Mục 5.1: Quản lý an toàn thông tin

1. Quản lý an toàn thông tin (ATTT) là gì?

a) Chỉ là việc cài đặt phần mềm diệt virus.

b) Chỉ là việc thiết lập tường lửa.

c) Là quá trình xác định, đánh giá và kiểm soát các rủi ro đối với tài sản thông tin của tổ chức.

d) Chỉ là việc sao lưu dữ liệu định kỳ.

2. Mục tiêu chính của quản lý ATTT là gì?

a) Tăng tốc độ xử lý của hệ thống.

b) Đảm bảo tính bí mật, toàn vẹn và sẵn sàng (CIA) của thông tin và hệ thống.

c) Giảm chi phí đầu tư cho công nghệ thông tin.

d) Theo dõi hoạt động của nhân viên.

3. Ba yếu tố cốt lõi của an toàn thông tin (CIA Triad) là gì?

a) Chi phí, Hiệu quả, An ninh.

b) Phần cứng, Phần mềm, Mạng.

c) Tính bí mật (Confidentiality), Tính toàn vẹn (Integrity), Tính sẵn sàng (Availability).

d) Xác thực, Trao quyền, Quản trị.

4. Đánh giá rủi ro ATTT là quá trình gì?

a) Cài đặt các bản vá lỗi bảo mật.

b) Xác định các mối đe dọa, lỗ hổng và tác động tiềm ẩn đối với tài sản thông tin.

c) Mua bảo hiểm cho hệ thống thông tin.

d) Đào tạo nhận thức về an toàn thông tin cho nhân viên.

5. Tài sản thông tin (Information Asset) bao gồm những gì?

a) Chỉ bao gồm phần cứng máy tính.

b) Chỉ bao gồm phần mềm ứng dụng.

c) Chỉ bao gồm dữ liệu khách hàng.

d) Bao gồm dữ liệu, phần cứng, phần mềm, dịch vụ, tài liệu, con người và uy tín của tổ chức.

6. Mối đe dọa (Threat) trong ATTT là gì?

a) Một điểm yếu trong hệ thống.

b) Bất kỳ tác nhân hoặc sự kiện nào có khả năng gây hại cho tài sản thông tin.

c) Một biện pháp kiểm soát an ninh.

d) Giá trị của tài sản thông tin.

7. Lỗ hổng (Vulnerability) trong ATTT là gì?

a) Một điểm yếu trong thiết kế, triển khai, vận hành hoặc quản lý hệ thống có thể bị khai thác bởi mối đe dọa.

b) Một cuộc tấn công thành công.

c) Một chính sách an toàn thông tin.

d) Một phần mềm độc hại.

8. Phương pháp đánh giá rủi ro "đường cơ sở" (Baseline Approach) dựa trên việc gì?

a) Phân tích chi tiết từng mối đe dọa và lỗ hổng.

b) Áp dụng các biện pháp kiểm soát an ninh được công nhận rộng rãi hoặc theo các tiêu chuẩn ngành.

c) Phỏng vấn các chuyên gia bảo mật.

d) Tính toán xác suất xảy ra tấn công.

9. Tại sao việc xác định giá trị tài sản thông tin lại quan trọng trong đánh giá rủi ro?

a) Để biết cần mua bao nhiêu phần cứng.

b) Để ưu tiên các nỗ lực bảo vệ và xác định mức độ tác động nếu tài sản bị tổn hại.

c) Để tính toán chi phí cài đặt phần mềm.

d) Để xác định số lượng nhân viên IT cần thiết.

10. Rủi ro (Risk) trong ATTT được định nghĩa như thế nào?

a) Chỉ là khả năng xảy ra một mối đe dọa.

b) Chỉ là sự tồn tại của một lỗ hổng.

c) Là khả năng một mối đe dọa khai thác một lỗ hổng gây tổn hại cho tài sản, thường được xem xét cùng với tác động tiềm ẩn.

d) Là chi phí để khắc phục sự cố.

11. Phương pháp đánh giá rủi ro "không chính thức" (Informal Approach) thường dựa vào yếu tố nào?

a) Các công thức toán học phức tạp.

b) Các tiêu chuẩn quốc tế nghiêm ngặt.

c) Kinh nghiệm và trực giác của các chuyên gia hoặc nhóm đánh giá, thường thông qua thảo luận và phỏng vấn.

d) Quét lỗ hổng tự động.

12. Phương pháp "phân tích chi tiết rủi ro" (Detailed Risk Analysis) khác với phương pháp đường cơ sở như thế nào?

a) Phân tích chi tiết chỉ áp dụng cho các hệ thống nhỏ.

b) Phân tích chi tiết đi sâu vào việc xác định tài sản cụ thể, mối đe dọa, lỗ hổng, xác suất xảy ra và tác động, thay vì chỉ áp dụng các kiểm soát chung.

c) Phân tích chi tiết không cần xác định tài sản.

d) Phân tích chi tiết ít tốn kém và nhanh hơn.

13. "Kiểm soát ATTT" (Security Control) là gì?

a) Một lỗ hổng bảo mật.

b) Một mối đe dọa tiềm ẩn.

c) Các biện pháp, chính sách, quy trình hoặc cơ chế được sử dụng để giảm thiểu hoặc quản lý rủi ro.

d) Một cuộc tấn công mạng.

14. Tại sao cần phải thực hiện đánh giá rủi ro định kỳ?

a) Vì luật pháp yêu cầu mỗi ngày.

b) Để kiểm tra xem nhân viên có tuân thủ quy định không.

c) Vì môi trường mối đe dọa, lỗ hổng, giá trị tài sản và hoạt động kinh doanh liên tục thay đổi.

d) Để có lý do mua thiết bị mới.

15. Phương pháp đánh giá rủi ro "kết hợp" (Combined Approach) là gì?

a) Chỉ sử dụng phương pháp đường cơ sở.

b) Chỉ sử dụng phương pháp phân tích chi tiết.

c) Kết hợp các yếu tố của phương pháp đường cơ sở, không chính thức và phân tích chi tiết để tận dụng ưu điểm của từng phương pháp.

d) Sử dụng một phương pháp hoàn toàn mới không liên quan.

16. Việc "chấp nhận rủi ro" (Risk Acceptance) có nghĩa là gì trong quản lý rủi ro ATTT?

a) Loại bỏ hoàn toàn rủi ro.

b) Chuyển giao rủi ro cho bên thứ ba.

c) Tổ chức quyết định không thực hiện hành động nào để giảm thiểu rủi ro (thường áp dụng cho rủi ro có tác động thấp hoặc chi phí xử lý quá cao).

d) Giảm thiểu khả năng xảy ra rủi ro.

17. Sự khác biệt cơ bản giữa đánh giá rủi ro định tính (Qualitative) và định lượng (Quantitative) là gì?

a) Định tính sử dụng số liệu chính xác, định lượng sử dụng mô tả.

b) Định tính sử dụng các thang đo mô tả (cao, trung bình, thấp) cho xác suất và tác động, trong khi định lượng cố gắng gán giá trị tiền tệ hoặc số liệu cụ thể cho rủi ro và tác động.

c) Định tính chỉ áp dụng cho tài sản vật lý, định lượng cho tài sản phi vật lý.

d) Định lượng luôn dễ thực hiện hơn định tính.

18. Trong phân tích chi tiết rủi ro, công thức cơ bản để ước tính rủi ro thường liên quan đến các yếu tố nào?

a) Chỉ có giá trị tài sản.

b) Chỉ có xác suất mối đe dọa.

c) Giá trị tài sản (AV), Mức độ phơi bày (EF - Exposure Factor), và Tỷ lệ xảy ra hàng năm (ARO - Annualized Rate of Occurrence) hoặc Xác suất mối đe dọa khai thác lỗ hổng và Tác động.

d) Chỉ có chi phí của biện pháp kiểm soát.

19. Tại sao việc lựa chọn phương pháp đánh giá rủi ro (đường cơ sở, không chính thức, chi tiết, kết hợp) lại phụ thuộc vào bối cảnh của tổ chức?

a) Vì mỗi phương pháp chỉ dùng được cho một ngành công nghiệp nhất định.

b) Vì các yếu tố như quy mô tổ chức, nguồn lực sẵn có, yêu cầu pháp lý, văn hóa doanh nghiệp và mức độ trưởng thành về ATTT sẽ ảnh hưởng đến tính khả thi và hiệu quả của từng phương pháp.

c) Vì các chuyên gia bảo mật chỉ biết một phương pháp duy nhất.

d) Vì phần mềm đánh giá rủi ro chỉ hỗ trợ một phương pháp.

20. "Rủi ro tồn dư" (Residual Risk) là gì?

a) Rủi ro trước khi áp dụng bất kỳ biện pháp kiểm soát nào.

b) Rủi ro đã được chuyển giao cho bên thứ ba.

c) Mức độ rủi ro còn lại sau khi đã áp dụng các biện pháp kiểm soát ATTT.

d) Rủi ro không thể xác định được.

Mục 5.2: Các bộ chuẩn quản lý ATTT

1. Bộ tiêu chuẩn ISO/IEC 27000 series liên quan đến lĩnh vực nào?

a) Quản lý chất lượng.

b) Quản lý an toàn thông tin.

c) Quản lý môi trường.

d) Quản lý dự án.

2. ISO/IEC 27001 là tiêu chuẩn về cái gì?

a) Hướng dẫn đánh giá rủi ro ATTT.

b) Các yêu cầu đối với Hệ thống quản lý an toàn thông tin (ISMS).

c) Các biện pháp kiểm soát ATTT chi tiết.

d) Quản lý sự cố ATTT.

3. ISMS là viết tắt của thuật ngữ nào?

a) Information Security Management Standard

b) Internet Security Management System

c) Information Security Management System

d) Internal Security Management Standard

4. Chu trình PDCA là viết tắt của các từ nào?

a) Prepare, Develop, Control, Assess

b) Plan, Do, Check, Act

c) Protect, Detect, Correct, Amend

d) Policy, Design, Configure, Audit

5. Giai đoạn "Plan" (Lập kế hoạch) trong chu trình PDCA của ISMS bao gồm việc gì?

a) Thực hiện các biện pháp kiểm soát.

b) Giám sát và đo lường hiệu quả.

c) Thiết lập chính sách, mục tiêu, quy trình và thủ tục ISMS liên quan đến quản lý rủi ro.

d) Thực hiện các hành động khắc phục.

6. Giai đoạn "Do" (Thực hiện) trong chu trình PDCA của ISMS bao gồm việc gì?

a) Đánh giá lại chính sách ATTT.

b) Xem xét kết quả giám sát.

c) Thực thi và vận hành chính sách, các biện pháp kiểm soát, quy trình và thủ tục ISMS đã lập kế hoạch.

d) Cập nhật kế hoạch quản lý rủi ro.

7. Giai đoạn "Check" (Kiểm tra) trong chu trình PDCA của ISMS bao gồm việc gì?

a) Đào tạo nhận thức cho nhân viên.

b) Triển khai các biện pháp kiểm soát mới.

c) Giám sát, xem xét, đo lường hiệu quả của quy trình so với chính sách, mục tiêu và báo cáo kết quả cho quản lý.

d) Xác định các tài sản thông tin.

8. Giai đoạn "Act" (Hành động) trong chu trình PDCA của ISMS bao gồm việc gì?

a) Lập kế hoạch ban đầu cho ISMS.

b) Thực hiện các quy trình đã định.

c) Chỉ báo cáo kết quả kiểm tra.

d) Thực hiện các hành động khắc phục và phòng ngừa dựa trên kết quả kiểm tra và xem xét của quản lý để cải tiến liên tục ISMS.

9. Tại sao chu trình PDCA lại quan trọng đối với ISMS theo ISO 27001?

a) Vì nó là yêu cầu bắt buộc của pháp luật.

b) Vì nó cung cấp một khuôn khổ cho việc thiết lập, triển khai, vận hành, giám sát, xem xét, duy trì và cải tiến liên tục ISMS.

c) Vì nó giúp giảm chi phí phần cứng.

d) Vì nó chỉ tập trung vào việc vá lỗi phần mềm.

10. ISO/IEC 27002 cung cấp cái gì?

a) Các yêu cầu để được chứng nhận ISMS.

b) Quy trình đánh giá rủi ro chi tiết.

c) Hướng dẫn thực hiện và các biện pháp kiểm soát ATTT tốt nhất (best practices) để hỗ trợ cho ISO 27001.

d) Các quy định về mã hóa dữ liệu.

11. "Tuyên bố về tính áp dụng" (Statement of Applicability - SoA) trong ISO 27001 là gì?

a) Một bản danh sách tất cả nhân viên được phép truy cập hệ thống.

b) Một tài liệu mô tả chi tiết về phần cứng và phần mềm.

c) Một tài liệu liệt kê các biện pháp kiểm soát được chọn từ Phụ lục A của ISO 27001 (hoặc nguồn khác), lý do lựa chọn và tình trạng triển khai của chúng.

d) Một báo cáo về các sự cố an ninh đã xảy ra.

12. Lợi ích của việc áp dụng ISMS theo ISO 27001 là gì?

a) Chỉ để có chứng chỉ treo tường.

b) Làm tăng số lượng sự cố an ninh.

c) Giúp tổ chức quản lý rủi ro ATTT một cách có hệ thống, tăng cường lòng tin của khách hàng/đối tác, tuân thủ pháp luật và cải tiến liên tục.

d) Giảm hiệu suất làm việc của nhân viên.

13. Phụ lục A của ISO 27001 chứa nội dung gì?

a) Các định nghĩa thuật ngữ.

b) Yêu cầu chi tiết về chính sách ATTT.

c) Một danh mục tham khảo các mục tiêu kiểm soát và biện pháp kiểm soát ATTT.

d) Hướng dẫn về quản lý sự cố.

14. Việc "cải tiến liên tục" (Continual Improvement) trong ISMS có nghĩa là gì?

a) Thay đổi toàn bộ hệ thống mỗi năm.

b) Quá trình định kỳ xem xét, đánh giá và thực hiện các thay đổi để nâng cao hiệu quả và sự phù hợp của ISMS.

c) Chỉ sửa lỗi khi có sự cố xảy ra.

d) Mua công nghệ mới nhất.

15. Ai chịu trách nhiệm cao nhất đối với ISMS trong một tổ chức?

a) Chỉ bộ phận IT.

b) Chỉ nhân viên bảo vệ.

c) Ban lãnh đạo cao nhất của tổ chức.

d) Khách hàng của tổ chức.

16. Mối quan hệ giữa ISO 27001 và ISO 27002 là gì?

a) ISO 27002 là phiên bản cũ của ISO 27001.

b) Chúng không liên quan đến nhau.

c) ISO 27001 đặt ra các yêu cầu cho ISMS, còn ISO 27002 cung cấp hướng dẫn và các biện pháp kiểm soát chi tiết để thực hiện các yêu cầu đó.

d) ISO 27001 dành cho doanh nghiệp lớn, ISO 27002 cho doanh nghiệp nhỏ.

17. Tại sao việc xác định "bối cảnh của tổ chức" (Context of the Organization) lại là một yêu cầu quan trọng trong ISO 27001:2013/2022?

a) Để liệt kê danh sách đối thủ cạnh tranh.

b) Để hiểu các yếu tố bên trong và bên ngoài, các bên quan tâm và yêu cầu của họ có thể ảnh hưởng đến khả năng ISMS đạt được kết quả dự kiến.

c) Để xác định màu sắc logo của công ty.

d) Để chọn nhà cung cấp phần cứng.

18. Sự khác biệt chính giữa "hành động khắc phục" (Corrective Action) và "hành động phòng ngừa" (Preventive Action) trong ISMS là gì?

a) Khắc phục là sửa lỗi, phòng ngừa là sao lưu dữ liệu.

b) Khắc phục áp dụng cho sự cố lớn, phòng ngừa cho sự cố nhỏ.

c) Hành động khắc phục nhằm loại bỏ nguyên nhân của sự không phù hợp đã xảy ra để ngăn tái diễn, trong khi hành động phòng ngừa (ít được nhấn mạnh trong phiên bản mới, tích hợp vào quản lý rủi ro) nhằm loại bỏ nguyên nhân của sự không phù hợp tiềm ẩn để ngăn chặn nó xảy ra.

d) Hành động phòng ngừa luôn tốn kém hơn hành động khắc phục.

19. Vai trò của "đánh giá nội bộ" (Internal Audit) trong ISMS theo ISO 27001 là gì?

a) Để kiểm tra xem nhân viên có đi làm đúng giờ không.

b) Để xác minh một cách độc lập xem các hoạt động và kết quả liên quan đến ISMS có tuân thủ các sắp xếp đã hoạch định (chính sách, quy trình, tiêu chuẩn) và có được thực hiện hiệu quả hay không.

c) Để đánh giá hiệu quả marketing.

d) Để cấp chứng chỉ ISO 27001.

20. Tại sao việc "xem xét của lãnh đạo" (Management Review) lại cần thiết cho sự thành công của ISMS?

a) Để lãnh đạo ký duyệt các hóa đơn.

b) Để kiểm tra email của nhân viên.

c) Để đảm bảo ISMS tiếp tục phù hợp, đầy đủ và hiệu quả; đưa ra các quyết định về cơ hội cải tiến và nhu cầu thay đổi ISMS, bao gồm chính sách và mục tiêu.

d) Để tổ chức tiệc ăn mừng.

Mục 5.3: Pháp luật và chính sách ATTT

1. Pháp luật về an toàn thông tin (ATTT) nhằm mục đích gì?

a) Chỉ để phạt các công ty công nghệ.

b) Quy định các hành vi được phép và không được phép liên quan đến thông tin và hệ thống thông tin, bảo vệ quyền lợi của cá nhân và tổ chức.

c) Khuyến khích việc chia sẻ thông tin cá nhân.

d) Giảm bớt các quy định về bảo mật.

2. Chính sách ATTT của một tổ chức là gì?

a) Một văn bản mô tả cấu trúc mạng.

b) Danh sách các phần mềm được phép cài đặt.

c) Các quy định, nguyên tắc và hướng dẫn cấp cao do ban lãnh đạo ban hành để định hướng việc bảo vệ tài sản thông tin.

d) Kế hoạch sao lưu dữ liệu hàng ngày.

3. Tại sao các tổ chức cần có chính sách ATTT?

a) Để làm phức tạp thêm công việc của nhân viên.

b) Để thiết lập các kỳ vọng rõ ràng về hành vi, trách nhiệm và cung cấp cơ sở cho việc thực thi các biện pháp kiểm soát ATTT.

c) Để tăng chi phí hoạt động.

d) Để lưu trữ mật khẩu của người dùng.

4. Luật An toàn thông tin mạng của Việt Nam được Quốc hội thông qua vào năm nào?

a) 2005

b) 2009

c) 2015

d) 2019

5. Hành vi nào sau đây thường bị cấm bởi pháp luật về ATTT?

a) Sử dụng mạng xã hội.

b) Gửi email cho đồng nghiệp.

c) Truy cập trái phép vào hệ thống máy tính của người khác.

d) Đọc tin tức trực tuyến.

6. Quyền riêng tư (Privacy) liên quan đến ATTT như thế nào?

a) Không liên quan gì đến ATTT.

b) ATTT là một phần quan trọng để bảo vệ quyền riêng tư, đảm bảo thông tin cá nhân không bị truy cập, sử dụng hoặc tiết lộ trái phép.

c) Quyền riêng tư chỉ áp dụng cho thông tin trên giấy.

d) ATTT làm giảm quyền riêng tư.

7. Luật pháp quốc tế về ATTT thường giải quyết các vấn đề nào?

a) Chỉ quy định về tốc độ Internet.

b) Chỉ quy định về tên miền.

c) Tội phạm mạng xuyên biên giới, bảo vệ dữ liệu cá nhân, sở hữu trí tuệ và hợp tác quốc tế trong điều tra.

d) Chỉ quy định về kích thước màn hình máy tính.

8. "Sở hữu trí tuệ" (Intellectual Property) trong bối cảnh ATTT bao gồm những gì?

a) Chỉ bao gồm phần cứng máy tính.

b) Các sản phẩm do trí tuệ con người tạo ra như phần mềm, mã nguồn, tác phẩm văn học nghệ thuật, bí mật kinh doanh được lưu trữ hoặc xử lý bằng hệ thống thông tin.

c) Chỉ bao gồm tên miền website.

d) Chỉ bao gồm mật khẩu người dùng.

9. Sự khác biệt giữa Luật (Law) và Chính sách (Policy) là gì?

a) Chính sách có tính bắt buộc cao hơn Luật.

b) Luật do cơ quan lập pháp ban hành, áp dụng rộng rãi và có chế tài pháp lý; Chính sách do tổ chức ban hành, áp dụng trong phạm vi tổ chức và có chế tài nội bộ.

c) Luật chỉ áp dụng cho cá nhân, Chính sách chỉ cho tổ chức.

d) Không có sự khác biệt nào.

10. Luật An ninh mạng của Việt Nam (2018) tập trung vào những khía cạnh nào khác biệt so với Luật ATTT mạng (2015)?

a) Chỉ tập trung vào mã hóa.

b) Nhấn mạnh hơn vào bảo vệ an ninh quốc gia trên không gian mạng, phòng chống khủng bố mạng, xử lý thông tin xấu độc và yêu cầu lưu trữ dữ liệu tại Việt Nam đối với một số nhà cung cấp dịch vụ.

c) Chỉ quy định về chữ ký số.

d) Bãi bỏ hoàn toàn Luật ATTT mạng 2015.

11. Tại sao việc tuân thủ pháp luật và quy định (Compliance) lại quan trọng đối với các tổ chức?

a) Chỉ để tránh bị phạt tiền.

b) Để tránh các chế tài pháp lý (phạt tiền, truy tố hình sự), bảo vệ uy tín, duy trì lòng tin của khách hàng và đảm bảo hoạt động kinh doanh bền vững.

c) Để được giảm thuế.

d) Để được quảng cáo miễn phí.

12. Một số luật của Mỹ có ảnh hưởng quốc tế đến ATTT bao gồm những luật nào?

a) Chỉ có luật về giao thông đường bộ.

b) Chỉ có luật về bầu cử tổng thống.

c) Ví dụ như DMCA (Digital Millennium Copyright Act) liên quan đến bản quyền số, HIPAA (Health Insurance Portability and Accountability Act) liên quan đến thông tin y tế.

d) Chỉ có luật về sở hữu súng.

13. Điều gì xảy ra nếu một tổ chức không tuân thủ các quy định về bảo vệ dữ liệu cá nhân (ví dụ: GDPR của EU)?

a) Không có gì xảy ra.

b) Chỉ bị cảnh cáo bằng lời nói.

c) Có thể đối mặt với các khoản phạt tài chính rất lớn, kiện tụng và tổn hại nghiêm trọng về uy tín.

d) Được chính phủ khen thưởng.

14. Vai trò của "Chính sách sử dụng chấp nhận được" (Acceptable Use Policy - AUP) là gì?

a) Quy định về trang phục công sở.

b) Xác định các hành vi được và không được phép khi sử dụng tài nguyên công nghệ thông tin của tổ chức (mạng, máy tính, email, internet).

c) Hướng dẫn cách cài đặt phần mềm.

d) Mô tả quy trình báo cáo sự cố.

15. Tại sao cần có sự hợp tác quốc tế trong việc chống tội phạm mạng?

a) Vì tội phạm mạng chỉ xảy ra ở một quốc gia.

b) Vì tội phạm mạng thường có tính chất xuyên biên giới, đòi hỏi sự phối hợp giữa các quốc gia trong việc chia sẻ thông tin, điều tra và truy bắt tội phạm.

c) Để các quốc gia cạnh tranh với nhau.

d) Vì luật pháp các nước giống hệt nhau.

16. Luật Giao dịch điện tử của Việt Nam quy định về vấn đề gì liên quan đến ATTT?

a) Chỉ quy định về tốc độ mạng.

b) Công nhận giá trị pháp lý của thông điệp dữ liệu, chữ ký điện tử, hợp đồng điện tử và các yêu cầu đảm bảo an toàn trong giao dịch điện tử.

c) Chỉ quy định về quảng cáo trực tuyến.

d) Quy định về việc sử dụng mạng xã hội.

17. Thách thức chính trong việc thực thi pháp luật đối với tội phạm mạng xuyên biên giới là gì?

a) Thiếu máy tính để điều tra.

b) Sự khác biệt về hệ thống pháp luật giữa các quốc gia, khó khăn trong việc thu thập bằng chứng điện tử ở nước ngoài và vấn đề về quyền tài phán.

c) Tội phạm mạng không sử dụng internet.

d) Ngôn ngữ lập trình quá phức tạp.

18. Tại sao việc cân bằng giữa an ninh quốc gia và quyền riêng tư của công dân lại là một vấn đề phức tạp trong pháp luật về ATTT/An ninh mạng?

a) Vì hai khái niệm này hoàn toàn giống nhau.

b) Vì các biện pháp tăng cường an ninh (như giám sát) có thể xâm phạm quyền riêng tư, đòi hỏi phải có cơ chế pháp lý rõ ràng, minh bạch và kiểm soát chặt chẽ để tránh lạm dụng.

c) Vì quyền riêng tư không quan trọng bằng an ninh quốc gia.

d) Vì công nghệ không đủ khả năng để thực hiện cả hai.

19. "Safe Harbor" hoặc "Privacy Shield" (nay đã bị vô hiệu hóa) là các cơ chế nhằm giải quyết vấn đề gì giữa EU và Mỹ?

a) Vấn đề về thuế quan thương mại.

b) Đảm bảo các công ty Mỹ tuân thủ các tiêu chuẩn bảo vệ dữ liệu cá nhân tương đương với EU khi truyền dữ liệu từ EU sang Mỹ.

c) Vấn đề về bản quyền phần mềm.

d) Vấn đề về tiêu chuẩn khí thải.

20. Luật pháp thường phải đối mặt với thách thức nào khi cố gắng bắt kịp với sự phát triển nhanh chóng của công nghệ và các hình thức tấn công mạng mới?

a) Luật pháp luôn đi trước công nghệ.

b) Công nghệ không thay đổi nên luật pháp không cần cập nhật.

c) Tốc độ phát triển công nghệ và các kỹ thuật tấn công mới thường nhanh hơn quá trình xây dựng và sửa đổi luật, khiến luật có thể trở nên lạc hậu hoặc không bao quát hết các tình huống mới.

d) Các nhà lập pháp không sử dụng máy tính.

Mục 5.4: Vấn đề đạo đức an toàn thông tin

1. Đạo đức (Ethics) trong an toàn thông tin đề cập đến điều gì?

a) Chỉ các quy định pháp luật.

b) Các nguyên tắc và chuẩn mực hành vi đúng đắn liên quan đến việc sử dụng và bảo vệ thông tin, hệ thống thông tin.

c) Chỉ các tiêu chuẩn kỹ thuật.

d) Chỉ hiệu suất của hệ thống.

2. Tại sao vấn đề đạo đức lại quan trọng trong lĩnh vực ATTT?

a) Vì nó giúp tăng lợi nhuận.

b) Vì nó làm cho hệ thống chạy nhanh hơn.

c) Vì các quyết định và hành động liên quan đến ATTT có thể ảnh hưởng lớn đến cá nhân, tổ chức và xã hội.

d) Vì nó là yêu cầu để được cấp chứng chỉ.

3. Hành vi nào sau đây được coi là phi đạo đức trong ATTT?

a) Sử dụng mật khẩu mạnh.

b) Cập nhật phần mềm thường xuyên.

c) Theo dõi email cá nhân của đồng nghiệp mà không được phép.

d) Báo cáo một lỗ hổng bảo mật cho quản trị viên.

4. Một trong những nguyên tắc đạo đức cơ bản trong ATTT là gì?

a) Chia sẻ thông tin cá nhân của người khác càng nhiều càng tốt.

b) Tôn trọng quyền riêng tư và bảo mật thông tin của người khác.

c) Khai thác mọi lỗ hổng tìm thấy để trục lợi cá nhân.

d) Sao chép phần mềm có bản quyền mà không trả tiền.

5. "(ISC)² Code of Ethics" là bộ quy tắc đạo đức dành cho đối tượng nào?

a) Chỉ dành cho luật sư.

b) Chỉ dành cho bác sĩ.

c) Các chuyên gia an toàn thông tin được chứng nhận bởi (ISC)².

d) Chỉ dành cho kế toán viên.

6. Một điều khoản trong bộ quy tắc đạo đức của (ISC)² yêu cầu các chuyên gia phải làm gì?

a) Luôn đặt lợi ích cá nhân lên trên hết.

b) Hành động một cách trung thực, công bằng, có trách nhiệm và hợp pháp.

c) Chia sẻ thông tin bí mật của khách hàng với đối thủ cạnh tranh.

d) Bẻ khóa hệ thống của người khác để kiểm tra kỹ năng.

7. "ACM Code of Ethics and Professional Conduct" là bộ quy tắc đạo đức của tổ chức nào?

a) Tổ chức Y tế Thế giới (WHO).

b) Liên Hợp Quốc (UN).

c) Association for Computing Machinery (Hiệp hội Máy tính).

d) Tổ chức Thương mại Thế giới (WTO).

8. Tại sao việc sử dụng tài sản công nghệ thông tin của công ty cho mục đích cá nhân lại có thể bị coi là vấn đề đạo đức?

a) Vì nó làm máy tính chạy chậm.

b) Vì đó có thể là sự lạm dụng tài nguyên của tổ chức, vi phạm chính sách và có thể gây ra rủi ro bảo mật.

c) Vì công ty không thích nhân viên giải trí.

d) Vì nó tốn điện.

9. Tình huống khó xử về đạo đức (Ethical Dilemma) trong ATTT là gì?

a) Lựa chọn giữa hai phần mềm diệt virus tốt.

b) Tình huống mà một chuyên gia phải lựa chọn giữa hai hoặc nhiều hành động, trong đó mỗi hành động đều có thể vi phạm một nguyên tắc đạo đức nào đó.

c) Quyết định nên sử dụng mật khẩu dài bao nhiêu ký tự.

d) Lựa chọn giữa việc sao lưu dữ liệu hàng ngày hay hàng tuần.

10. Ví dụ về một tình huống khó xử về đạo đức trong ATTT?

a) Có nên cài đặt bản vá bảo mật hay không.

b) Phát hiện một lỗ hổng nghiêm trọng trong sản phẩm của công ty, nhưng việc công bố có thể gây thiệt hại lớn về tài chính và uy tín, trong khi việc che giấu có thể khiến khách hàng gặp rủi ro.

c) Nên sử dụng mạng Wi-Fi công cộng hay mạng di động.

d) Có nên xóa các file tạm thời hay không.

11. Tại sao việc phân biệt giữa hành vi phi đạo đức và hành vi bất hợp pháp lại quan trọng?

a) Vì chúng luôn luôn giống nhau.

b) Vì một hành vi có thể phi đạo đức nhưng không bất hợp pháp (hoặc ngược lại), và việc hiểu rõ sự khác biệt giúp xác định cách xử lý phù hợp.

c) Vì hành vi phi đạo đức không bao giờ bị xử lý.

d) Vì hành vi bất hợp pháp luôn được chấp nhận về mặt đạo đức.

12. Trách nhiệm đạo đức của một chuyên gia ATTT khi phát hiện hoạt động bất hợp pháp hoặc phi đạo đức trong tổ chức của mình là gì?

a) Hoàn toàn phớt lờ nó.

b) Tham gia vào hoạt động đó.

c) Cân nhắc các nghĩa vụ đối với tổ chức, công chúng và nghề nghiệp, có thể bao gồm việc báo cáo thông qua các kênh thích hợp theo chính sách và pháp luật.

d) Đăng thông tin lên mạng xã hội ngay lập tức.

13. "Computer Ethics Institute" đã đưa ra 10 điều răn về đạo đức máy tính. Một trong số đó là gì?

a) Bạn nên sử dụng máy tính để làm hại người khác.

b) Bạn không nên sử dụng tài nguyên máy tính của người khác mà không được phép hoặc không bồi thường thích đáng.

c) Bạn nên xem trộm các tập tin của người khác.

d) Bạn nên sao chép phần mềm có bản quyền bất cứ khi nào có thể.

14. Vấn đề đạo đức liên quan đến việc thu thập và sử dụng dữ liệu người dùng (ví dụ: bởi các công ty công nghệ lớn) là gì?

a) Việc thu thập dữ liệu giúp máy tính chạy nhanh hơn.

b) Mối lo ngại về quyền riêng tư, sự minh bạch trong việc thu thập, mục đích sử dụng dữ liệu và khả năng lạm dụng thông tin cá nhân.

c) Dữ liệu người dùng không có giá trị.

d) Việc thu thập dữ liệu luôn luôn hợp pháp.

15. Tại sao việc đào tạo nhận thức về đạo đức ATTT cho nhân viên lại cần thiết?

a) Để nhân viên biết cách hack hệ thống.

b) Để giúp nhân viên hiểu các nguyên tắc hành xử đúng đắn, nhận diện các tình huống rủi ro về đạo đức và biết cách hành động phù hợp.

c) Để tăng thời gian làm việc của nhân viên.

d) Để thay thế cho các biện pháp kiểm soát kỹ thuật.

16. Mối quan hệ giữa văn hóa tổ chức và đạo đức ATTT là gì?

a) Không có mối quan hệ nào.

b) Một văn hóa tổ chức coi trọng sự trung thực, trách nhiệm và minh bạch sẽ thúc đẩy hành vi đạo đức trong ATTT và ngược lại.

c) Văn hóa tổ chức chỉ liên quan đến trang phục.

d) Đạo đức ATTT quyết định văn hóa tổ chức.

17. Thách thức trong việc áp dụng các bộ quy tắc đạo đức ATTT mang tính toàn cầu vào các nền văn hóa khác nhau là gì?

a) Các bộ quy tắc này chỉ viết bằng tiếng Anh.

b) Các chuẩn mực và giá trị đạo đức có thể khác biệt giữa các nền văn hóa, dẫn đến sự diễn giải và ưu tiên khác nhau đối với các nguyên tắc đạo đức chung.

c) Công nghệ ở các nước khác nhau là hoàn toàn khác biệt.

d) Không có thách thức nào cả.

18. Khi một công nghệ mới (ví dụ: AI, IoT) phát triển, những vấn đề đạo đức mới nào có thể nảy sinh trong lĩnh vực ATTT?

a) Công nghệ mới luôn giải quyết mọi vấn đề đạo đức cũ.

b) Các vấn đề liên quan đến thiên vị thuật toán (algorithmic bias), quyền riêng tư trong môi trường kết nối liên tục, trách nhiệm giải trình của hệ thống tự động, và khả năng lạm dụng công nghệ cho mục đích xấu.

c) Công nghệ mới làm cho ATTT trở nên đơn giản hơn về mặt đạo đức.

d) Không có vấn đề đạo đức mới nào nảy sinh.

19. Tại sao việc cân nhắc "lợi ích công cộng" (Public Good) lại quan trọng trong các quyết định về đạo đức ATTT?

a) Vì lợi ích công cộng không liên quan đến ATTT.

b) Vì các quyết định về ATTT (ví dụ: tiết lộ lỗ hổng, chia sẻ thông tin về mối đe dọa) có thể ảnh hưởng đến sự an toàn và phúc lợi của cả cộng đồng, không chỉ riêng cá nhân hay tổ chức.

c) Vì chỉ có chính phủ mới quan tâm đến lợi ích công cộng.

d) Vì lợi ích công cộng luôn đối lập với lợi ích của tổ chức.

20. Vai trò của các tổ chức nghề nghiệp (như (ISC)², ACM, ISACA) trong việc thúc đẩy đạo đức ATTT là gì?

a) Chỉ để thu phí thành viên.

b) Chỉ để tổ chức các cuộc thi hack.

c) Xây dựng và duy trì các bộ quy tắc đạo đức, cung cấp đào tạo, chứng nhận và tạo diễn đàn thảo luận, góp phần nâng cao chuẩn mực hành vi và trách nhiệm nghề nghiệp trong cộng đồng ATTT.

d) Chỉ để bán sách giáo trình.