

**NGHIÊN CỨU, XÂY DỰNG MÔ HÌNH MẠNG AN TOÀN CHO CÔNG TY CỔ PHẦN THƯƠNG MẠI HỒNG ANH**

**BÁO CÁO BÀI TẬP LỚN**

**HỌC PHẦN AN NINH MẠNG**

GVHD: T.s Phạm Văn Hiệp

Lớp: 20241IT6070001

Nhóm 8: Hoàng Hải Đăng - 2021606104

Dương Văn Trường - 2023600260

Trần Văn Hoàng - 2021607887

Lữ Sơn Trường - 2021601393

**Hà Nội 2024**

c

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

------------

# **LỜI MỞ ĐẦU**

An ninh mạng đã trở thành một lĩnh vực quan trọng và đa dạng trong lĩnh vực khoa học máy tính và công nghệ thông tin. Nó liên quan đến việc bảo vệ dữ liệu, ngăn chặn các cuộc tấn công mạng, quản lý danh sách truy câp,.... Được áp dụng trong tất cả các doanh nghiệp, cơ quan chính phủ, ngân hàng,...

Mạng không dây đang trở thành một phần quan trọng và không thể thiếu trong môi trường công nghiệp và doanh nghiệp ngày nay. Sự tiện lợi và tính linh hoạt của mạng không dây đã giúp nâng cao hiệu suất làm việc, tạo điều kiện thuận lợi cho làm việc từ xa, và cung cấp sự kết nối liền mạch. Tuy nhiên, với sự tiến bộ trong kỹ thuật, mạng không dây cũng mang theo các rủi ro bảo mật đáng kể, chẳng hạn như việc truy cập trái phép, đánh cắp dữ liệu và tấn công mạng. Vì vậy, việc xây dựng một mô hình mạng không dây an toàn là một nhiệm vụ quan trọng và không thể bỏ qua trong việc quản lý và bảo vệ dữ liệu của công ty.

Dưới sự hướng dẫn của TS. Phạm Văn Hiệp, bọn em đã hoàn thành đề tài. Mặc dù đã cố gắng hết sức nhưng nhóm chúng em cũng không thể tránh khỏi những sai sót trong quá trình làm bài. Vì vậy rất mong thầy thông cảm và chia sẻ ý kiến để nhóm chúng em có thể hoàn thiện đề tài.

Chúng em xin chân thành cảm ơn!

# **CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI**

* 1. **Tổng quan về An ninh mạng**
     1. **Khái niệm**

**An ninh mạng (Cybersecurity)** là tập hợp các biện pháp, công nghệ và quy trình được thiết kế để bảo vệ hệ thống, mạng lưới và dữ liệu khỏi các cuộc tấn công, truy cập trái phép, hoặc thiệt hại. An ninh mạng đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin số.



* + 1. **Mục tiêu chính của An ninh mạng**

Mục tiêu chính của an ninh mạng là bảo vệ thông tin và hệ thống khỏi các mối đe dọa và tấn công. Dưới đây là một số mục tiêu cụ thể:

* **Bảo mật thông tin:** Đảm bảo rằng thông tin nhạy cảm và quan trọng được bảo vệ khỏi truy cập trái phép và rò rỉ.
* **Tính toàn vẹn:** Đảm bảo rằng dữ liệu không bị thay đổi hoặc giả mạo trong quá trình lưu trữ hoặc truyền tải.
* **Tính sẵn sàng:** Đảm bảo rằng hệ thống và dịch vụ luôn sẵn sàng và hoạt động liên tục, không bị gián đoạn do các cuộc tấn công hoặc sự cố.
* **Xác thực:** Đảm bảo rằng người dùng và hệ thống được xác thực đúng cách để ngăn chặn truy cập trái phép.
* **Kiểm soát truy cập:** Đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài nguyên và thông tin quan trọng.
* **Bảo vệ chống lại các mối đe dọa:** Phát hiện và ngăn chặn các cuộc tấn công mạng, phần mềm độc hại, và các mối đe dọa khác.
* **Đảm bảo tuân thủ:** Đảm bảo rằng các hệ thống và quy trình tuân thủ các quy định và tiêu chuẩn an ninh mạng.
  + 1. **Các mối đe dọa trong An ninh mạng**

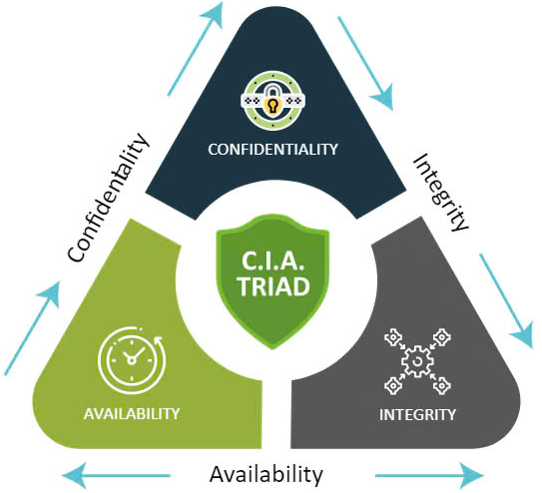
An ninh mạng được lập nên để chống lại những mối đe dọa ảnh hưởng đến người sử dụng như:

* **Malware:** Phần mềm độc hại như virus, worm, trojan...
* **Hacking:** Việc xâm nhập trái phép vào hệ thống máy tính.
* **Phishing:** Lừa đảo trực tuyến để đánh cắp thông tin cá nhân.
* **DDoS:** Tấn công từ chối dịch vụ để làm quá tải hệ thống.
* **Ransomware:** Mã độc mã hóa dữ liệu và đòi tiền chuộc.
* **Lỗ hổng bảo mật:** Các điểm yếu trong phần mềm, hệ điều hành...
  + 1. **Các biện pháp bảo vệ An ninh mạng**
* **Cập nhật phần mềm:** Luôn cập nhật các bản vá bảo mật mới nhất.
* **Sử dụng mật khẩu mạnh:** Tạo mật khẩu phức tạp và duy nhất cho mỗi tài khoản.
* **Xác thực hai yếu tố:** Thêm một lớp bảo mật bằng cách yêu cầu xác thực qua email, SMS hoặc ứng dụng.
* **Firewall:** Tường lửa giúp chặn các kết nối không đáng tin cậy.
* **Giải pháp bảo mật:** Sử dụng các phần mềm diệt virus, hệ thống phát hiện xâm nhập...
* **Đào tạo nhận thức:** Nâng cao nhận thức về an ninh mạng cho người dùng.
* **Sao lưu dữ liệu:** Thường xuyên sao lưu dữ liệu để phòng trường hợp bị mất dữ liệu.

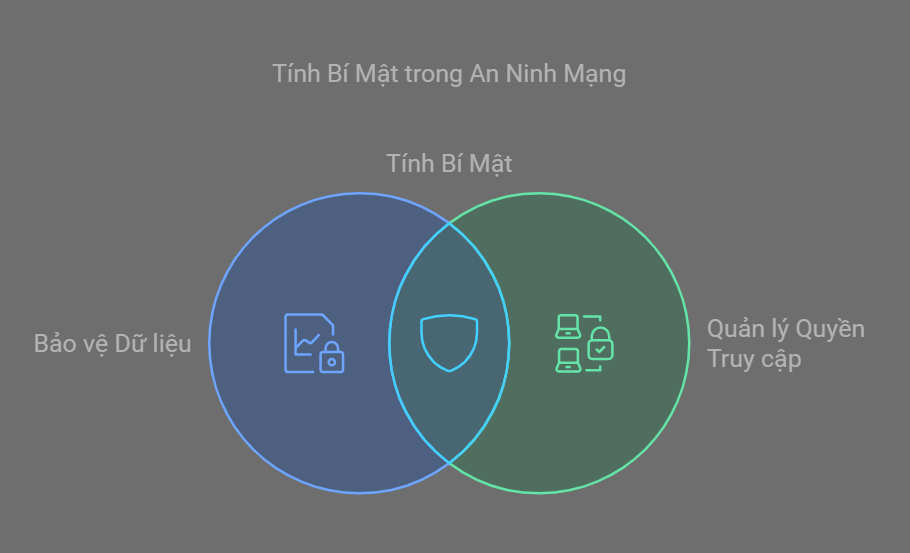
An ninh mạng là một lĩnh vực phức tạp và luôn thay đổi. Để bảo vệ bản thân và tổ chức trước các mối đe dọa, cần có sự kết hợp giữa các giải pháp công nghệ và các biện pháp quản lý.

* 1. **Các kiến thức cơ sở**
     1. **An toàn thông tin (Mô hình CIA)**

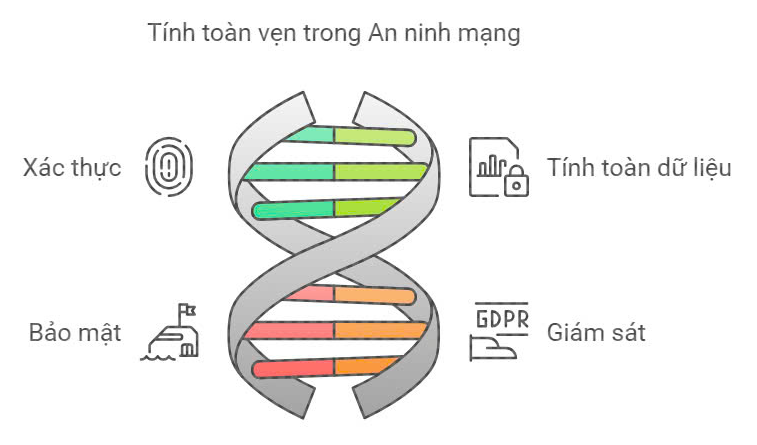
Mô hình bộ ba CIA gồm có: Confidentiality (tính bí mật), Integrity (tính toàn vẹn) và Availability (tính sẵn sàng). Ba nguyên tắc cốt lõi này phải dẫn đường cho tất cả các hệ thống an ninh mạng. Bộ ba CIA cũng cung cấp một công cụ đo (tiêu chuẩn để đánh giá) đói với các thực hiện an ninh. Mọi vi phạm bất kì một trong ba nguyên tắc này đều có thể gây hậu quả nghiêm trọng đối với tất cả các thành phần có liên quan.



* **Tính bí mật:** là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhảy cảm đó được che giấu với người dùng không được cấp phép. Gồm 2 nội dung là bí mật về dữ liệu và quyền riêng tư. Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất.



* **Tính toàn vẹn:** Là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó Bảo đảm sự chính xác về dữ liệu và hệ thống.

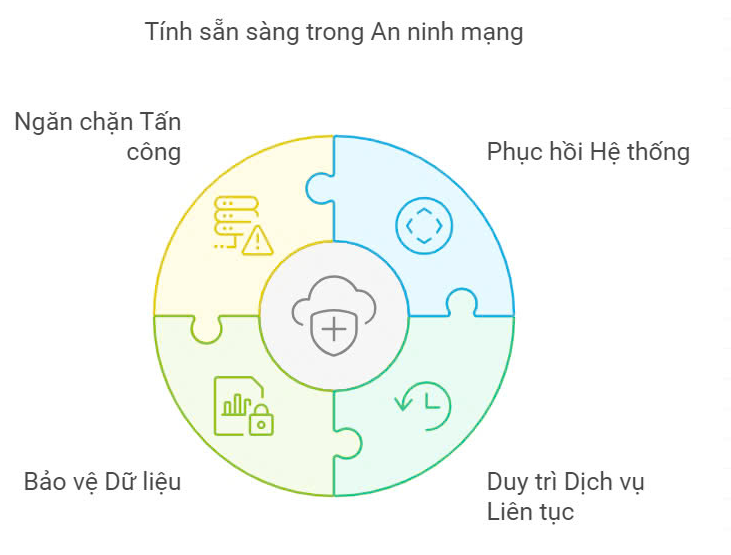


Có 3 mục đích chính của việc đảm bảo tính toàn vẹn:

* Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.
* Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chú tâm của những người sử dụng được phép.
* Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

Tính toàn vẹn gồm có toàn vẹn về dữ liệu và toàn vẹn của hệ thống, trong đó:

* Toàn vẹn dữ liệu: Đảm bảo rằng dữ liệu và các chương trình chỉ được thay đổi theo bởi người được cấp quyền.
* Tính toàn vẹn của hệ thống: Đảm bảo rằng một hệ thống thực hiện chức năng dự kiến của nó một cách nguyên vẹn, không bị
* thao túng trái phép một cách có chủ ý hoặc vô ý.
* **Tính sẵn sàng:** Đảm bảo truy cập và sử dụng thông tin kịp thời và đáng tin cậy. Mất tính sẵn sàng là sự gián đoạn truy cập hoặc gián đoán sử dụng thông tin hoặc gián đoạn sử dụng hệ thống thông tin. Do đó, tính sẵn sàng có liên quan đến độ tin cậy của hệ thống.



* + 1. **An toàn mạng máy tính**

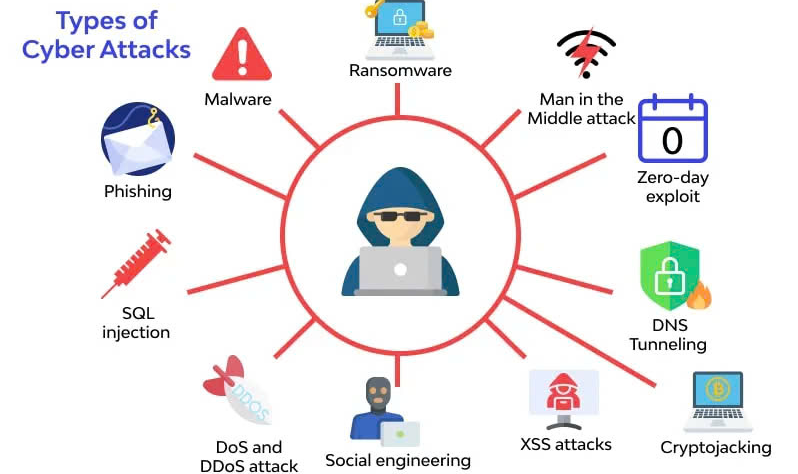
**An toàn mạng máy tính** (Network Security) là tập hợp các biện pháp, công nghệ, và quy trình được sử dụng để bảo vệ các hệ thống mạng máy tính khỏi các mối đe dọa, tấn công, và truy cập trái phép. Mục tiêu chính của an toàn mạng là đảm bảo tính **bảo mật**, **toàn vẹn**, và **khả dụng** của dữ liệu và tài nguyên trong hệ thống mạng

* **Các mối đe dọa mạng phổ biến:**
* **Malware (Phần mềm độc hại):** Gồm virus, sâu (worms), ransomware, spyware, adware.
* **Phishing (Lừa đảo):** Sử dụng email hoặc website giả mạo để đánh cắp thông tin nhạy cảm.
* **DDoS (Tấn công từ chối dịch vụ):** Làm tê liệt hệ thống bằng cách gửi lượng lớn yêu cầu đến máy chủ.
* **Man-in-the-Middle Attack:** Tấn công chặn thông tin giữa hai bên giao tiếp.
* **Zero-Day Exploits:** Lỗ hổng chưa được phát hiện hoặc chưa được vá trong phần mềm/hệ thống.
* **Các biện pháp bảo mật:**
* **Sử dụng tường lửa (Firewall):** Lọc và kiểm soát lưu lượng mạng ra vào.
* **Mã hóa (Encryption):** Bảo vệ dữ liệu bằng cách chuyển đổi thông tin sang dạng không thể đọc được.
* **Hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS):** Phát hiện và phản ứng với các mối đe dọa.
* **Xác thực hai yếu tố (2FA):** Tăng cường bảo mật cho tài khoản.
* **Cập nhật và vá lỗi phần mềm:** Giảm nguy cơ bị tấn công qua các lỗ hổng.
  + 1. **Tấn công mạng**

**Tấn công mạng** (Cyber Attack) là hành động cố ý nhằm xâm nhập, làm gián đoạn, hoặc làm tổn hại đến các hệ thống máy tính, mạng lưới, hoặc dữ liệu. Các cuộc tấn công mạng thường do cá nhân, nhóm, hoặc tổ chức thực hiện với nhiều mục đích khác nhau như đánh cắp thông tin, phá hoại hệ thống, hoặc gây thiệt hại về tài chính và uy tín.

**Các loại tấn công mạng phổ biến:**

* Phishing: Lừa người dùng cung cấp thông tin cá nhân qua email giả mạo hoặc trang web giả.
* Malware: Sử dụng phần mềm độc hại như virus, worm, Trojan để xâm nhập và gây hại.
* SQL Injection: Tấn công vào cơ sở dữ liệu qua các lỗ hổng trên ứng dụng web.
* Man-in-the-Middle (MitM): Nghe lén hoặc can thiệp vào giao tiếp giữa hai bên.
* Zero-Day Exploits: Tấn công các lỗ hổng chưa được phát hiện hoặc vá lỗi.
* Brute Force Attack: Thử tất cả các tổ hợp mật khẩu để truy cập.



**Phòng chống tấn công mạng:**

* Cập nhật phần mềm thường xuyên để vá các lỗ hổng bảo mật.
* Sử dụng mật khẩu mạnh và kích hoạt xác thực hai yếu tố (2FA).
* Cảnh giác với email lạ và không nhấp vào các liên kết hoặc tải xuống tệp không rõ nguồn gốc.
* Cài đặt phần mềm chống virus và tường lửa (firewall).
* Sao lưu dữ liệu định kỳ để khôi phục trong trường hợp xảy ra sự cố.
  1. **Nội dung nghiên cứu**
     1. **Lý do chọn đề tài**

Trong bối cảnh ngày càng gia tăng các mối đe dọa về an ninh mạng, việc bảo vệ hệ thống thông tin của các doanh nghiệp, đặc biệt là các công ty cổ phần, là cực kỳ quan trọng. Công ty CP thương mại Hồng Anh, với sự phát triển nhanh chóng và mở rộng quy mô hoạt động, đối mặt với nhiều thách thức trong việc đảm bảo an toàn thông tin và bảo mật mạng. Việc xây dựng một mô hình mạng an toàn giúp giảm thiểu rủi ro từ các cuộc tấn công mạng, bảo vệ tài sản dữ liệu và uy tín của công ty.

Đề tài này sẽ giúp nâng cao nhận thức về an ninh mạng trong môi trường doanh nghiệp, đồng thời cung cấp những giải pháp cụ thể và hiệu quả nhằm bảo vệ thông tin và đảm bảo hoạt động ổn định của công ty trong dài hạn. Hơn nữa, việc nghiên cứu và xây dựng mô hình này cũng góp phần nâng cao kiến thức và kỹ năng thực tế về an ninh mạng trong bối cảnh công nghệ ngày càng phát triển.

Đề tài "Nghiên cứu, xây dựng mô hình mạng an toàn cho Công ty CP thương mại Hồng Anh" được chọn vì tính cấp thiết và tầm quan trọng của việc đảm bảo an ninh mạng trong môi trường doanh nghiệp hiện nay. Với sự phát triển mạnh mẽ của công nghệ thông tin và việc áp dụng các hệ thống mạng trong hầu hết các hoạt động kinh doanh, các công ty đang phải đối mặt với những nguy cơ tiềm ẩn liên quan đến bảo mật thông tin và an ninh mạng.

Trong đó, các công ty cổ phần (CP) thường có quy mô lớn và cấu trúc tổ chức phức tạp, điều này khiến cho việc bảo vệ thông tin trở thành một thách thức lớn hơn. Dữ liệu của công ty, từ các thông tin khách hàng, tài chính, cho đến các bí mật công nghệ đều là những mục tiêu hấp dẫn đối với các hacker và những kẻ tấn công mạng. Một lỗ hổng bảo mật dù nhỏ cũng có thể dẫn đến những thiệt hại nghiêm trọng về tài chính và uy tín của công ty. Vì vậy, xây dựng và triển khai một mô hình mạng an toàn không chỉ giúp giảm thiểu rủi ro từ các cuộc tấn công mạng, mà còn bảo vệ thông tin quan trọng, tạo dựng niềm tin cho khách hàng và đối tác.

Ngoài ra, công ty CP thương mại Hồng Anh, với sự phát triển không ngừng về quy mô và hệ thống thông tin, cũng cần phải thích ứng với các thách thức của môi trường mạng hiện đại, bao gồm các mối đe dọa từ phần mềm độc hại, tấn công DDoS (Distributed Denial of Service), lỗ hổng bảo mật trong phần mềm, và các rủi ro đến từ người dùng bên trong (insider threats). Việc triển khai một mô hình mạng an toàn sẽ giúp công ty chủ động phòng ngừa và ứng phó với các mối đe dọa này, tạo ra một môi trường làm việc và giao dịch an toàn cho cả nhân viên và khách hàng.

Bên cạnh đó, xây dựng mô hình mạng an toàn còn giúp công ty tuân thủ các yêu cầu pháp lý về bảo mật dữ liệu, đặc biệt là trong bối cảnh các quy định như GDPR (General Data Protection Regulation) tại châu Âu hay các luật bảo vệ dữ liệu cá nhân tại Việt Nam đang trở nên ngày càng nghiêm ngặt. Việc không tuân thủ các quy định này có thể dẫn đến các hậu quả nghiêm trọng, từ các khoản phạt tài chính cho đến việc mất uy tín và sự tin tưởng từ phía khách hàng.

Cuối cùng, đề tài này không chỉ mang lại giá trị thiết thực đối với công ty, mà còn giúp sinh viên có cơ hội nghiên cứu, tìm hiểu và áp dụng các kiến thức lý thuyết về an ninh mạng vào thực tiễn. Đây cũng là cơ hội để phát triển các kỹ năng thiết kế, triển khai và quản lý hệ thống mạng an toàn, từ đó đóng góp vào sự nghiệp phát triển bền vững của ngành công nghệ thông tin và an ninh mạng.

* + 1. **Mục tiêu nghiên cứu**

Mục tiêu chính của đề tài "Nghiên cứu và xây dựng mô hình mạng an toàn cho Công ty CP thương mại Hồng Anh" là thiết lập và triển khai một mô hình mạng an toàn hiệu quả, phù hợp với các yêu cầu đặc thù của công ty. Mô hình này sẽ sử dụng các phương pháp và công cụ an ninh mạng hiện đại, đảm bảo hệ thống thông tin của công ty luôn được bảo vệ khỏi các mối đe dọa từ bên ngoài và bên trong. Để đạt được mục tiêu này, các mục tiêu cụ thể sau sẽ được thực hiện:

* **Phân tích và đánh giá hiện trạng bảo mật của công ty:**

Xác định các nguy cơ tiềm ẩn và điểm yếu trong hệ thống mạng hiện tại của công ty: Phân tích chi tiết các lỗ hổng bảo mật, các mối đe dọa tiềm tàng từ các cuộc tấn công mạng, phần mềm độc hại, tấn công DDoS (Distributed Denial of Service), và các mối nguy hiểm đến từ các nhân viên hoặc người dùng bên trong công ty.

Đánh giá các biện pháp bảo mật hiện có của công ty: Xem xét hiệu quả của các giải pháp bảo mật hiện tại như tường lửa, mã hóa dữ liệu, và các hệ thống phát hiện và phòng chống xâm nhập (IDS/IPS), từ đó xác định các điểm cần cải thiện.

* **Xác định và đề xuất các yêu cầu bảo mật đặc thù của công ty:**

Nghiên cứu và đưa ra yêu cầu bảo mật cụ thể cho công ty: Dựa trên các yếu tố như quy mô công ty, loại hình hoạt động và dữ liệu quan trọng, xác định các yêu cầu bảo mật đặc biệt như bảo mật thông tin khách hàng, dữ liệu tài chính, và bảo mật các giao dịch trực tuyến.

Lựa chọn và đề xuất các biện pháp bảo mật tối ưu: Đưa ra các giải pháp bảo mật phù hợp với yêu cầu của công ty, bao gồm việc triển khai mã hóa, kiểm soát truy cập, và các biện pháp ngăn ngừa rủi ro bảo mật.

* **Thiết kế mô hình mạng an toàn cho công ty:**

Phát triển kiến trúc mạng an toàn tổng thể: Xây dựng mô hình mạng an toàn toàn diện bao gồm các thành phần cốt lõi như firewall, IDS/IPS, VPN (Virtual Private Network), các cổng bảo mật và các giải pháp kiểm soát truy cập.

Thiết kế mô hình bảo mật linh hoạt và mở rộng: Đảm bảo rằng mô hình mạng an toàn có khả năng mở rộng trong tương lai, đáp ứng sự phát triển của công ty. Thiết kế cấu trúc mạng sao cho dễ dàng thêm vào các thành phần bảo mật mới khi cần thiết.

Lựa chọn các công cụ bảo mật tiên tiến và phù hợp: Xác định các công cụ và giải pháp bảo mật phù hợp để triển khai trong mô hình mạng, như hệ thống giám sát an ninh mạng thời gian thực, phân tích lưu lượng mạng và các công cụ kiểm tra bảo mật.

* **Triển khai mô hình mạng an toàn trên môi trường mô phỏng:**

Sử dụng công cụ mô phỏng như Packet Tracer để triển khai mô hình mạng an toàn: Sử dụng Packet Tracer, một công cụ mô phỏng mạng mạnh mẽ, để tạo dựng và kiểm tra các thành phần trong mô hình mạng an toàn. Việc mô phỏng sẽ giúp kiểm tra khả năng tương tác giữa các thành phần bảo mật và xác nhận tính khả thi của mô hình.

Thiết lập và cấu hình các giải pháp bảo mật trong mô hình: Cấu hình firewall, IDS/IPS, VPN và các cơ chế bảo mật khác trong Packet Tracer để đảm bảo chúng hoạt động hiệu quả, bảo vệ hệ thống mạng khỏi các mối đe dọa tiềm ẩn.

* **Kiểm tra và xác nhận tính hiệu quả của các giải pháp bảo mật:**

Thực hiện các bài kiểm tra bảo mật để đánh giá hiệu quả của mô hình: Sử dụng các phương pháp kiểm tra như tấn công mô phỏng (penetration testing), đánh giá khả năng chống lại các mối đe dọa từ bên ngoài và bên trong, và kiểm tra khả năng phản ứng của hệ thống trước các sự cố an ninh.

Đo lường hiệu quả của các biện pháp bảo mật: Đánh giá các chỉ số về hiệu suất bảo mật, bao gồm thời gian phát hiện và phản ứng với sự cố, mức độ bảo vệ dữ liệu và hệ thống mạng, và mức độ giảm thiểu rủi ro an ninh.

* **Đề xuất các giải pháp duy trì và cập nhật hệ thống bảo mật lâu dài:**

Xây dựng kế hoạch bảo trì và cập nhật hệ thống bảo mật: Đảm bảo rằng hệ thống bảo mật được duy trì và cập nhật thường xuyên, theo dõi các mối đe dọa mới và thay đổi trong môi trường công nghệ.

Đào tạo nhân viên và nâng cao nhận thức về bảo mật: Đưa ra các chương trình đào tạo cho nhân viên về các biện pháp bảo mật cơ bản và các chính sách bảo mật nội bộ, giúp họ nhận thức được vai trò của mình trong việc bảo vệ hệ thống mạng.

* **Đảm bảo tuân thủ các tiêu chuẩn và quy định về bảo mật thông tin**:

Tuân thủ các quy định pháp lý và tiêu chuẩn quốc tế về bảo mật thông tin: Đảm bảo rằng mô hình bảo mật đáp ứng các yêu cầu pháp lý về bảo vệ dữ liệu cá nhân và bảo mật thông tin, như GDPR hoặc các quy định bảo mật trong nước.