách và quy trình dựa trên đánh giá rủi ro để bảo mật tài sản thông tin.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
a) Lãnh đạo an ninh thông tin (tt)

- Thiết lập cấu trúc quản lý an ninh để chỉ định các vai trò, trách nhiệm, quyền hạn và trách nhiệm cá nhân.
- Phát triển các kế hoạch và khởi xướng các hành động để cung cấp InfoSec đầy đủ cho mạng, cơ sở hạ tầng, hệ thống và thông tin.
- Coi InfoSec là một phần không thể thiếu của vòng đời hệ thống.
- Cung cấp nhận thức, đào tạo và giáo dục về InfoSec cho nhân viên.
- Tiến hành thử nghiệm và đánh giá định kỳ về hiệu quả của các chính sách và quy trình InfoSec.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
a) Lãnh đạo an ninh thông tin (tt)

- Tạo và thực hiện kế hoạch hành động khắc phục để giải quyết mọi điểm kém hiệu quả của InfoSec.
- Phát triển và triển khai các quy trình ứng phó sự cố.
- Thiết lập các kế hoạch, quy trình và thử nghiệm để cung cấp tính liên tục của hoạt động.
- Sử dụng hướng dẫn thực hành tốt nhất về an ninh, chẳng hạn như loạt tiêu chuẩn ISO 27000, để đo lường hiệu suất InfoSec.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
a) Lãnh đạo an ninh thông tin (tt)

Sáu nguyên tắc quản trị an ninh thông tin:

1. Thiết lập an ninh thông tin trên toàn tổ chức.
2. Áp dụng phương pháp tiếp cận dựa trên rủi ro.
3. Đặt ra hướng đi cho các quyết định đầu tư.
4. Đảm bảo tuân thủ các yêu cầu nội bộ và bên ngoài.
5. Nuôi dưỡng môi trường tích cực về an ninh.
6. Xem xét hiệu suất liên quan đến kết quả kinh doanh.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
b) Kết quả quản trị an ninh thông tin

Năm mục tiêu của quản trị an ninh thông tin (InfoSec) như sau:

1. Căn chỉnh chiến lược InfoSec với CL kinh doanh để hỗ trợ các MTTC.
2. Quản lý rủi ro bằng cách (=) thực hiện các biện pháp thích hợp để quản lý và giảm thiểu các mối đe dọa đối với các nguồn thông tin.
3. Quản lý nguồn lực = sử dụng kiến thức và cơ sở hạ tầng InfoSec một cách hiệu quả và thiết thực.
4. Đo lường hiệu suất = đo lường, giám sát và báo cáo các số liệu quản trị InfoSec để đảm bảo đạt được các MTTC (mục tiêu tổ chức).
5. Cung cấp giá trị = tối ưu các khoản ĐT InfoSec để hỗ trợ các MTTC.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
c) Cấp độ quy hoạch

Kế hoạch chiến lược (KHCL) chung của tổ chức được chuyển thành các KHCL cho từng bộ phận hoặc hoạt động chính, bước tiếp theo là chuyển các KHCL thành các mục tiêu chiến thuật hướng tới việc đạt được các thành tựu cụ thể, có thể đo lường, có thể đạt được và có thời hạn.

Các KHCL được sử dụng để tạo ra các kế hoạch chiến thuật (KHCT), KHCT trung vào các cam kết sẽ hoàn thành trong vòng một hoặc hai năm. Mỗi mục tiêu phải cụ thể và phải có ngày hoàn thành.

Các KHCT được sử dụng để lập kế hoạch hoạt động (KHHĐ), các nhà quản lý và nhân viên sử dụng KHHĐ để tổ chức thực hiện nhiệm vụ hàng ngày.

1.4. Quản lý an ninh thông tin
1.4.1. Lập kế hoạch và quản trị an ninh thông tin
d) Lập kế hoạch và CISO

Kế hoạch chiến lược được xây dựng ở cấp cao nhất của tổ chức nhằm tạo ra một chiến lược tổng thể. Khi các cấp thấp hơn trong hệ thống tham gia, kế hoạch từ cấp trên được phát triển chi tiết hơn, phù hợp với chức năng cụ thể. Các kế hoạch cấp cao này được chuyển thành các kế hoạch chiến lược chức năng, như tài chính, CNTT và hoạt động, sau đó phân nhỏ thành kế hoạch chiến thuật cho các nhà quản lý giám sát. Cuối cùng, các kế hoạch này cung cấp định hướng cho các hoạt động thực hiện bởi các nhân viên không thuộc cấp quản lý.

1.4. Quản lý an ninh thông tin
1.4.2. Chính sách, tiêu chuẩn và thực hành an ninh thông tin

Các chương trình an ninh tốt bắt đầu và kết thúc bằng chính sách. An ninh thông tin chủ yếu là vấn đề quản lý, không phải vấn đề kỹ thuật, và chính sách là công cụ quản lý bắt buộc nhân viên phải hoạt động theo cách giữ gìn an ninh của tài sản thông tin.

Ba loại chính sách an ninh (CSAN):

1. CSAN thông tin doanh nghiệp (EISP - Enterprise Information Security Policy).
2. CSAN vấn đề cụ thể (ISSP - Issue-Specific Security Policy).
3. CSAN hệ thống cụ thể (SysSP - System-Specific Security Policy).

• 1.4. Quản lý an ninh thông tin

1.4.2. Chính sách, tiêu chuẩn và thực hành an ninh thông tin

a) Chính sách an ninh thông tin doanh nghiệp (EISP)

Bao gồm các yếu tố sau:

- Tổng quan về triết lý của công ty về bảo mật.
- Thông tin về cấu trúc của tổ chức an ninh thông tin và những người thực hiện vai trò an ninh thông tin.
- Trách nhiệm được nêu rõ ràng về an ninh được chia sẻ bởi tất cả các thành viên của tổ chức (nhân viên, nhà thầu, cố vấn, đối tác và khách truy cập).
- Trách nhiệm được nêu rõ ràng về an ninh dành riêng cho từng vai trò trong tổ chức.

1.4. Quản lý an ninh thông tin
1.4.2. Chính sách, tiêu chuẩn và thực hành an ninh thông tin
b) Chính sách an ninh vấn đề cụ thể (ISSP)

Bao gồm các thành phần:

- Tuyên bố về Chính sách
- Quyền truy cập và sử dụng thiết bị được ủy quyền
- Sử dụng thiết bị bị cấm
- Quản lý hệ thống
- Vi phạm Chính sách
- Rà soát và sửa đổi chính sách
- Giới hạn trách nhiệm

• 1.4. Quản lý an ninh thông tin
1.4.2. Chính sách, tiêu chuẩn và thực hành an ninh thông tin
c) Chính sách an ninh cho hệ thống cụ thể (SysSP)

SysSP có thể được chia thành hai nhóm chung, SysSP hướng dẫn quản lý và SysSP thông số kỹ thuật hoặc chúng có thể được kết hợp thành một tài liệu chính sách duy nhất chứa các thành phần của cả hai.

- Tài liệu hướng dẫn quản lý SysSP
- Thông số kỹ thuật SysSP

• 1.4. Quản lý an ninh thông tin

1.4.2. Chính sách, tiêu chuẩn và thực hành an ninh thông tin

d) Phát triển và triển khai chính sách an ninh hiệu quả

Để các chính sách (CS)có hiệu quả và có thể bảo vệ được về mặt pháp lý, cần phải thực hiện đúng các bước sau:

1. Phát triển: Các CS phải được viết theo các thực hành được ngành chấp nhận và được ban quản lý chính thức phê duyệt.
2. Phổ biến: Các chính sách phải được phổ biến.
3. Xem xét: Các CS phải dễ đọc và được tất cả nhân viên đọc.
4. Hiểu: Các CS phải được tất cả nhân viên hiểu.
5. Tuân thủ: Các CS phải được chính thức chấp thuận.
6. Thực thi: Các CS phải được áp dụng thống nhất cho tất cả nhân viên.

1.4. Quản lý an ninh thông tin
1.4.3. Chương trình Giáo dục, Đào tạo và Nhận thức về An ninh (SETA)

Chương trình SETA (Security Education, Training, and Awareness) bao gồm ba thành phần riêng biệt: giáo dục an ninh, đào tạo an ninh và nhận thức về an ninh. Mục đích của SETA là tăng cường an ninh bằng cách thực hiện các hoạt động sau:

- Nâng cao nhận thức về nhu cầu bảo vệ tài nguyên hệ thống.

- Phát triển các kỹ năng và kiến thức để người dùng máy tính có thể thực hiện công việc của mình an toàn hơn.

- Xây dựng kiến thức chuyên sâu khi cần thiết để thiết kế, triển khai hoặc vận hành các chương trình an ninh cho các tổ chức và hệ thống.

1.4. Quản lý an ninh thông tin
1.4.4. Bản thiết kế, mô hình và khung an ninh thông tin

Bản thiết kế là việc triển khai chi tiết của tổ chức về khung an ninh thông tin. Bản thiết kế chỉ rõ các nhiệm vụ và thứ tự thực hiện chúng, giống như bản thiết kế của kiến trúc sư đóng vai trò là khung thiết kế cho việc xây dựng một tòa nhà. Khung là nền tảng triết lý mà bản thiết kế được thiết kế, giống như phong cách hoặc phương pháp mà kiến trúc sư được đào tạo.

Tiêu chuẩn và mô hình an ninh thông tin hiệu quả:

- Tiêu chuẩn ISO 27000
- Mô hình an ninh NIST

1.5. Các thành phần trong một HTTT

- Hệ thống thông tin không chỉ là phần cứng và phần mềm máy tính; nó bao gồm nhiều thành phần khác nhau, tất cả cùng hoạt động để hỗ trợ các hoạt động cá nhân và chuyên nghiệp. Các thành phần như: Software, Hardware, Data, People, Procedures, Network.
- Mỗi thành phần của HTTT có điểm mạnh và điểm yếu riêng, cũng như các đặc điểm và công dụng riêng. Mỗi thành phần của HTTT cũng có những yêu cầu bảo mật riêng của nó.

1.5. Các thành phần trong một HTTT
1.5.1. Software

- Bao gồm các ứng dụng, hệ điều hành và các tiện ích lệnh kết hợp, là thành phần IS khó bảo mật nhất.
- Ngành công nghiệp CNTT tràn lan các báo cáo cảnh báo về lỗ hổng, lỗi, điểm yếu hoặc các vấn đề cơ bản khác trong phần mềm.
- Các chương trình phần mềm thường được tạo ra theo những hạn chế của quản lý dự án, hạn chế thời gian, chi phí và nhân lực. Thay vì được tích hợp ngay từ đầu như một phần không thể thiếu, bảo mật thông tin thường chỉ được xem xét sau cùng.

1.5. Các thành phần trong một HTTT
1.5.2. Hardware

- Phần cứng là công nghệ vật lý chứa và thực thi phần mềm, lưu trữ và vận chuyển dữ liệu, đồng thời cung cấp giao diện để nhập và xóa thông tin khỏi hệ thống.
- Các chính sách bảo mật vật lý coi phần cứng là tài sản vật lý và bảo vệ tài sản vật lý khỏi bị hư hại hoặc trộm cắp. Áp dụng các công cụ bảo mật vật lý truyền thống, chẳng hạn như khóa và chìa khóa, hạn chế quyền truy cập và tương tác với các thành phần phần cứng của hệ thống thông tin.

1.5. Các thành phần trong một HTTT
1.5.3. Data

- Dữ liệu được lưu trữ, xử lý và truyền đi bởi hệ thống máy tính phải được bảo vệ. Dữ liệu thường là tài sản có giá trị nhất của một tổ chức và do đó là mục tiêu chính của các cuộc tấn công có chủ đích.
- Vì dữ liệu và thông tin tồn tại ở dạng vật lý trong nhiều tổ chức dưới dạng báo cáo giấy, ghi chú viết tay và bản in máy tính, nên việc bảo vệ thông tin vật lý cũng quan trọng như việc bảo vệ thông tin điện tử dựa trên máy tính.

1.5. Các thành phần trong một HTTT
1.5.4. People

- Con người luôn là mối đe dọa lớn đối với an ninh thông tin, thường được coi là mắt xích yếu nhất trong chương trình an ninh thông tin của một tổ chức.
- Nếu các biện pháp chính sách, giáo dục và đào tạo, nâng cao nhận thức và công nghệ không được sử dụng đúng cách để ngăn chặn hành vi vô tình hoặc cố ý làm hỏng hoặc mất thông tin.
- Kỹ nghệ xã hội hội thường được sử dụng để thao túng con người để có được thông tin truy cập trái phép về một hệ thống.

1.5. Các thành phần trong một HTTT
1.5.5. Procedures

- Quy trình là các hướng dẫn bằng văn bản để hoàn thành một nhiệm vụ cụ thể. Khi người dùng trái phép có được quy trình của tổ chức, điều đó gây ra mối đe dọa đến tính toàn vẹn của thông tin.
- Hầu hết các tổ chức cung cấp các quy trình cho nhân viên để họ có thể truy cập vào hệ thống thông tin, nhưng nhiều công ty không đảm bảo giáo dục đầy đủ về cách sử dụng quy trình an toàn. Việc đào tạo nhân viên về bảo mật quy trình quan trọng không kém so với việc bảo vệ hệ thống thông tin về mặt vật lý.

1.5. Các thành phần trong một HTTT
1.5.6. Network

- Mạng là thành phần HTTT, truyền tải dữ liệu và thông tin giữa các thành phần của hệ thống thông tin. Việc sử dụng mạng đã làm gia tăng nhu cầu bảo mật cho máy tính và thông tin
- Khi các hệ thống thông tin được kết nối với nhau để tạo thành mạng LAN và các mạng LAN này được kết nối với các mạng khác như Internet, các thách thức bảo mật mới nhanh chóng xuất hiện.

Cảm ơn các bạn,

Chúc các bạn thành công!