NỘI DUNG ÔN TẬP MÔN TRIỂN KHAI AN NINH HỆ THỐNG

Bài thu hoạch thực hành cuối kì

Phúc Lâm - TH09 – 03/11/2024

Yêu cầu:

Để chuẩn bị tốt cho thi cuối kỳ sắp tới, các em ôn tập vào các nội dung trọng điểm sau (dựa trên các LO - chuẩn đầu ra của môn học):

1. **Xác định và giải thích được các mối nguy hiểm với một hệ thống cho trước**
    a. Yêu cầu: Cho 1 sơ đồ hệ thống mạng, sinh viên phân tích và xác định được 3 mối nguy hiểm khác nhau. Làm cơ sở cho nội dung 2:
2. **Vẽ và giải thích được sơ đồ mạng an toàn cho một tình huống cụ thể (DMZ, Firewall, Digital signature)**
    a. Yêu cầu: Sinh viên vẽ và giải thích được sơ đồ mạng đáp ứng an toàn cho các mối hiểm hoạ đã phân tích ở trên
3. **Giải thích được 1 số điều khoản liên quan đến quy tắc ứng xử ACM và vi phạm luật an ninh mạng đối với tình huống cụ thể**

Yêu cầu: Dựa vào hành động của người tham gia hệ thống CNTT trong một tình huống cụ thể, sinh viên phân tích người đó vi phạm điều khoản nào trong bộ quy tắc ứng xử ACM và vi phạm luật an ninh mạng và hình thức bị xử lý.

CLOs	Chuẩn đầu ra của học phần	SO/PI
1	Thiết kế các thành phần bảo mật trong hệ thống mạng.	**2**
2	Vận dụng nguyên lý bảo mật de xác định các giải pháp bảo mật trong hệ thống mạng	**1**
3	Phân tích được tác động của an ninh hệ thống tại đơn vị hiện tại đến cá nhân, tổ chức, xã hội	**4**

MỤC LỤC

LO1 + LO2 XÁC ĐỊNH VÀ GIẢI THÍCH ĐƯỢC CÁC MỐI NGUY HIỂM VỚI HỆ THỐNG CHO TRƯỚC.

I. Hiểm họa, rủi ro, tấn công và lỗ hổng là gì?

Hiểm họa, rủi ro, tấn công và lỗ hổng là những khái niệm cốt lõi của an toàn thông tin. Tuy nhiên, các thuật này thường xuyên bị sử dụng nhầm lẫn và chồng chéo lẫn nhau. Mặc dù, có những mối liên hệ nhất định giữa các khái niệm này, nhưng chúng là các thuật ngữ riêng biệt với ý nghĩa khác nhau.

1.1. Hiểm họa

Hiểm họa là những khả năng gây hại cho hệ thống thông tin, có thể làm thay đổi, hư hại, hoặc gián đoạn dữ liệu. Hiểm họa có thể xuất phát từ tự nhiên (như thiên tai), lỗi không chủ ý (như thao tác sai của nhân viên), hoặc từ tấn công có chủ đích (như mã độc, tấn công mạng).

Chúng có thể xuất phát từ:

- **Tự nhiên**: Bão, lũ lụt.
- **Không chủ ý**: Lỗi của nhân viên, quản trị viên cấu hình sai.
- **Có chủ ý**: Tấn công mạng, mã độc, lừa đảo, kỹ nghệ xã hội.

Ví dụ: Cuộc tấn công WannaCry năm 2017 là một hiểm họa lớn đối với các hệ thống máy tính toàn cầu.

1.2. Lỗ hổng

Lỗ hổng là các điểm yếu hoặc thiếu sót trong hệ thống, phần mềm hoặc quy trình, tạo cơ hội cho hiểm họa khai thác. Các lỗ hổng phổ biến bao gồm lỗi bảo mật phần mềm (như SQL Injection), cấu hình sai, hoặc thiếu các biện pháp bảo vệ như tường lửa.

Lỗ hổng là điểm yếu trong hệ thống có thể bị khai thác để gây hại, ví dụ:

- **Phần mềm**: SQL Injection, XSS.
- **Cấu hình sai**: Máy chủ không bảo mật, truyền dữ liệu không mã hóa.
- **Vật lý**: Thiếu bảo mật tại các trung tâm dữ liệu.

1.3. Rủi ro

Rủi ro là khả năng thiệt hại xảy ra khi một hiểm họa khai thác thành công lỗ hổng của hệ thống. Rủi ro có thể dẫn đến mất mát tài chính, tổn thất dữ liệu, hoặc ảnh hưởng đến uy tín của tổ chức.

Rủi ro = Hiểm họa × Lỗ hổng
Mức độ rủi ro = Xác xuất xảy ra rủi ro × Thiệt hại ước tính

1.4. Tấn công

Tấn công là hành vi cố ý nhằm khai thác các lỗ hổng để gây hại cho hệ thống. Ví dụ, một cuộc tấn công mạng có thể nhắm đến việc đánh cắp dữ liệu nhạy cảm hoặc phá hoại hoạt động của tổ chức.

Tấn công là hành động khai thác lỗ hổng để gây hại cho hệ thống, bao gồm:

- **Tấn công vật lý**: Phá hoại thiết bị.
- **Tấn công mạng**: SQL Injection, XSS, DDoS.

II. PHÂN TÍCH MỐI HIỂM HỌA ĐE DỌA AN NINH HỆ THỐNG

2.1. Các sơ đồ trên sẽ tiềm ẩn các mối hiểm hoạ như:

Các sơ đồ sau đây được cho là không bảo đảm an toàn, tiềm ẩn nhiều mối hiểm hoạ đe doạ an ninh hệ thống:

1- Hệ thống chưa cho thấy có giải pháp khi mất dữ liệu xảy ra

2- Do không có tường lửa kiểm soát truy cập tập trung nên người dùng bên trong hệ thống dễ bị nhiễm ransomware

3- Sơ đồ 1, 2, 3: Nếu đường mạng interet bị mất kết nối thì toàn bộ hệ thống bị gián đoạn kết nối internet.

4- Do không có lớp tường lửa bảo vệ giám sát nên các máy tính bên trong dễ dàng truy cập tới các địa chỉ không tin cậy bên ngoài và dễ bị ăn cắp thông tin

5- Server không được bảo vệ bởi Firewall nên hacker bên ngoài có thể tấn công trực diện

6- Kẻ tấn công có thể sử dụng các công cụ hack wifi và thực hiện tấn công ARP rồi sử dụng Packet Sniffing để ăn cắp thông tin.

7- Thiếu hệ thống sao lưu dữ liệu: Nếu không có hệ thống sao lưu định kỳ và khôi phục dữ liệu (backup & recovery), dữ liệu có thể bị mất vĩnh viễn trong trường hợp hệ thống bị tấn công, sự cố phần cứng, hoặc lỗi con người.

8- Không có giải pháp phát hiện và ngăn chặn xâm nhập (IDS/IPS): Điều này tạo điều kiện cho các cuộc tấn công như SQL Injection, XSS (Cross-Site Scripting) và tấn công zero-day mà không bị phát hiện và ngăn chặn kịp thời.

9- Thiếu hệ thống phân tích lưu lượng mạng: Không giám sát lưu lượng mạng khiến các hành vi bất thường không bị phát hiện kịp thời, cho phép hacker âm thầm truy cập dữ liệu trong thời gian dài mà không ai hay biết.

10- Thiếu kiểm soát băng thông: Khi không có thiết bị quản lý băng thông, việc tiêu tốn băng thông quá mức có thể làm nghẽn mạng và gây gián đoạn các dịch vụ quan trọng, cũng dễ bị tấn công DoS (Từ chối dịch vụ).

11- Thiếu hệ thống xác thực đa yếu tố (MFA): Thiếu xác thực đa yếu tố khiến hệ thống dễ bị truy cập trái phép, nhất là khi mật khẩu bị lộ hoặc bị hack.

12- Không có cơ chế quản lý truy cập thiết bị: Các thiết bị không bảo mật có thể truy cập tự do vào mạng nội bộ, dễ gây rủi ro lây nhiễm mã độc từ các thiết bị nhiễm phần mềm độc hại.

13- Thiếu giám sát và bảo mật thiết bị IoT: Các thiết bị IoT, camera, cảm biến không được bảo vệ kỹ có thể bị hacker tấn công và biến thành điểm xâm nhập, cho phép hacker theo dõi hoặc điều khiển các thiết bị.

14- Không có giải pháp kiểm soát nội dung: Người dùng có thể truy cập các trang web hoặc tải các file không an toàn, dễ bị nhiễm phần mềm độc hại hoặc lây lan ransomware.

2.2. Giải pháp:

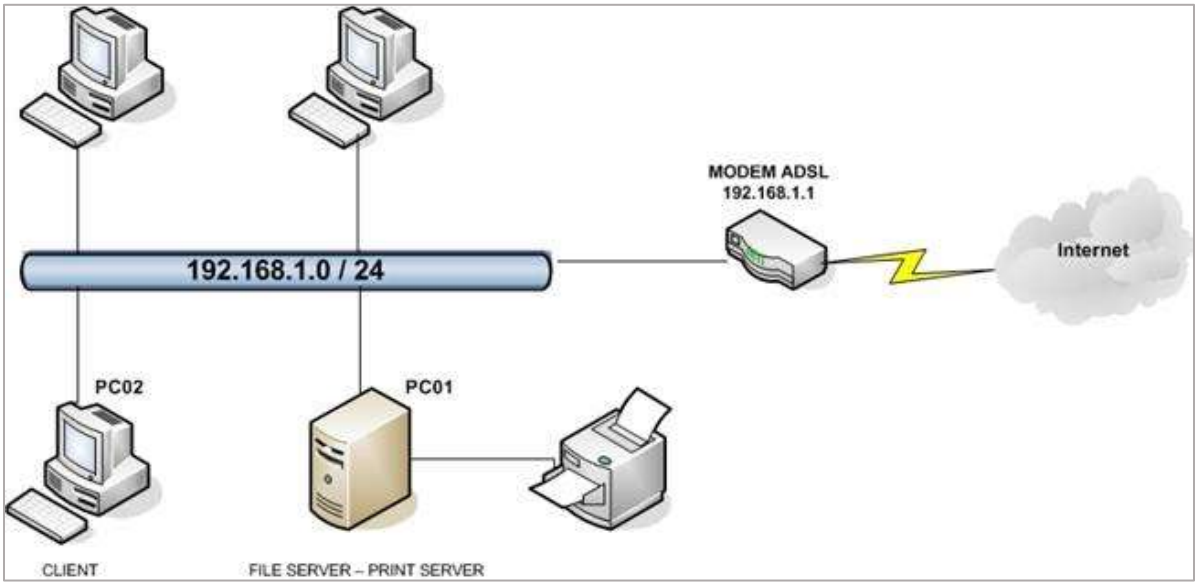
1- Tăng cường an ninh cho hệ thống với thiết lập các chính sách Policies cho mật khẩu
2- Thiết lập tường lửa để bảo vệ, thiết lập vùng DMZ đưa Server vào vùng DMZ.
3- Tăng cường bảo mật email với ứng dụng Digital signature
4- Thiết lập hệ thống giám sát mạng bằng Zabbix server
5- Xây dựng Domain Controller để quản trị xác thực người dùng tập trung
6- Sử dụng Wifi Controller để tăng cường kiểm soát Wifi
7- Thêm đường kết nối internet để gia tăng tính sẵn sàng High Availability (HA)
8- Thiết lập hệ thống sao lưu và khôi phục dữ liệu tự động: Đảm bảo sao lưu định kỳ và thử nghiệm khôi phục dữ liệu để tránh mất mát vĩnh viễn.
9- Triển khai hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Giúp phát hiện sớm các cuộc tấn công và ngăn chặn xâm nhập bất hợp pháp.
10- Thiết lập hệ thống phân tích lưu lượng mạng: Sử dụng công cụ như Wireshark hoặc Splunk để phân tích các mẫu lưu lượng và phát hiện dấu hiệu bất thường.
11- Quản lý băng thông: Cài đặt thiết bị quản lý băng thông để kiểm soát, đảm bảo lưu lượng truy cập không ảnh hưởng đến hiệu suất của các dịch vụ quan trọng.
12- Áp dụng xác thực đa yếu tố (MFA): Tăng cường bảo mật đăng nhập cho các tài khoản quan trọng bằng cách yêu cầu mã OTP hoặc thông báo qua ứng dụng di động.
13- Giám sát và quản lý truy cập thiết bị IoT: Thiết lập chính sách bảo mật cho thiết bị IoT và kiểm soát quyền truy cập từ các thiết bị này.
14- Cài đặt hệ thống kiểm soát nội dung: Sử dụng giải pháp như Web Filtering để chặn các trang web không an toàn và ngăn ngừa tải các file có khả năng chứa mã độc.
15- Đào tạo nhân viên về an ninh mạng: Tổ chức các khóa đào tạo định kỳ để nâng cao nhận thức về an toàn thông tin cho nhân viên, giảm thiểu rủi ro từ hành vi con người.
16- Xây dựng chính sách Backup thường xuyên và lưu trữ tại nhiều vị trí: Ngoài lưu trữ tại chỗ, cần lưu trữ bản sao ở trung tâm dữ liệu khác để đảm bảo khả năng khôi phục.

2.3. Một số lưu ý khi không trang bị thiết bị mạng

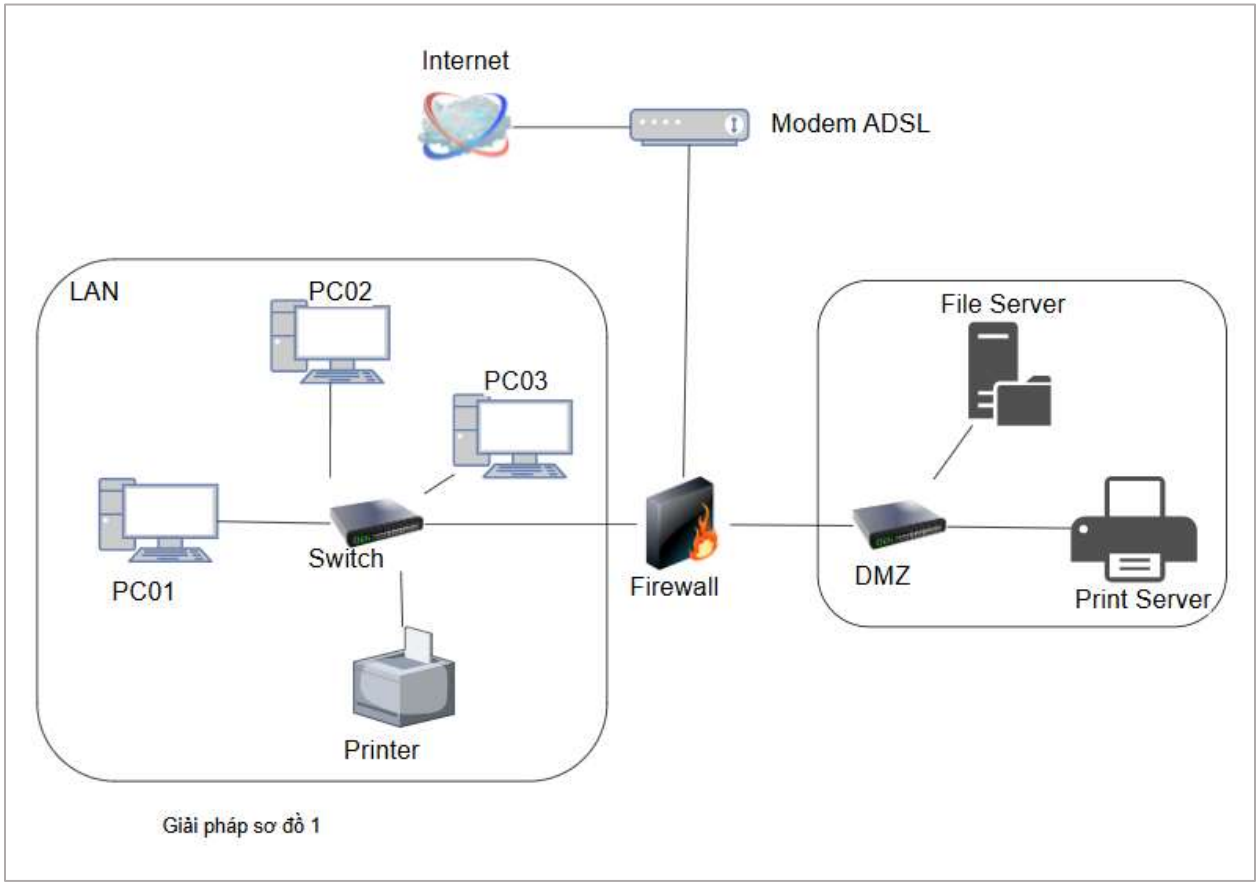
- **Router**: Nếu không có router, doanh nghiệp sẽ khó quản lý luồng dữ liệu ra/vào mạng, không thể kết nối mạng nội bộ với internet. Các rủi ro bao gồm mất khả năng giám sát lưu lượng từ internet, làm tăng nguy cơ tấn công từ bên ngoài và thiếu kiểm soát luồng dữ liệu.
- **Switch**: Thiếu switch sẽ hạn chế kết nối giữa các thiết bị trong mạng nội bộ, làm giảm hiệu suất kết nối và tăng rủi ro bị nghẽn dữ liệu tại các điểm truy cập đơn lẻ.
- **Access Point (AP)**: Thiếu AP sẽ gây gián đoạn kết nối không dây, khiến doanh nghiệp phải dựa vào kết nối dây. Người dùng có thể cố gắng tự tạo điểm truy cập không dây bằng các thiết bị cá nhân, dẫn đến lỗ hổng bảo mật (mạng "shadow IT").
- **Firewall**: Thiếu firewall để lại lỗ hổng lớn, cho phép các lưu lượng không được kiểm duyệt truy cập vào mạng. Các cuộc tấn công từ bên ngoài, như **tấn công từ chối dịch vụ (DDoS)**, **tấn công brute-force** hay **phát tán phần mềm độc hại**, có thể dễ dàng vượt qua rào cản bảo mật.
- **VPN Gateway**: Thiếu VPN khiến các kết nối từ xa không được mã hóa, tạo nguy cơ cho dữ liệu nhạy cảm bị đánh cắp qua các mạng công cộng, làm tăng khả năng bị **tấn công đánh cắp dữ liệu (man-in-the-middle)** và **lộ lọt thông tin**.
- **IDS/IPS**: Nếu không có hệ thống IDS/IPS, doanh nghiệp sẽ không phát hiện sớm các cuộc tấn công mạng, chẳng hạn như tấn công SQL Injection hoặc các mối đe dọa zero-day. Các cuộc tấn công có thể diễn ra trong thời gian dài mà không bị phát hiện.
- **Network Access Control (NAC)**: Thiếu NAC khiến việc quản lý thiết bị truy cập vào mạng trở nên khó khăn, dễ bị **tấn công từ nội bộ** hoặc từ các thiết bị lạ.
- **Server**: Không có server, doanh nghiệp sẽ thiếu nền tảng xử lý và lưu trữ dữ liệu, làm gián đoạn các dịch vụ quan trọng. Điều này tạo cơ hội cho các hành vi xâm nhập, truy cập trái phép, và đánh cắp thông tin nếu người dùng tìm cách lưu trữ tạm thời trên các thiết bị khác.

- **NAS/SAN**: Thiếu thiết bị lưu trữ chia sẻ dễ dẫn đến việc các tệp quan trọng bị phân tán không an toàn trên nhiều thiết bị cá nhân, làm tăng nguy cơ **mất mát dữ liệu** và **rò rỉ thông tin**.
- **Modem**: Không có modem sẽ không thể kết nối với Internet, nhưng doanh nghiệp có thể sử dụng các phương án thay thế không an toàn để kết nối tạm thời, chẳng hạn dùng điểm phát sóng từ thiết bị cá nhân, tạo cơ hội cho các cuộc tấn công man-in-the-middle.
- **Proxy Server**: Nếu thiếu proxy, doanh nghiệp không kiểm soát được truy cập và các trang web được phép truy cập. Các cuộc tấn công có thể dễ dàng xảy ra hơn thông qua các trang web không an toàn và phần mềm độc hại.

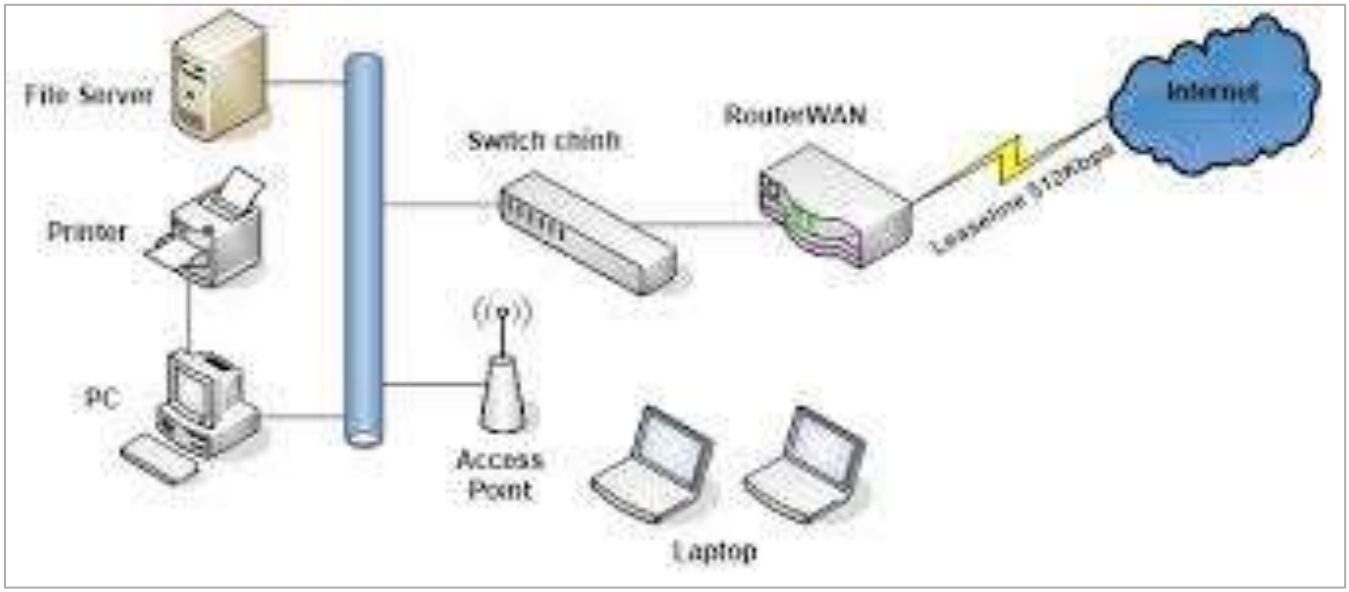
2.4.1. Sơ đồ 1:



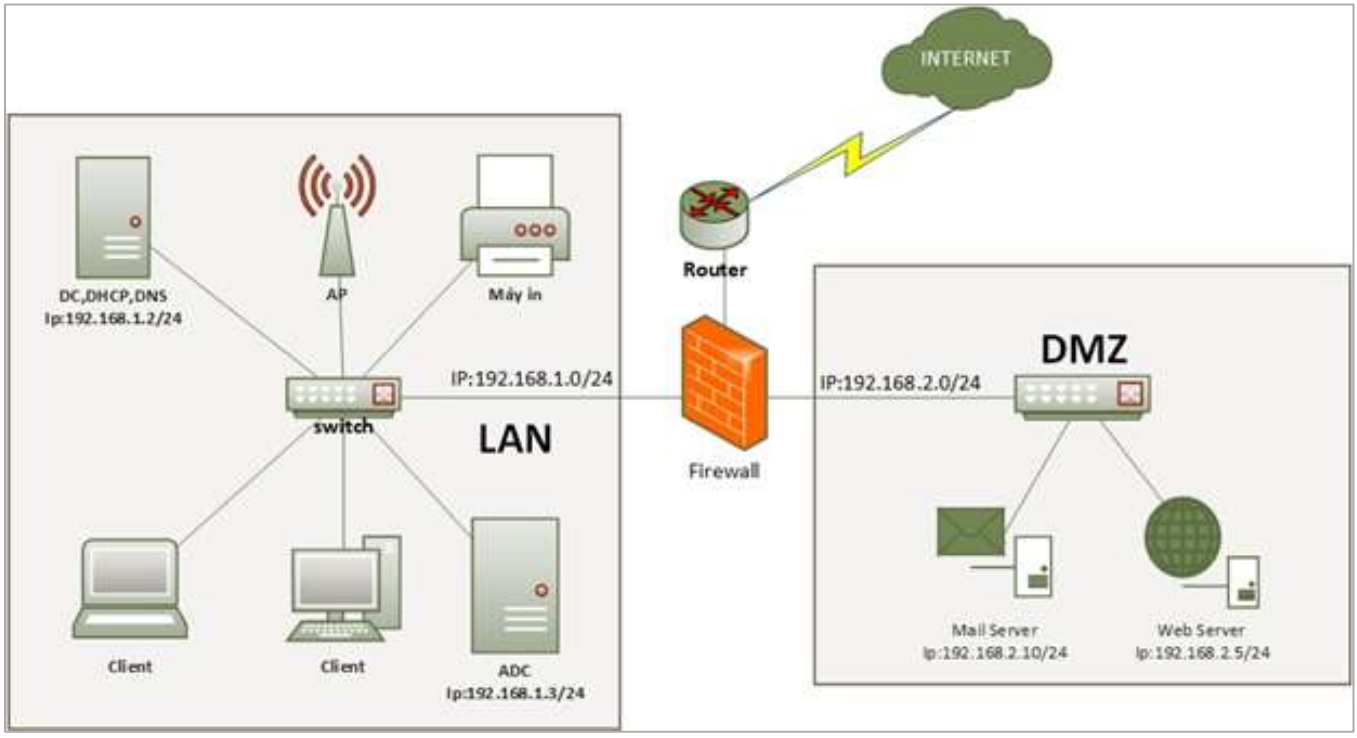
2.4.2. Giải pháp 1



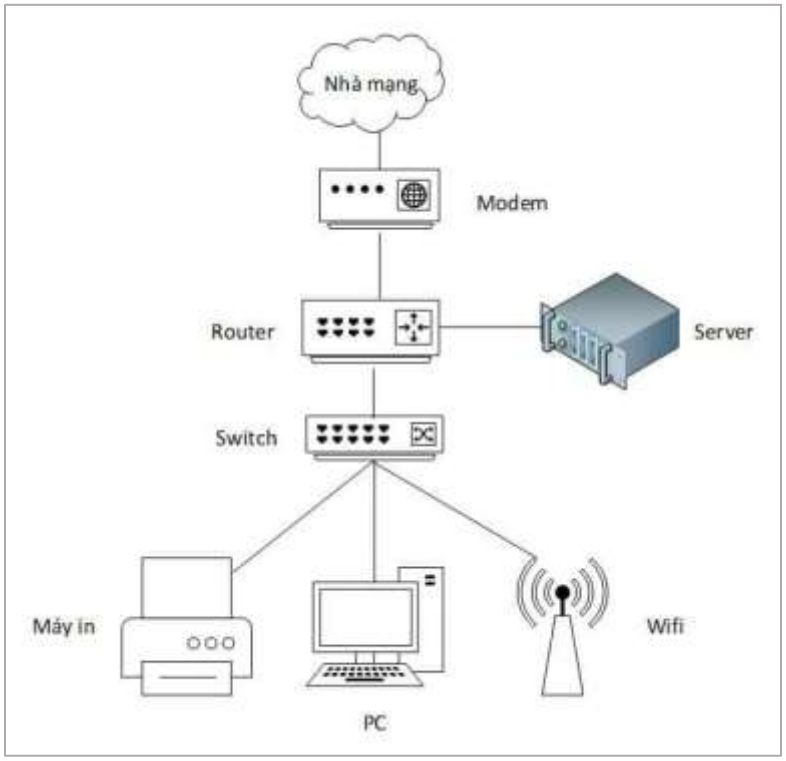
2.5.1. Sơ đồ 2



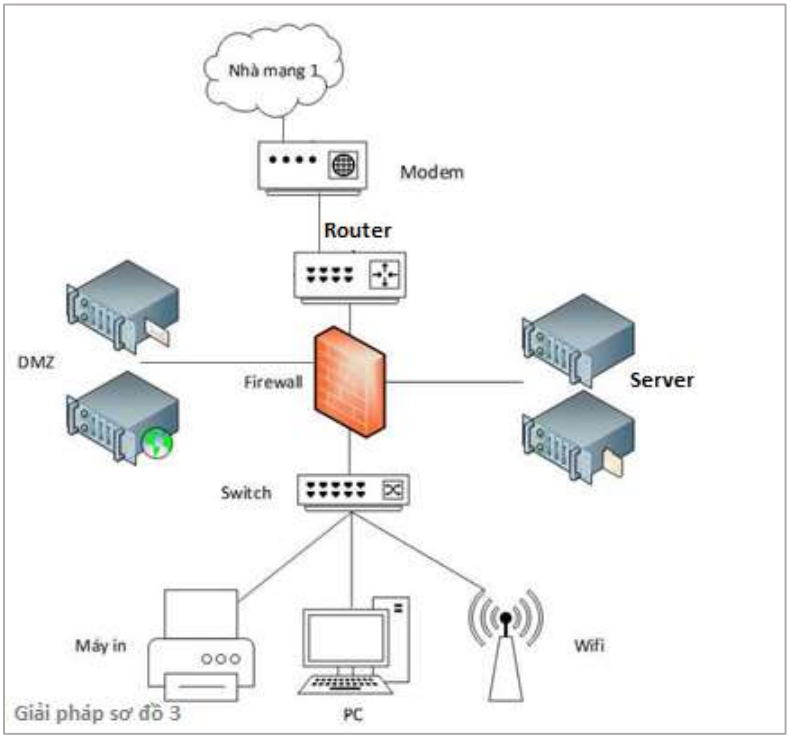
2.5.2. Giải pháp 2



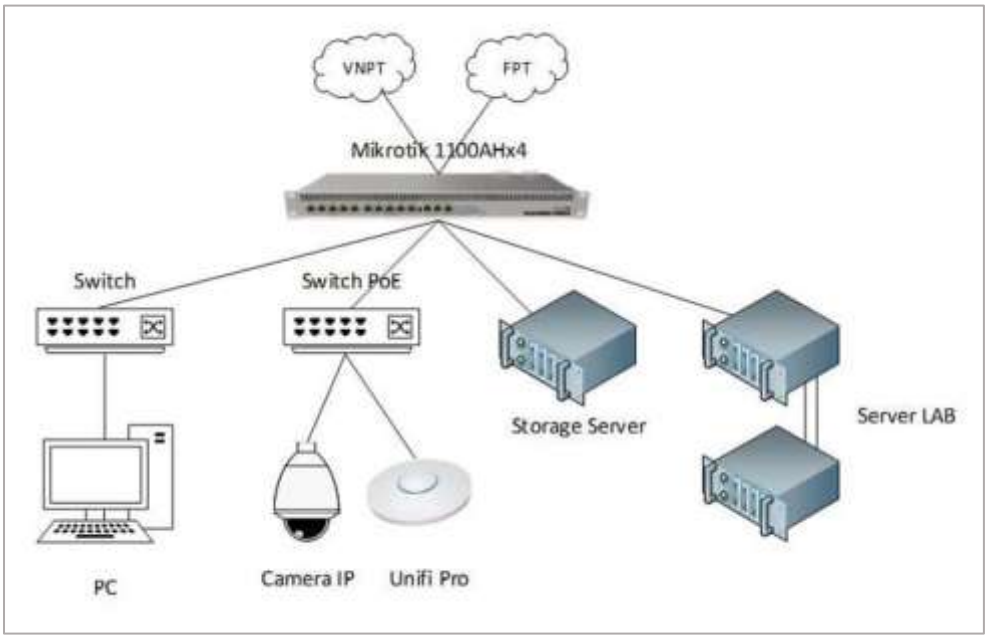
2.6.1. Sơ đồ 3



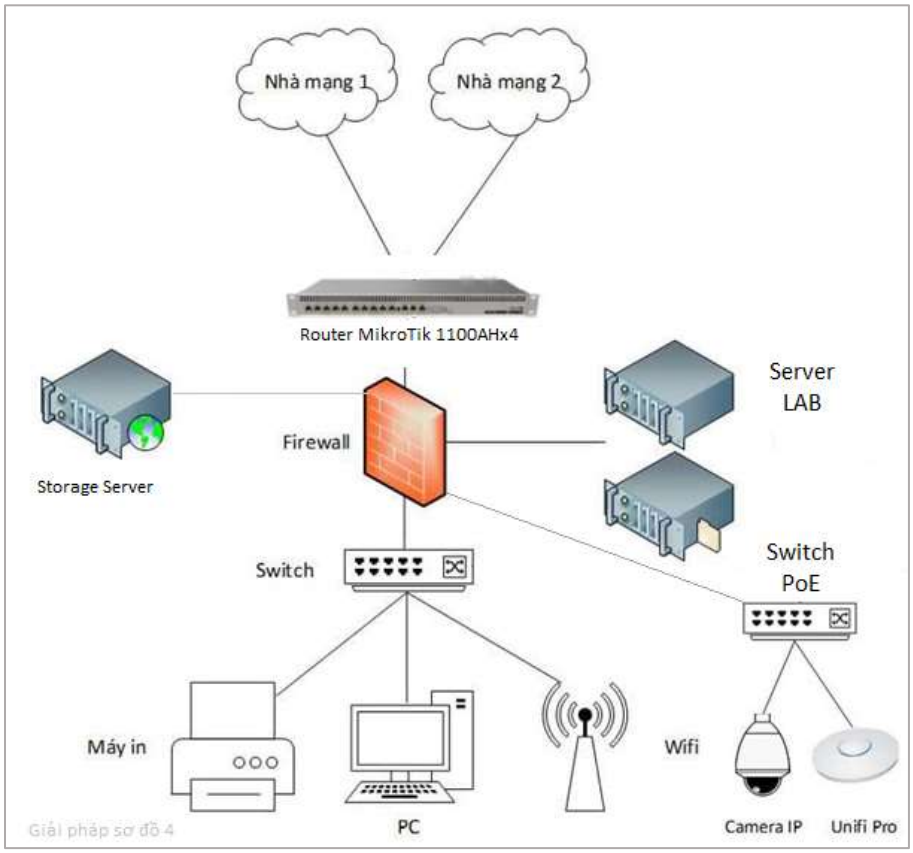
2.6.2. Giải pháp 3



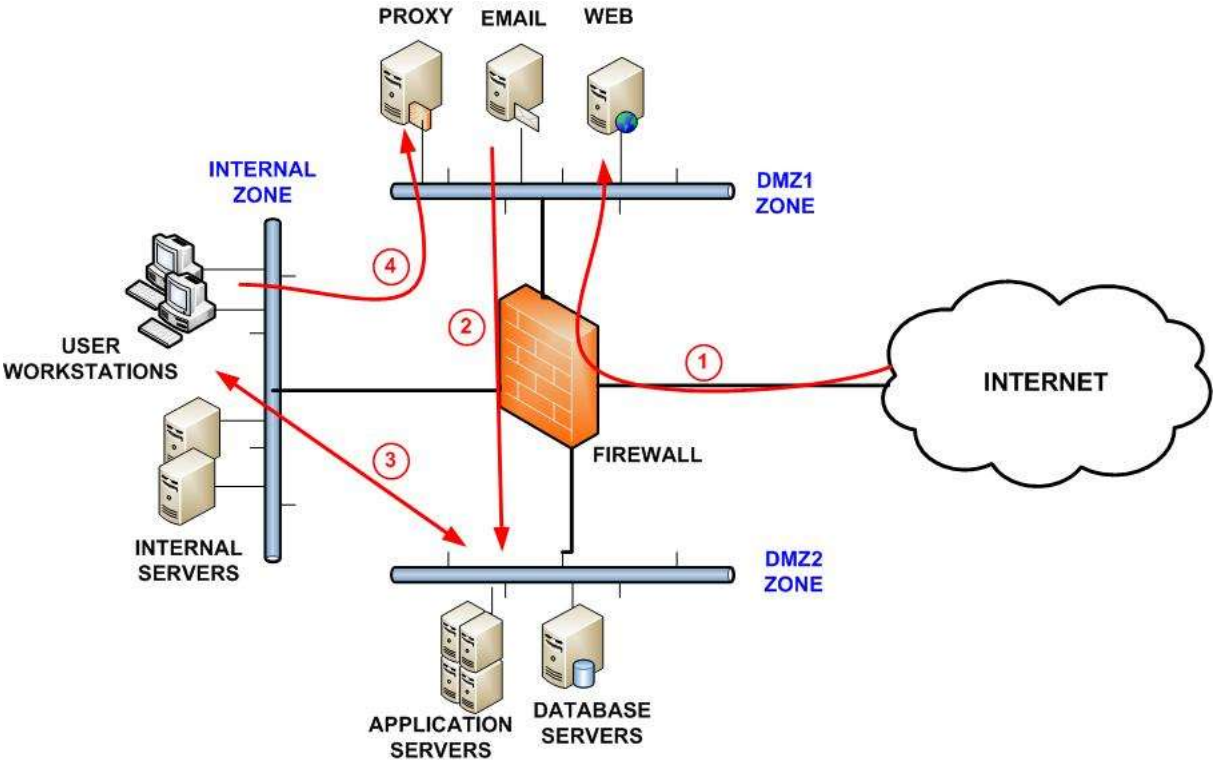
2.7.1. Sơ đồ 4



2.7.2. Giải pháp 4



2.8. Giải thích được tường lửa kiểm soát truy cập giữa các thành phần sơ đồ mạng:



1. **Bước 1: Từ Internet vào DMZ1 Zone**
    - Lưu lượng truy cập từ Internet đến DMZ1 Zone sẽ đi qua tường lửa để kiểm soát và giới hạn các kết nối vào các dịch vụ trong DMZ1, bao gồm Proxy, Email, và Web server.
    - Tường lửa sẽ áp dụng các quy tắc bảo mật để ngăn chặn các mối đe dọa từ Internet trước khi chúng có thể tiếp xúc với các dịch vụ trong DMZ1.
2. **Bước 2: Từ DMZ1 Zone đi vào DMZ2 Zone**
    - Sau khi lưu lượng được cho phép vào DMZ1, tường lửa tiếp tục kiểm tra và cho phép kết nối từ DMZ1 sang DMZ2 Zone. DMZ2 là khu vực chứa các máy chủ ứng dụng và cơ sở dữ liệu.
    - Điều này cho phép các dịch vụ trong DMZ1 (như Web hoặc Proxy server) có thể liên lạc với các máy chủ trong DMZ2 nếu cần, chẳng hạn để truy xuất dữ liệu từ

cơ sở dữ liệu. Tường lửa sẽ kiểm soát chặt chẽ các kết nối này để bảo đảm chỉ những truy cập cần thiết mới được phép.

3. **Bước 3: Trao đổi hai chiều giữa DMZ2 Zone và Internal Zone**
    - Tường lửa sẽ cho phép trao đổi dữ liệu hai chiều giữa các máy chủ trong DMZ2 và khu vực nội bộ (Internal Zone). Các máy chủ nội bộ có thể truy cập vào các dịch vụ ứng dụng hoặc cơ sở dữ liệu trong DMZ2 để thực hiện các tác vụ cần thiết, và ngược lại, các máy chủ trong DMZ2 cũng có thể gửi phản hồi về khu vực nội bộ.
    - Tuy nhiên, tường lửa sẽ giới hạn và giám sát kỹ lưỡng những kết nối này để tránh rủi ro bảo mật, chỉ cho phép các lưu lượng hợp lệ và an toàn.
4. **Bước 4: Từ Internal Zone ra lại DMZ1 Zone**
    - Người dùng từ các máy trạm trong khu vực nội bộ (Internal Zone) có thể cần truy cập các dịch vụ tại DMZ1, chẳng hạn như Proxy, Email, hoặc Web server.
    - Tường lửa sẽ kiểm tra các kết nối từ nội bộ ra DMZ1 và chỉ cho phép những truy cập được cấp quyền, đảm bảo rằng lưu lượng từ mạng nội bộ khi ra ngoài được bảo mật và tuân thủ các chính sách an ninh đã đặt ra.

Tóm lại, tường lửa đóng vai trò quan trọng trong việc kiểm soát và bảo vệ các kết nối qua lại giữa Internet, DMZ1, DMZ2 và Internal Zone, giúp đảm bảo an toàn và giảm thiểu rủi ro bảo mật trong toàn bộ hệ thống mạng.

LO3 PHÂN TÍCH TÌNH HUỐNG

3.1. Tình huống 1

Người quản trị hệ thống website của 1 ngân hàng phát hiện ra cơ chế thực hiện backup và Restore của hệ thống có vấn đề và nó đã không hoạt động hơn 6 tháng nay. Tuy nhiên anh ta không biết cách khắc phục và anh ta cũng không báo cho ban giám đốc. Tháng vừa rồi hệ thống Website bị sự cố và cần các bản backup để restore hệ thống thì không có để thực hiện.

- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử của người quản trị.**
    - Trách nhiệm chuyên môn: không thực hiện việc backup và restore hệ thống trong suốt 6 tháng quá là thiếu trách nhiệm. Người quản trị phải đảm bảo hệ thống luôn hoạt động ổn định và bảo vệ dữ liệu.
    - Tính trung thực: việc không báo cáo với ban giám đốc về vấn đề này thể hiện sự thiếu trung thực và không tuân thủ quy định công việc, gây nguy hiểm cho hoạt động của ngân hàng.
    - Bảo vệ quyền lợi người khác: Hành động không khắc phục sự cố dẫn đến việc mất dữ liệu, có thể gây thiệt hại nghiêm trong cho ngân hàng và khách hàng.
- **Nếu ở vị trí người quản trị hệ thống, bạn sẽ hành xử như thế nào?**
    - Ngay lập tức thông báo cho ban giám đốc về tình trạng không hoạt động của cơ chế backup và restore.
    - Hợp tác với các chuyên gia để tìm hiểu và khắc phục sự cố này ngay lập tức.
    - Đưa ra các biện pháp khắc phục và cải tiến quy trình backup để ngăn chặn sự cố tương tự trong tương lai.

3.2. Tình huống 2

Một nhân viên IT của công ty đầu tư chứng khoán có thể theo dõi và đọc được emails, documentations, thậm chí ghi băng được những trao đổi CEO, CFO và điều này sẽ giúp nhân viên đó mua bán stocks hữu hiệu, kiếm được nhiều tiền cho bản thân hoặc bán tin tức cho những đối thủ cạnh tranh... Trong một lần uống café nhân viên IT đó đã tiết lộ thông tin bảo mật cho một người bạn thân và sau đó nhận về một số tiền gọi là quà là 100 ngàn đô.

- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của bạn A.**
    - **Tính trung thực:** Nhân viên IT đã sử dụng thông tin mật để trục lợi cá nhân, vi phạm nguyên tắc trung thực và bảo mật
    - **Trách nhiệm bảo mật:** Hành vi tiết lộ thông tin nhạy cảm gây ảnh hưởng đến hoạt động của công ty và có thể dẫn đến thiệt hại tài chính cho tổ chức.
    - **Bán thông tin:** Việc bán thông tin cho đối thủ cạnh tranh không chỉ vi phạm qui định công ty mà còn có thể cấu thành tội phạm kinh tế.
- **Nếu ở vị trí người người A, bạn sẽ hành xử như thế nào?**
    - Không tham gia vào việc theo dõi và tiết lộ thông tin bí mật
    - Đặt sự trung thực và bảo mật lên hàng đầu, báo cáo hành vi vi phạm cho cấp trên hoặc cơ quan chức năng nếu cần thiết.

3.3. Tình huống 3

Bạn làm cho công ty chuyên thiết kế Website cho các khách hàng. Ban lãnh đạo của công ty luôn yêu cầu bạn dùng chính Website của khách hàng mà công ty thiết kế để đặt backlinks đến Website công ty mình. Mục tiêu là SEO Website cho công ty. Các khách hàng không hề biết việc làm này của công ty. Và điều đáng nói hơn nữa là có những website công ty đặt backlink thông qua một dòng text có fontsize nhỏ (2px), màu chữ trắng vì sợ khách hàng biết và phàn nàn. Bạn đã làm đều này từ nhiều năm trước đến nay.

- **Dựa vào qui tắc ứng xử ACM (Association for Computing Machinery), Anh/Chị hãy cho biết Ban lãnh đạo của công ty vi phạm nguyên tắc nào? Giải thích ý nghĩa của nguyên tắc đó và tính đúng/sai của Ban lãnh đạo công ty trên.**
    - Trách nhiệm bảo mật: Ban lãnh đạo đã vi phạm nguyên tắc bảo vệ thông tin của khách hàng bằng cách sử dụng website của họ để đặt backlink mà không thông báo.
    - Tính minh bạch: Việc sử dụng backlink qua text nhỏ mà khách hàng không biết đến thể hiện sự thiếu minh bạch và không trung thực.
- **Dựa vào Luật An ninh mạng Việt Nam (Luật số: 24/2018/QH14), Anh/Chị hãy cho biết Ban lãnh đạo của công ty vi phạm điều luật nào? Giải thích ý nghĩa của điều luật đó và tính đúng/sai của hành vi trên.**
    - Việc sử dụng trái phép thông tin và quyền lợi của khách hàng có thể vi phạm điều 18 Luật An ninh mạng, nơi quy định về bảo vệ thông tin cá nhân và bảo vệ quyền lợi hợp pháp của cá nhân, tổ chức.

3.4. Tình huống 4

Bạn là kỹ sư phần mềm tại một công ty mới thành lập. Công ty đang phát triển một ứng dụng mới cho phép nhân viên bán hàng tạo ra và gửi email báo giá bán hàng và hóa đơn của khách hàng từ điện thoại thông minh của họ. Bộ phận maketing của công ty bạn đã giới thiệu ứng dụng này cho một tập đoàn lớn và nói rằng ứng dụng này hiện nay đã sẵn sàng. Nhưng thực tế, tại thời điểm này ứng dụng vẫn còn chứa khá nhiều lỗi, cần phải hơn 1 tháng thì ứng dụng mới được khắc phục các lỗi nghiêm trọng. Tuy nhiên, trưởng nhóm testing đã báo cáo rằng tất cả các lỗi đã được tìm ra và có thể khắc phục dễ dàng. Do sự cạnh tranh khốc liệt trong ngành công nghiệp phần mềm trên điện thoại thông minh, ban giám đốc quyết định công ty phải là "người đầu tiên" đưa ứng dụng này ra thị trường cho dù vẫn biết ứng dụng chưa hoàn chỉnh. Nếu sản phẩm này không xuất hiện đầu tiên, công ty khởi nghiệp của bạn có thể sẽ bị phá sản. Bạn là người có trách nhiệm đưa sản phẩm đó ra thị trường.

- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc.**
    - Nguyên tắc 1: Bảo vệ và tôn trọng quyền lợi của người khác: Ban giám đốc đã quyết định phát hành một sản phẩm chưa hoàn chỉnh, có thể gây ra trải nghiệm tiêu cực cho người dùng. Việc này không tôn trọng quyền lợi của khách hàng và có thể gây thiệt hại cho danh tiếng công ty trong mắt khách hàng.
    - Nguyên tắc 2: Cung cấp thông tin chính xác và đầy đủ: Việc marketing rằng ứng dụng "đã sẵn sàng" khi thực tế sản phẩm còn nhiều lỗi là hành vi gây hiểu nhầm, không cung cấp thông tin chính xác cho khách hàng và đối tác.
    - Nguyên tắc 3: Trách nhiệm xã hội: Việc phát hành sản phẩm chưa hoàn chỉnh không chỉ ảnh hưởng đến người dùng mà còn đến toàn bộ ngành công nghiệp phần mềm, dẫn đến sự mất niềm tin từ phía khách hàng vào các sản phẩm công nghệ.
- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của bạn nếu bạn đồng ý đưa sản phẩm ra trong tuần tới.**
    - Nguyên tắc 1: Bảo vệ và tôn trọng quyền lợi của người khác: Bằng cách đồng ý phát hành một sản phẩm chưa hoàn chỉnh, bạn sẽ gây hại đến trải nghiệm của khách hàng và có thể làm tổn hại đến quyền lợi của họ.
    - Nguyên tắc 2: Cung cấp thông tin chính xác và đầy đủ: Bạn sẽ tiếp tay cho hành vi không trung thực khi quảng bá sản phẩm chưa hoàn chỉnh như một sản phẩm hoàn hảo.
    - Nguyên tắc 3: Trách nhiệm cá nhân: Bạn cũng có trách nhiệm trong việc bảo vệ danh tiếng của công ty và ngành công nghiệp phần mềm nói chung. Việc phát hành một sản phẩm không đạt tiêu chuẩn có thể gây thiệt hại lớn về mặt tài chính và uy tín.

- **Nếu bạn muốn đưa sản phẩm ra tuần tới mà không vi phạm quy tắc xứng xử thì bạn sẽ làm gì và giải thích lý do tại sao**

- **Thảo luận với ban giám đốc về tình trạng thực tế của ứng dụng**: Cung cấp một báo cáo chi tiết về các lỗi còn tồn tại và rủi ro liên quan đến việc phát hành sản phẩm không hoàn chỉnh.
- **Đề xuất lùi thời gian phát hành**: Trình bày lý do vì sao việc phát hành một sản phẩm lỗi không chỉ là sai lầm về mặt đạo đức mà còn có thể dẫn đến hậu quả tài chính và danh tiếng nghiêm trọng cho công ty.
- **Tìm kiếm giải pháp thay thế**: Nếu có thể, đề xuất một giải pháp tạm thời, chẳng hạn như phát hành một bản beta cho một nhóm người dùng hạn chế, trong khi tiếp tục khắc phục các lỗi trước khi phát hành chính thức.
- **Đảm bảo minh bạch trong thông tin**: Nếu sản phẩm vẫn được phát hành, hãy đảm bảo rằng khách hàng được thông báo rõ ràng về tình trạng của ứng dụng và các lỗi có thể xảy ra, đồng thời cung cấp cam kết về việc sẽ sửa chữa và cập nhật trong thời gian sớm nhất.

3.5. Tình huống 5

Để giám sát tất cả hành động truy cập web của các nhân viên trong công ty. Ban giám đốc đã xây dựng một ứng dụng ghi nhận lại hết tất cả các lịch sử sử dụng máy tính của các nhân viên. Phần mềm ghi nhận lịch sử truy cập web, ghi nhận lại hết thao tác gõ bàn phím, các màn hình máy tính được theo dõi 24/24. Ban giám đốc thường xuyên vào ứng dụng này kiểm soát xem ai đã truy cập nội dung mang tính giải trí trong giờ làm việc hoặc đang làm gì trên màn hình,... nhằm mục tiêu nhắc nhỡ cũng như phạt cảnh cáo các nhân viên vi phạm.

- **Nếu bạn là ban giám đốc - người quyết định giám sát nhân viên bằng hình thức trên thì bạn có thông báo trước cho người dùng hay không?**
    - Tôi sẽ **thông báo trước cho nhân viên** về việc giám sát này. Điều này không chỉ thể hiện sự minh bạch mà còn giúp xây dựng lòng tin giữa công ty và nhân viên. Việc thông báo rõ ràng về việc theo dõi các hành động trực tuyến của nhân viên có thể bao gồm:

- **Mục đích của việc giám sát**: Giải thích rằng mục tiêu không chỉ là quản lý hành vi mà còn là để bảo vệ tài sản của công ty và đảm bảo môi trường làm việc hiệu quả.
- **Phạm vi giám sát**: Cung cấp thông tin về những gì sẽ được theo dõi, như lịch sử truy cập web và thao tác gõ bàn phím, để nhân viên có thể nhận thức và có thể thay đổi hành vi của mình nếu cần.
- **Quyền lợi và quyền riêng tư**: Đảm bảo nhân viên hiểu rằng quyền riêng tư của họ sẽ được tôn trọng trong một số khía cạnh nhất định và rằng việc theo dõi này sẽ được thực hiện một cách công bằng.
- Việc thông báo rõ ràng sẽ giúp giảm bớt lo lắng và hiểu lầm trong đội ngũ nhân viên.

- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc này**
  - Nguyên tắc 1: Bảo vệ và tôn trọng quyền lợi của người khác: Việc theo dõi 24/24 các hoạt động của nhân viên mà không thông báo hoặc không có sự đồng ý của họ là một sự xâm phạm vào quyền riêng tư. Nhân viên có quyền được biết và có sự đồng ý trước khi công ty theo dõi hành vi của họ.
  - Nguyên tắc 2: Cung cấp thông tin chính xác và đầy đủ: Nếu ban giám đốc không minh bạch về mục đích và phạm vi của việc giám sát, họ đang vi phạm quy tắc này. Nhân viên cần phải được thông báo về lý do và cách thức mà thông tin của họ sẽ được sử dụng.
  - Nguyên tắc 3: Trách nhiệm xã hội: Việc theo dõi chặt chẽ và có tính xâm phạm như vậy có thể dẫn đến môi trường làm việc không thoải mái, giảm động lực làm việc và sự tin tưởng của nhân viên. Điều này không chỉ ảnh hưởng đến sức khỏe tâm lý của nhân viên mà còn có thể tác động tiêu cực đến hiệu suất làm việc tổng thể của công ty.
  - Nguyên tắc 4: Khuyến khích phát triển và học hỏi: Một môi trường làm việc mà nhân viên cảm thấy họ đang bị giám sát quá mức có thể dẫn đến việc họ không

dám sáng tạo hoặc thử nghiệm trong công việc. Sự sợ hãi về việc bị theo dõi có thể kìm hãm sự phát triển cá nhân và nghề nghiệp của họ.

3.6. Tình huống 6

Một công ty kinh doanh phần mềm sử dụng phần mềm Ptraker. Đây là phần mềm giúp người dùng có thể xem tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh, bật - tắt 3G/GPRS của điện thoại bị giám sát. Thậm chí người sử dụng còn có thể ra lệnh điều khiển từ xa điện thoại bị cài Ptracker bằng cách nhắn tin tới điện thoại này.

- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người ra quyết định kinh doanh phần mềm này.**
    - **Tôn trọng quyền riêng tư của người khác**: Phần mềm Ptracker có khả năng truy cập tin nhắn, danh bạ, ghi âm cuộc gọi, và định vị của điện thoại. Điều này vi phạm nghiêm trọng quyền riêng tư của người dùng mà không có sự đồng ý rõ ràng. Theo nguyên tắc của ACM, việc sử dụng hoặc cung cấp phần mềm gây xâm phạm quyền riêng tư là không đạo đức.
    - **Trung thực và đáng tin cậy**: Phần mềm Ptracker được thiết kế để có thể điều khiển từ xa thiết bị của người khác, điều này tạo ra một công cụ nguy hiểm nếu rơi vào tay người dùng với mục đích xấu. Việc kinh doanh một phần mềm có thể bị lạm dụng để theo dõi và xâm nhập quyền riêng tư không tuân thủ nguyên tắc trung thực và bảo vệ người dùng.
    - **Trách nhiệm với xã hội**: Công ty kinh doanh phần mềm này không đảm bảo rằng sản phẩm của họ không bị lạm dụng để xâm phạm quyền riêng tư. Điều này thể hiện sự thiếu trách nhiệm với xã hội khi đưa ra một sản phẩm có nguy cơ cao cho an toàn và quyền riêng tư của cá nhân.
- **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người dùng phần mềm trên để theo dõi và điều khiển điện thoại của người khác**
    - **Tôn trọng quyền riêng tư của người khác**: Người dùng không được phép xâm nhập vào quyền riêng tư của người khác, bao gồm việc truy cập tin nhắn,

cuộc gọi và định vị mà không có sự đồng ý. Điều này là hành vi xâm phạm quyền riêng tư nghiêm trọng, vi phạm nguyên tắc của ACM về bảo vệ quyền riêng tư cá nhân.

- **Trung thực và công bằng**: Việc sử dụng phần mềm để theo dõi và kiểm soát thiết bị của người khác là hành vi thiếu trung thực và thiếu công bằng, vì nó được thực hiện mà không có sự chấp thuận. ACM khuyến nghị hành động một cách trung thực và công bằng với những người khác.
- **Tránh gây hại cho người khác**: Người dùng có thể lợi dụng phần mềm này để gây ra thiệt hại tinh thần hoặc tài chính cho chủ thiết bị, vi phạm nguyên tắc không gây hại của ACM.

3.7. Tình huống 7

Người quản trị mạng của một công ty nhỏ được giao giải quyết mọi vấn đề liên quan đến việc cài đặt, cấu hình các phần cứng cũng như phần mềm trên hệ thống máy tính. Khi cài mới hoặc cập nhật các phần mềm đều có các đề xuất chi tiền mua các phần mềm có bản quyền. Tuy nhiên người quản trị không bao giờ mua các phần mềm có bản quyền đó về cài đặt mà chỉ cài đặt các bản crack. Số tiền mua bản quyền hằng năm người quản trị chiếm đoạt hết. Do dùng các phần mềm crack nên thỉnh thoảng người quản trị phải tìm các key crack trên các trang crack để cấu hình lại các phần mềm.

- ***Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người quản trị.***
    - **Tính trung thực và đáng tin cậy**: Người quản trị mạng đã gian lận trong việc quản lý ngân sách cho các phần mềm bản quyền bằng cách sử dụng các phần mềm crack. Thay vì mua các phần mềm có bản quyền như đề xuất, người quản trị lại chiếm đoạt số tiền này. Việc này vi phạm nguyên tắc trung thực và đáng tin cậy vì người quản trị đã không trung thực với công ty và lợi dụng chức vụ để thu lợi cá nhân.
    - **Trách nhiệm chuyên môn**: Người quản trị mạng có trách nhiệm cung cấp và duy trì hệ thống an toàn, đáng tin cậy cho công ty. Tuy nhiên, việc sử dụng phần

mềm crack là vi phạm bản quyền và có thể gây rủi ro bảo mật lớn cho hệ thống. Điều này thể hiện sự thiếu trách nhiệm trong việc đảm bảo an toàn và hợp pháp hóa phần mềm trong công ty.

- **Tôn trọng quyền sở hữu trí tuệ**: Việc sử dụng các phần mềm crack mà không mua bản quyền là hành vi xâm phạm quyền sở hữu trí tuệ. Theo nguyên tắc của ACM, các chuyên gia công nghệ thông tin cần tôn trọng quyền sở hữu trí tuệ của những sản phẩm mà họ sử dụng, bao gồm cả việc mua bản quyền phần mềm nếu cần.
- **Tránh gây hại cho người khác**: Hành vi sử dụng phần mềm crack có thể dẫn đến các vấn đề như nhiễm mã độc hoặc làm mất dữ liệu do các phần mềm không rõ nguồn gốc. Điều này có thể gây tổn thất cho công ty và ảnh hưởng đến các thành viên khác trong công ty, đi ngược với nguyên tắc tránh gây hại.

- ***Phân tích mối nguy hại của hành vi của người quản trị mạng ảnh hưởng đến doanh nghiệp.***
  - **Nguy cơ bảo mật**: Phần mềm crack thường có nguồn gốc không rõ ràng và có thể chứa mã độc (malware), virus, hoặc các phần mềm gián điệp. Việc cài đặt các phần mềm này có thể làm tăng nguy cơ xâm nhập hệ thống, dẫn đến rò rỉ dữ liệu và các cuộc tấn công mạng. Điều này đe dọa đến an toàn thông tin và tài sản kỹ thuật số của công ty.
  - **Rủi ro pháp lý**: Sử dụng phần mềm không bản quyền là hành vi vi phạm bản quyền và có thể dẫn đến các vấn đề pháp lý. Công ty có thể bị phạt hoặc kiện tụng bởi các nhà phát triển phần mềm nếu bị phát hiện sử dụng phần mềm crack. Điều này có thể gây thiệt hại tài chính và ảnh hưởng đến uy tín của công ty.
  - **Hiệu suất hệ thống kém ổn định**: Các phần mềm crack thường không được cập nhật thường xuyên và có thể không ổn định, dẫn đến hiệu suất hệ thống không tốt và có thể gây ra lỗi phần mềm. Điều này làm giảm hiệu quả làm việc và ảnh hưởng đến năng suất của nhân viên.
  - **Mất lòng tin từ cấp quản lý và đồng nghiệp**: Khi các hành vi gian lận của người quản trị mạng bị phát hiện, điều này có thể làm giảm lòng tin từ phía công

ty đối với bộ phận IT và ảnh hưởng đến hình ảnh chuyên nghiệp của công ty. Đồng thời, nó có thể tạo ra môi trường làm việc không an toàn và không đáng tin cậy.

IV. MỘT SỐ TÌNH HUỐNG TÌM HIỂU LUẬT AN NINH MẠNG

4.1. Tình huống 1

Do thiếu tiền ăn chơi, A và B đã lập ra nhiều tài khoản facebook ảo để bán điện thoại qua mạng. Hai bạn chụp ảnh những chiếc điện thoại và lấy những hình ảnh trên mạng để đăng bán với giá rẻ hơn so với giá thị trường và đặt ra quy định là khách hàng mua hàng được quyền đổi trả nhưng không được xem hàng trước khi thanh toán tiền. Đến lúc giao hàng, 2 bạn đã bỏ một hộp khẩu trang y tế thay vì điện thoại. Sau đó, 02 bạn xóa tài khoản facebook với mục đích khách hàng sau khi phát hiện sẽ không liên lạc được.

Hỏi, nếu A và B rủ em tham gia thì em có tham gia cùng không? Vì sao?

Gợi ý trả lời:

Không, vì hành vi của A và B là vi phạm pháp luật. Vi phạm điều cấm của **Luật An ninh mạng** (hành vi sử dụng công nghệ thông tin để chiếm đoạt tải sản).

Điều 174 **Bộ luật hình sự 2015** sửa đổi bổ sung quy định về Tội lừa đảo chiếm đoạt tài sản nhưu sau:

Tìm hiểu Luật An ninh mạng 2018

1. Người nào bằng thủ đoạn gian dối chiếm đoạt tài sản của người khác trị giá từ 2.000.000 đồng đến dưới 50.000.000 đồng hoặc dưới 2.000.000 đồng nhưng thuộc một trong các trường hợp sau đây, thì bị phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:

a) Đã bị xử phạt vi phạm hành chính về hành vi chiếm đoạt tài sản mà còn vi phạm;

b) Đã bị kết án về tội này hoặc về một trong các tội quy định tại các điều 168, 169, 170, 171, 172, 173, 175 và 290 của Bộ luật này, chưa được xóa án tích mà còn vi phạm;

c) Gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội;

d) Tài sản là phương tiện kiếm sống chính của người bị hại và gia đình họ96.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 02 năm đến 07 năm:

a) Có tổ chức;

b) Có tính chất chuyên nghiệp;

c) Chiếm đoạt tài sản trị giá từ 50.000.000 đồng đến dưới 200.000.000 đồng;

d) Tái phạm nguy hiểm;

đ) Lợi dụng chức vụ, quyền hạn hoặc lợi dụng danh nghĩa cơ quan, tổ chức;

e) Dùng thủ đoạn xảo quyệt;

g)97 (được bãi bỏ)

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 15 năm:

a) Chiếm đoạt tài sản trị giá từ 200.000.000 đồng đến dưới 500.000.000 đồng;

b)98 (được bãi bỏ)

c) Lợi dụng thiên tai, dịch bệnh.

4. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 12 năm đến 20 năm hoặc tù chung thân:

a) Chiếm đoạt tài sản trị giá 500.000.000 đồng trở lên;

Sự cần thiết ban hành Luật An ninh mạng

b)99 (được bãi bỏ)

c) Lợi dụng hoàn cảnh chiến tranh, tình trạng khẩn cấp.

5. Người phạm tội còn có thể bị phạt tiền từ 10.000.000 đồng đến 100.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

Câu trả lời ngắn:

Em **không nên tham gia** vì:

1. **Vi phạm pháp luật**: Hành vi của A và B là lừa đảo qua mạng, vi phạm Luật An ninh mạng và có thể bị xử lý hình sự theo Bộ luật Hình sự.
2. **Ảnh hưởng uy tín cá nhân**: Tham gia lừa đảo gây mất uy tín, ảnh hưởng xấu đến danh tiếng và mối quan hệ xã hội của em.
3. **Rủi ro pháp lý**: Em sẽ phải chịu trách nhiệm nếu hành vi bị phát hiện, có thể bị xử phạt hành chính hoặc truy cứu trách nhiệm hình sự.
4. **Trách nhiệm đạo đức**: Là công dân, em nên sống trung thực và tuân thủ pháp luật, không gây hại cho người khác.

4.2. Tình huống 2

A và B là hai bạn rất thân từ khi còn là học sinh tiểu học đến trung học cơ sở, nhưng đến năm lớp 8 thì A và B không còn thân thiết và chơi với nhau nữa.

B đã dùng tài khoản mạng xã hội Facebook để đăng tải các thông tin về bí mật của cá nhân A như tính cách, những đặc điểm trên cơ thể, về gia đình A, nói xấu A…và chia sẻ thông tin này đến bạn bè của A và nhận được nhiều bình luận từ người dùng Facebook. A rất buồn và đã đề nghị B gở bỏ các thông tin nhưng B không gở dẫn đến A phải bỏ học.

Hỏi: Việc B dùng mạng xã hội Facebook để đăng tải các thông tin về bí mật của cá nhân A như tính cách, những đặc điểm trên cơ thể, về gia đình A có đúng pháp luật không? Vì sao

Gợi ý Trả lời:

Hành vi của B là vi phạm pháp luật, vì theo Điều 18 *Luật An ninh mạng* thì Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử Đăng tải, phát tán thông tin trên không gian mạng có nội dung bí mật cá nhân, bí mật gia đình và đời sống riêng tư

gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân là vi phạm pháp luật.

Hành vi của B sẽ bị xử phạt như thế nào: Phạt tiền từ 10-20 triệu đồng đối với hành vi: Cung cấp, trao đổi, truyền đưa hoặc lưu trữ, sử dụng thông tin số nhằm đe dọa, quấy rối, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của người khác.

Nghị định số 174/2013/NĐ-CP ngày 03/11/2013 của Chính phủ quy định xử phạt vi pham hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện.

Câu trả lời ngắn:

Việc B dùng mạng xã hội Facebook để đăng tải các thông tin bí mật cá nhân và nói xấu A **là vi phạm pháp luật** vì:

1. **Xâm phạm quyền riêng tư**: Theo Luật An ninh mạng và Bộ luật Dân sự, việc tiết lộ thông tin bí mật đời tư của người khác khi chưa được phép là hành vi xâm phạm quyền riêng tư và danh dự cá nhân của A.
2. **Hành vi xúc phạm danh dự, nhân phẩm**: Luật An ninh mạng quy định rõ ràng việc tung tin, nói xấu và làm tổn thương người khác trên mạng là bất hợp pháp. Hành vi của B đã gây ảnh hưởng nghiêm trọng đến tinh thần của A, thậm chí khiến A phải bỏ học.
3. **Hành vi bị xử lý**: Theo quy định pháp luật, hành vi này có thể bị xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự về tội làm nhục người khác hoặc vi phạm quyền riêng tư.

4.3. Tình huống 3

Theo các bạn khi sử dụng mạng internet, nhất là mạng xã hội như facebook thì chúng ta không được đăng tải, phát tán những nội dung gì?

Gợi ý trả lời:

Theo quy định tại Điều 18 Luật An ninh mạng thì hành vi Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định dưới đây là vi phạm pháp luật:

1. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

2. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm:

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm:

a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

4. Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm:

a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác;

b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

5. Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế – xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

Câu trả lời ngắn:

Khi sử dụng mạng internet, đặc biệt là mạng xã hội như Facebook, chúng ta **không nên đăng tải hoặc phát tán** các nội dung sau:

1. **Thông tin sai sự thật**: Tránh lan truyền tin đồn, tin giả mạo hoặc thông tin chưa được xác thực vì có thể gây hoang mang và hiểu lầm.
2. **Thông tin xâm phạm quyền riêng tư**: Không tiết lộ bí mật đời tư của người khác mà không được phép, như thông tin cá nhân, hình ảnh, hoặc các chi tiết nhạy cảm.
3. **Nội dung bạo lực, xúc phạm, gây thù hận**: Không đăng tải nội dung công kích, xúc phạm danh dự, nhân phẩm của người khác, hoặc kích động bạo lực và hận thù.
4. **Nội dung vi phạm pháp luật**: Tránh chia sẻ nội dung liên quan đến các hành vi trái pháp luật như lừa đảo, khiêu dâm, kích động phạm tội.
5. **Nội dung vi phạm bản quyền**: Không phát tán tài liệu, hình ảnh, video có bản quyền mà không có sự cho phép của chủ sở hữu.

4.4. Tình huống 4

Bạn A học lớp 9 rất thích đốt pháo, lân la lên mạng bạn A được một tài khoản facebook mời mua pháo với giá 200k/hộp. A đã nói dối bố mẹ là cần 200k để nộp tiền học,

sau khi bố mẹ cho tiền thì A đã mua card điện thoại rồi nhắn mã số cho người bán pháo trên mạng để mua pháo về đốt.

Hỏi: Việc A lên mạng xã hội mua pháo có đúng không?, vì sao?

Gợi ý trả lời:

Hành vi của người bán pháo cũng như của A là vi phạm pháp luật, vì theo Điểm d Khoản 1 Điều 18 Luật An ninh mạng thì hành vi Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật là vi phạm pháp luật.

Hành vi của A sẽ bị xử lý: Phạt tiền từ 5 đến 10 triệu đồng về hành vi Sản xuất, tàng trữ, mua, bán, vận chuyển trái phép pháo, thuốc pháo và đồ chơi nguy hiểm (Nghị định 167/2013/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy và chữa cháy; phòng, chống bạo lực gia đình)

Câu trả lời ngắn:

Việc A lên mạng xã hội để mua pháo **là không đúng** vì:

1. **Vi phạm pháp luật**: Pháo là mặt hàng bị cấm mua bán, sử dụng ở Việt Nam (trừ một số loại pháo hoa không nổ được phép sử dụng theo quy định). Việc mua và sử dụng pháo là hành vi trái pháp luật và có thể bị xử phạt hành chính hoặc truy cứu trách nhiệm hình sự.
2. **Nguy hiểm đến an toàn cá nhân và cộng đồng**: Đốt pháo có nguy cơ cao gây ra tai nạn, cháy nổ, ảnh hưởng đến sức khỏe và an toàn của bản thân cũng như những người xung quanh.
3. **Thiếu trung thực với bố mẹ**: A đã nói dối bố mẹ để lấy tiền mua pháo, điều này không chỉ sai về mặt đạo đức mà còn làm mất lòng tin của gia đình.

Vì vậy, hành vi này là không đúng cả về mặt pháp luật và đạo đức.