|  |
| --- |
|  |
| **BỘ CÔNG THƯƠNG**  **TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**  **---------------------------------------** |
|  |
| ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC |
| NGÀNH CÔNG NGHỆ THÔNG TIN |
| **XÂY DỰNG VÀ TRIỂN KHAI MÔ HÌNH MẠNG AN TOÀN CHO DOANH NGHIỆP QUY MÔ NHỎ** |
|  |
|  |
| **GVHD:** *Ths.Nguyễn Thị Thanh Huyền* |
| **Sinh viên:** Tàng Trọng Phi |
| **Mã số sinh viên:** *2021604136* |
|  |
|  |
|  |
| **Hà Nội – Năm 2025** |
|  |
|  |
| **BỘ CÔNG THƯƠNG**  **TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**  **---------------------------------------** |
|  |
| ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC |
| NGÀNH CÔNG NGHỆ THÔNG TIN |
| **XÂY DỰNG VÀ TRIỂN KHAI MÔ HÌNH MẠNG AN TOÀN CHO DOANH NGHIỆP QUY MÔ NHỎ** |
|  |
|  |
| **GVHD:** Ths.Nguyễn Thị Thanh Huyền |
| **Sinh viên:** Tàng Trọng Phi |
| **Mã số sinh viên:** 2021604136 |
|  |
|  |
|  |
| **Hà Nội – Năm 2025** |

**LỜI CAM ĐOAN**

Em xin cam đoan là đề tài “Xây Dựng Và Triển Khai Mô Hình Mạng An Toàn Cho Doanh Nghiệp Quy Mô Nhỏ” là do em tự khảo sát, tìm hiểu và tự tay thực hiện thiết kế các chức năng của phần mềm, hoàn thiện phần mềm và viết báo cáo của phầm mềm. Mọi tài liệu tham khảo (nếu có) sẽ được trích dẫn nguồn theo quy định.

Nếu có dấu hiệu đi sao chép đề tài thì em xin chịu mọi trách nhiệm.

Tàng Trọng Phi

**LỜI CẢM ƠN**

Qua gần bốn năm học tập, em được tiếp cận học hỏi và trau rồi các kiến thức cần thiết. Cùng với sự hỗ trợ của Khoa Công Nghệ Thông Tin em đã bắt đầu quá trình thực tập tốt nghiệp của mình. Khoảng thời gian thực tập tuy không dài nhưng em đã được học hỏi rất nhiều thứ, được tự nghiên cứu và gặt hái được nhiều kết quả tốt.

Em xin chân thành gửi lời cảm ơn cô Nguyễn Thị Thanh Huyền – người rất tận tình hướng dẫn từ những ngày em bắt đầu việc làm đồ án.

Bản báo cáo dưới đây là kết quả của một quá trình nghiên cứu, tìm hiểu và thực hành. Em rất mong sẽ có được những ý kiến đóng góp của thầy cô, để bản báo cáo này cũng như bản thân em được hoàn thiện hơn nữa.

Em xin chân thành cảm ơn!

Sinh viên thực hiện

*Tàng Trọng Phi*

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

............................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................

**NHẬN XÉT CỦA GIẢNG VIÊN PHẢN BIỆN**

..........................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................

LỜI NÓI ĐẦU

Trong thời đại chuyển đổi số, sự phát triển nhanh chóng của công nghệ thông tin không chỉ mang lại nhiều lợi ích vượt bậc mà còn đặt ra những thách thức lớn về an ninh mạng. Các doanh nghiệp quy mô nhỏ thường gặp khó khăn trong việc xây dựng và triển khai hệ thống mạng an toàn do hạn chế về nguồn lực và kiến thức chuyên môn. Những rủi ro như tấn công từ chối dịch vụ (DDoS), đánh cắp dữ liệu hay tấn công bằng mã độc đã và đang gây ra nhiều thiệt hại nghiêm trọng, ảnh hưởng trực tiếp đến hoạt động và uy tín của doanh nghiệp. Nhằm tìm hiểu và giải quyết những vấn đề này, đề tài “Xây dựng và triển khai mô hình mạng an toàn cho doanh nghiệp quy mô nhỏ” được thực hiện với mục tiêu không chỉ đáp ứng yêu cầu bảo mật cơ bản mà còn mang lại hiệu quả triển khai và vận hành.

**Phạm vi nghiên cứu:** tập trung vào việc thiết kế, triển khai và kiểm thử một mô hình mạng an toàn phù hợp với các doanh nghiệp quy mô nhỏ. Mô hình bao gồm các thành phần cơ bản như Domain Controller, Web Server, Mail Server và các hệ thống hỗ trợ khác, đồng thời mô phỏng các kịch bản tấn công mạng phổ biến như tấn công leo thang đặc quyền (Privilege Escalation), di chuyển ngang (Lateral Movement) để đưa ra các biện pháp phòng thủ hiệu quả.

**Mục tiêu của đề tài:** xây dựng một hệ thống mạng an toàn, có khả năng phòng chống các mối đe dọa phổ biến, dễ triển khai và quản lý. Đề tài không chỉ hướng tới việc đảm bảo tính bảo mật mà còn phải mang lại hiệu quả vận hành cao, phù hợp với các doanh nghiệp nhỏ vốn có nguồn lực hạn chế.

Bài báo cáo được chia thành bốn chương với nội dung chính như sau:

**Chương 1: Tổng quan về an ninh mạng doanh nghiệp**

Phần này sẽ trình bày cơ sở lý thuyết về an ninh mạng, những nguy cơ thường gặp đối với doanh nghiệp quy mô nhỏ và các yêu cầu cơ bản để xây dựng một hệ thống mạng an toàn.

**Chương 2: Thiết kế và triển khai mô hình mạng an toàn**

Sau khi tìm hiểu về cơ sở lý thuyết, chúng ta sẽ tập trung vào việc phân tích yêu cầu, thiết kế kiến trúc mạng và triển khai các thành phần chính trong hệ thống, từ đó xây dựng một mô hình mạng an toàn hoàn chỉnh.

**Chương 3: Kiểm thử và đánh giá hệ thống mạng**

Chương này trình bày quá trình kiểm thử các chức năng bảo mật của mô hình mà chúng ta đã xây dựng, đánh giá hiệu quả phòng thủ của hệ thống thông qua các kịch bản tấn công giả lập và phân tích các kết quả thu được.

**Chương 4: Đề xuất giải pháp và hướng phát triển**

Dựa trên các kết quả kiểm thử và đánh giá, chương này sẽ đưa ra các giải pháp cải thiện bảo mật cho hệ thống mạng, đồng thời định hướng các nghiên cứu và triển khai trong tương lai.

**Phần kết luận**

Tổng hợp lại những kết quả đạt được, đánh giá mức độ hoàn thiện của hệ thống và rút ra các bài học kinh nghiệm trong quá trình thực hiện.

Qua đề tài này, em không chỉ nắm vững các kiến thức chuyên môn mà còn có cơ hội thực hành triển khai một hệ thống mạng thực tế, góp phần hỗ trợ các doanh nghiệp nhỏ xây dựng hệ thống mạng an toàn, hiệu quả và bền vững.

# CHƯƠNG 1: TỔNG QUAN AN NINH MẠNG DOANH NGHIỆP

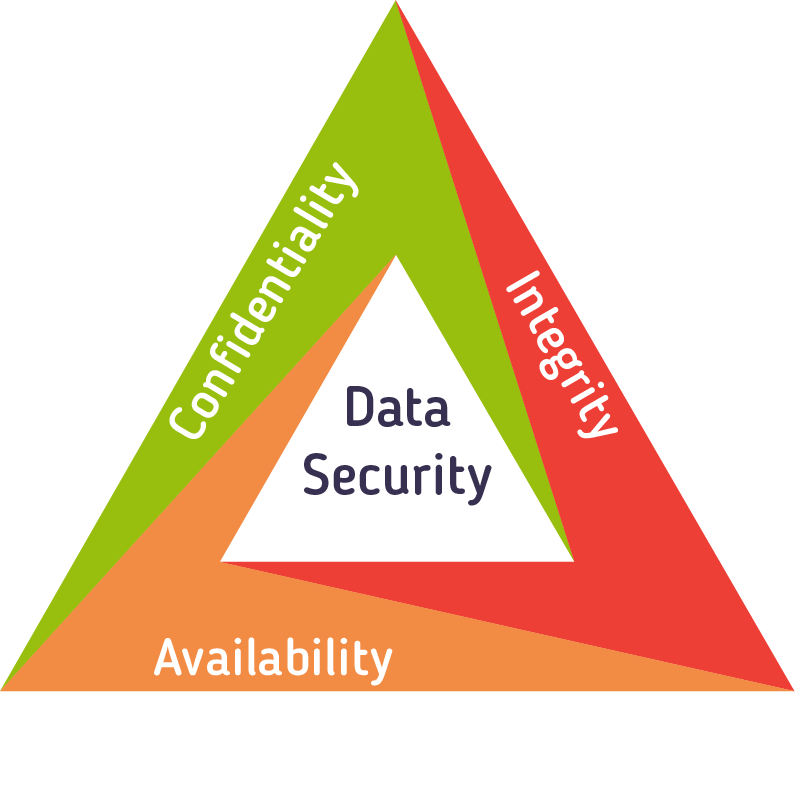
## Giới thiệu chung về bảo mật doanh nghiệp

### Khái niệm bảo mật doanh nghiệp

Bảo mật doanh nghiệp là tập hợp các biện pháp, quy trình và công nghệ được triển khai nhằm bảo vệ thông tin, dữ liệu và tài sản của tổ chức khỏi các mối đe dọa, tấn công và truy cập trái phép. Mục tiêu là đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin, đồng thời duy trì hoạt động liên tục và hiệu quả của doanh nghiệp.

Mục tiêu của bảo mật doanh nghiệp:

* Bảo vệ thông tin nhạy cảm: Đảm bảo rằng thông tin quan trọng của doanh nghiệp, như dữ liệu khách hàng, thông tin tài chính và bí mật kinh doanh, được bảo vệ khỏi truy cập trái phép và lạm dụng.
* Đảm bảo tính toàn vẹn của dữ liệu: Ngăn chặn việc thay đổi, xóa hoặc hư hỏng dữ liệu một cách trái phép, đảm bảo rằng thông tin luôn chính xác và đáng tin cậy.
* Đảm bảo tính sẵn sàng của hệ thống: Đảm bảo rằng các hệ thống và dịch vụ quan trọng luôn sẵn sàng hoạt động, giảm thiểu thời gian gián đoạn và đảm bảo liên tục trong kinh doanh.
* Tuân thủ quy định pháp lý và tiêu chuẩn ngành: Đảm bảo rằng doanh nghiệp tuân thủ các quy định pháp lý liên quan đến bảo mật thông tin và các tiêu chuẩn ngành, tránh các hình phạt và tổn hại đến uy tín.
* Quản lý rủi ro: Xác định, đánh giá và giảm thiểu các rủi ro liên quan đến bảo mật thông tin, bao gồm cả rủi ro từ bên ngoài và bên trong tổ chức.
* Nâng cao nhận thức và đào tạo nhân viên: Tăng cường nhận thức về bảo mật thông tin trong toàn bộ nhân viên, cung cấp đào tạo và hướng dẫn để họ hiểu và tuân thủ các chính sách bảo mật của doanh nghiệp.



*Hình 1.1: Tam giác bảo mật CIA*

Việc đạt được các mục tiêu trên không chỉ giúp bảo vệ tài sản và thông tin của doanh nghiệp mà còn xây dựng lòng tin với khách hàng và đối tác, tạo nền tảng vững chắc cho sự phát triển bền vững của tổ chức

### Tầm quan trọng của bảo mật trong doanh nghiệp

Trong bối cảnh toàn cầu hóa và chuyển đổi số, bảo mật thông tin đã trở thành một yếu tố sống còn đối với sự tồn tại và phát triển của các tổ chức, doanh nghiệp. Mối đe dọa bảo mật ngày càng gia tăng và trở nên phức tạp, đe dọa trực tiếp đến các tài nguyên quan trọng và uy tín của doanh nghiệp. Do đó, bảo mật không chỉ là một yêu cầu công nghệ mà còn là chiến lược cần thiết để duy trì sự bền vững và khả năng cạnh tranh trong môi trường kinh doanh hiện đại. Các lý do sau đây làm rõ tầm quan trọng của bảo mật đối với doanh nghiệp:

Bảo vệ tài sản và thông tin quan trọng

* Thông tin doanh nghiệp: Các dữ liệu nhạy cảm như thông tin khách hàng, bí mật thương mại, tài sản trí tuệ, và chiến lược phát triển doanh nghiệp là những tài sản vô giá mà các tổ chức cần bảo vệ. Bảo mật giúp ngăn chặn các mối đe dọa như tấn công mạng và truy cập trái phép, từ đó bảo vệ những tài sản quan trọng này khỏi bị đánh cắp hoặc bị rò rỉ.
* Bảo mật dữ liệu cá nhân: Doanh nghiệp cũng cần đảm bảo bảo vệ dữ liệu cá nhân của khách hàng và nhân viên, tránh để thông tin bị sử dụng sai mục đích hoặc bị lộ. Vi phạm bảo mật trong vấn đề này không chỉ gây thiệt hại tài chính mà còn làm giảm uy tín và lòng tin của khách hàng.

Ngăn ngừa các cuộc tấn công mạng và vi phạm bảo mật

* Các mối đe dọa từ bên ngoài: Các mối đe dọa như tấn công hacker, phần mềm độc hại (malware), ransomware, và các loại tấn công khác có thể gây thiệt hại nặng nề cho doanh nghiệp. Mất mát dữ liệu, gián đoạn hoạt động, hoặc bị tống tiền đều có thể tác động nghiêm trọng đến sự ổn định tài chính và danh tiếng của tổ chức.
* Mối đe dọa từ bên trong: Bên cạnh các tấn công từ bên ngoài, các nguy cơ đến từ nhân viên hoặc các đối tượng nội bộ có quyền truy cập vào hệ thống cũng không thể xem nhẹ. Vì vậy, quản lý chặt chẽ quyền truy cập và giám sát nội bộ là yếu tố quan trọng trong chiến lược bảo mật doanh nghiệp.

Tuân thủ pháp lý và giảm thiểu rủi ro pháp lý

* Các quy định bảo mật: Các doanh nghiệp phải tuân thủ các quy định bảo mật nghiêm ngặt, như GDPR tại Liên minh Châu Âu, HIPAA trong ngành y tế tại Mỹ, hay các quy định bảo mật thông tin trong ngành tài chính. Vi phạm các yêu cầu này không chỉ dẫn đến các khoản phạt tài chính lớn mà còn làm tổn hại đến uy tín và gây ra các vấn đề pháp lý phức tạp.
* Bảo vệ quyền lợi của khách hàng: Việc bảo vệ thông tin khách hàng là yếu tố quyết định sự tin tưởng và hợp tác lâu dài. Vi phạm bảo mật có thể dẫn đến mất lòng tin của khách hàng, ảnh hưởng đến mối quan hệ với họ và gây thiệt hại lớn về tài chính.

Giảm thiểu tác động của các sự cố bảo mật

* Giảm thiểu thiệt hại: Một hệ thống bảo mật vững mạnh giúp giảm thiểu thiệt hại khi xảy ra sự cố, đồng thời giúp tổ chức khôi phục nhanh chóng và hiệu quả. Các biện pháp như sao lưu dữ liệu và kế hoạch ứng phó với sự cố bảo mật là cần thiết để bảo vệ doanh nghiệp khỏi những tác động tiêu cực.
* Tăng khả năng phục hồi: Các doanh nghiệp có hệ thống bảo mật mạnh mẽ sẽ có khả năng duy trì hoạt động trong mọi tình huống, ngay cả khi gặp phải các sự cố bảo mật nghiêm trọng. Điều này giúp doanh nghiệp duy trì sự ổn định và khả năng cạnh tranh lâu dài.

Bảo vệ uy tín và niềm tin của khách hàng

* Đảm bảo sự tin tưởng: Một doanh nghiệp có hệ thống bảo mật hiệu quả sẽ tạo được niềm tin và sự an tâm cho khách hàng và đối tác. Ngược lại, vi phạm bảo mật có thể làm mất lòng tin của khách hàng và đối tác, gây thiệt hại lớn về uy tín và các cơ hội kinh doanh trong tương lai.
* Tạo lợi thế cạnh tranh: Doanh nghiệp nào sở hữu một chiến lược bảo mật rõ ràng và mạnh mẽ sẽ tạo ra lợi thế cạnh tranh vượt trội. Khách hàng sẽ ưu tiên hợp tác với các doanh nghiệp bảo vệ tốt dữ liệu của họ và tuân thủ nghiêm ngặt các tiêu chuẩn bảo mật.

Cải thiện hiệu suất và sự ổn định của hệ thống

* Giảm thiểu gián đoạn hoạt động: Các sự cố bảo mật có thể gây gián đoạn hoạt động kinh doanh, dẫn đến thiệt hại về tài chính và thời gian. Bảo mật giúp giảm thiểu các sự cố này và duy trì hoạt động của doanh nghiệp một cách ổn định.
* Tăng cường hệ thống và quy trình làm việc: Hệ thống bảo mật hiệu quả cũng giúp doanh nghiệp tối ưu hóa các quy trình làm việc và kiểm soát tốt hơn các nguy cơ bảo mật, từ đó nâng cao hiệu suất hoạt động và khả năng phát triển bền vững.

Chống lại các mối đe dọa từ đối thủ cạnh tranh

* Cạnh tranh không lành mạnh: Các đối thủ có thể tìm cách xâm nhập vào hệ thống của doanh nghiệp để đánh cắp thông tin hoặc làm gián đoạn hoạt động. Bảo mật là biện pháp giúp doanh nghiệp bảo vệ mình khỏi những hành vi cạnh tranh không lành mạnh này.
* Bảo vệ tài sản trí tuệ: Tài sản trí tuệ như các phát minh, sáng chế hay chiến lược kinh doanh là nguồn lực quý giá mà doanh nghiệp cần bảo vệ khỏi bị sao chép hoặc đánh cắp bởi các đối thủ cạnh tranh.

Hệ quả nghiêm trọng từ các cuộc tấn công bảo mật doanh nghiệp:

* Vụ tấn công vào Yahoo (2014): Hơn 500 triệu tài khoản người dùng bị xâm nhập, khiến Yahoo mất rất nhiều niềm tin từ khách hàng và các đối tác kinh doanh. Đây là một trong những vụ vi phạm bảo mật lớn nhất trong lịch sử, ảnh hưởng trực tiếp đến danh tiếng của Yahoo và làm giảm giá trị thương hiệu.
* Vụ tấn công vào Sony (2014): Sự cố tấn công mạng vào Sony, trong đó hacker đã xâm nhập vào hệ thống và phát tán thông tin nhạy cảm, gây thiệt hại tài chính đáng kể. Đây là một ví dụ điển hình về sự ảnh hưởng lâu dài mà một vụ vi phạm bảo mật có thể gây ra đối với uy tín và niềm tin của khách hàng.
* Vụ rò rỉ dữ liệu của Equifax (2017): Equifax, một trong ba tổ chức tín dụng lớn nhất ở Mỹ, đã để lộ thông tin cá nhân của hơn 145 triệu người dùng. Vi phạm này không chỉ ảnh hưởng đến uy tín của công ty mà còn gây ra thiệt hại lớn về tài chính và mất lòng tin của khách hàng.



*Hình 1.2: Thông báo của Yahoo về việc dữ liệu người dùng bị xâm phạm*

Do đó bảo mật doanh nghiệp không chỉ là yếu tố để bảo vệ tài sản thông tin mà còn là yếu tố quyết định sự tồn tại và phát triển bền vững của doanh nghiệp. Các vụ vi phạm bảo mật nổi bật như Yahoo, Sony và Equifax đã chứng minh rằng một sự cố bảo mật có thể hủy hoại hoàn toàn uy tín và niềm tin của khách hàng, từ đó ảnh hưởng lớn đến sự phát triển và khả năng cạnh tranh của doanh nghiệp

### Các nguy cơ và mối đe dọa hiện tại

Bảo mật doanh nghiệp không chỉ đối mặt với các mối đe dọa truyền thống, mà còn phải đối diện với những nguy cơ ngày càng phức tạp do sự phát triển nhanh chóng của công nghệ và phương thức tấn công mạng. Các mối đe dọa hiện nay có thể được phân loại thành các nhóm chính như sau:

* Tấn công mạng từ bên ngoài
  + Tấn công DDoS (Distributed Denial of Service): Tấn công làm nghẽn hệ thống bằng cách gửi một lượng lớn yêu cầu đến máy chủ, khiến hệ thống không thể hoạt động bình thường. Các doanh nghiệp lớn và tổ chức tài chính thường xuyên phải đối mặt với loại tấn công này.
  + Ransomware (Mã độc tống tiền): Các cuộc tấn công ransomware ngày càng phổ biến và tinh vi hơn. Hacker mã hóa dữ liệu của doanh nghiệp và yêu cầu tiền chuộc để giải mã. Những vụ tấn công như WannaCry (2017) và NotPetya (2017) đã gây thiệt hại lớn cho các tổ chức, trong đó có cả các doanh nghiệp Việt Nam.
  + Phishing (Lừa đảo qua email): Tấn công lừa đảo qua email nhằm đánh cắp thông tin nhạy cảm như mật khẩu, số thẻ tín dụng, và thông tin đăng nhập. Phishing thường được sử dụng để xâm nhập vào các hệ thống quan trọng của doanh nghiệp, từ đó có thể thực hiện các cuộc tấn công khác.
* Tấn công nội bộ
  + Nhân viên phản bội hoặc sơ suất: Mối đe dọa không chỉ đến từ hacker mà còn có thể đến từ nhân viên nội bộ có quyền truy cập vào dữ liệu nhạy cảm. Việc nhân viên không tuân thủ các quy trình bảo mật, hoặc thậm chí cố ý bán thông tin cho kẻ xấu, có thể gây tổn hại nghiêm trọng cho doanh nghiệp.
  + Sai sót trong quản lý quyền truy cập: Doanh nghiệp thường gặp phải tình trạng cấp quyền truy cập không chính xác cho nhân viên hoặc đối tác, tạo cơ hội cho kẻ tấn công lợi dụng lỗ hổng trong hệ thống.
* Tấn công vào chuỗi cung ứng
  + Tấn công vào đối tác và nhà cung cấp: Những kẻ tấn công không chỉ nhắm mục tiêu vào các doanh nghiệp trực tiếp mà còn có thể tấn công vào các nhà cung cấp và đối tác của doanh nghiệp. Những cuộc tấn công vào chuỗi cung ứng đã trở thành một xu hướng nguy hiểm, vì hacker có thể lợi dụng lỗ hổng trong hệ thống của đối tác để xâm nhập vào doanh nghiệp.
* Lỗi phần mềm và bảo mật yếu kém
  + Lỗ hổng phần mềm: Các phần mềm và ứng dụng mà doanh nghiệp sử dụng có thể có lỗ hổng bảo mật mà kẻ tấn công có thể khai thác. Những lỗ hổng này có thể được phát hiện qua các cuộc tấn công vào các phần mềm phổ biến như Windows, Oracle, hay các hệ thống mạng của doanh nghiệp.
  + Thiếu cập nhật và bảo mật không đầy đủ: Nhiều doanh nghiệp không chú trọng vào việc cập nhật phần mềm bảo mật, khiến cho các hệ thống của họ dễ dàng bị tấn công qua những lỗ hổng đã được biết đến nhưng chưa được vá.
* Mối đe dọa từ công nghệ mới
  + IoT (Internet of Things): Các thiết bị IoT, từ máy tính, điện thoại đến các thiết bị đeo được, khi được kết nối vào mạng nội bộ của doanh nghiệp, có thể mở ra những cơ hội cho hacker tấn công. Sự thiếu sót trong bảo mật của các thiết bị này khiến cho chúng trở thành điểm yếu trong hệ thống bảo mật tổng thể.
  + AI và học máy (Machine Learning): Mặc dù AI và học máy có thể hỗ trợ tăng cường bảo mật, chúng cũng có thể bị lợi dụng bởi hacker để tạo ra các cuộc tấn công thông minh hơn, khó bị phát hiện hơn.
* Mối đe dọa từ các quy định pháp lý và vi phạm quyền riêng tư
  + Vi phạm bảo mật và quy định về dữ liệu: Các doanh nghiệp phải đối mặt với áp lực lớn trong việc tuân thủ các quy định bảo mật dữ liệu, chẳng hạn như GDPR ở châu Âu. Vi phạm quy định này có thể dẫn đến những khoản phạt nặng và mất uy tín lâu dài.

Các mối đe dọa bảo mật hiện nay đang ngày càng phức tạp và tinh vi hơn. Doanh nghiệp cần nhận thức rõ ràng về những nguy cơ này và triển khai các biện pháp bảo mật mạnh mẽ, đồng thời duy trì một quy trình quản lý bảo mật chặt chẽ để bảo vệ tài sản và dữ liệu quan trọng.

## Các thành phần của hệ thống bảo mật doanh nghiệp

### 1.2.1 Mạng và hạ tầng

Mạng và hạ tầng là nền tảng quan trọng trong hệ thống bảo mật doanh nghiệp, giúp bảo vệ các tài nguyên, dữ liệu và hoạt động của tổ chức khỏi các mối đe dọa bên ngoài và bên trong. Để đảm bảo hệ thống mạng hoạt động an toàn, các biện pháp bảo mật cần được tích hợp vào từng lớp của mạng, từ kết nối bên ngoài đến các thiết bị nội bộ.

#### 1.2.1.1 Tường lửa (Firewall)

Khái niệm: Tường lửa là thiết bị hoặc phần mềm bảo mật giám sát và kiểm soát lưu lượng mạng đi vào và ra khỏi doanh nghiệp. Tường lửa có thể hoạt động ở nhiều cấp độ khác nhau: từ tường lửa mạng (ngăn chặn lưu lượng giữa các mạng) đến tường lửa ứng dụng (bảo vệ các ứng dụng cụ thể, ví dụ như web).

Cách thức hoạt động:

* + Tường lửa trạng thái (Stateful firewall): Giám sát và theo dõi trạng thái của các kết nối, chỉ cho phép lưu lượng dữ liệu có sự xác nhận hợp lệ giữa hai điểm kết nối.
  + Tường lửa không trạng thái (Stateless firewall): Lọc lưu lượng dựa trên các quy tắc, không theo dõi trạng thái kết nối, thường được sử dụng trong các mạng đơn giản.

Chức năng: Tường lửa giúp ngăn chặn các tấn công từ bên ngoài như DDoS, xâm nhập trái phép, phần mềm độc hại, đồng thời kiểm soát các kết nối không mong muốn từ bên trong mạng doanh nghiệp.

#### 1.2.1.2 Hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS)

IDS là hệ thống giám sát và phát hiện các hành vi bất thường hoặc tấn công trong mạng của doanh nghiệp. IPS không chỉ phát hiện mà còn ngăn chặn các mối đe dọa ngay lập tức.

Cách thức hoạt động:

* + IDS: Quét và phân tích lưu lượng mạng để tìm các dấu hiệu của tấn công như SQL Injection, Cross-Site Scripting (XSS), hoặc các hành vi lạ. IDS có thể hoạt động ở mức độ mạng (Network-based IDS) hoặc mức độ host (Host-based IDS).
  + IPS: Hoạt động tương tự IDS, nhưng có thể chủ động can thiệp bằng cách ngắt kết nối hoặc chặn các yêu cầu có dấu hiệu tấn công.

Chức năng: IDS/IPS giúp phát hiện các tấn công đang diễn ra và ngăn chặn kịp thời, giảm thiểu tổn thất do các cuộc tấn công gây ra.

#### 1.2.1.3 Mạng riêng ảo (VPN)

VPN tạo ra một kết nối an toàn và bảo mật cho phép người dùng từ xa truy cập vào mạng nội bộ của doanh nghiệp qua internet. Mạng này mã hóa toàn bộ dữ liệu truyền tải, giúp bảo vệ khỏi các mối đe dọa từ mạng công cộng.

Cách thức hoạt động: VPN sử dụng các giao thức mã hóa như IPSec (Internet Protocol Security), SSL (Secure Sockets Layer), hoặc L2TP (Layer 2 Tunneling Protocol) để tạo "đường hầm" bảo mật giữa các thiết bị và máy chủ.

Chức năng: VPN giúp bảo vệ dữ liệu nhạy cảm khi nhân viên làm việc từ xa, tránh bị đánh cắp thông qua các cuộc tấn công trên mạng công cộng.

#### 1.2.1.4 Phân đoạn mạng (Network Segmentation)

Phân đoạn mạng là quá trình chia mạng doanh nghiệp thành các phân đoạn riêng biệt, mỗi phân đoạn có các mức độ bảo mật khác nhau tùy theo tính chất của dữ liệu và tài nguyên.

Cách thức hoạt động: Phân đoạn có thể thực hiện bằng cách sử dụng các VLAN (Virtual Local Area Network) hoặc firewall giữa các phân đoạn để kiểm soát lưu lượng giữa các phân vùng mạng khác nhau.

Chức năng: Phân đoạn mạng giúp cô lập các hệ thống quan trọng và giảm thiểu khả năng lây lan của tấn công từ phân đoạn này sang phân đoạn khác, đảm bảo bảo mật cho các dữ liệu nhạy cảm.

#### 1.2.1.5 Bộ lọc email và kiểm tra nội dung

Bộ lọc email bảo vệ hệ thống mạng khỏi các cuộc tấn công phishing, spam, và các email có chứa tệp đính kèm độc hại.

Cách thức hoạt động: Hệ thống lọc email sẽ quét nội dung email, các tệp đính kèm, và liên kết trong email. Các email được kiểm tra sẽ được so khớp với cơ sở dữ liệu về các mối đe dọa đã biết, hoặc dựa trên hành vi để phát hiện các dấu hiệu lừa đảo.

Chức năng: Bộ lọc email giúp ngăn chặn các mối đe dọa từ email, đặc biệt là các chiến dịch phishing nhằm đánh cắp thông tin người dùng hoặc tải phần mềm độc hại vào hệ thống.

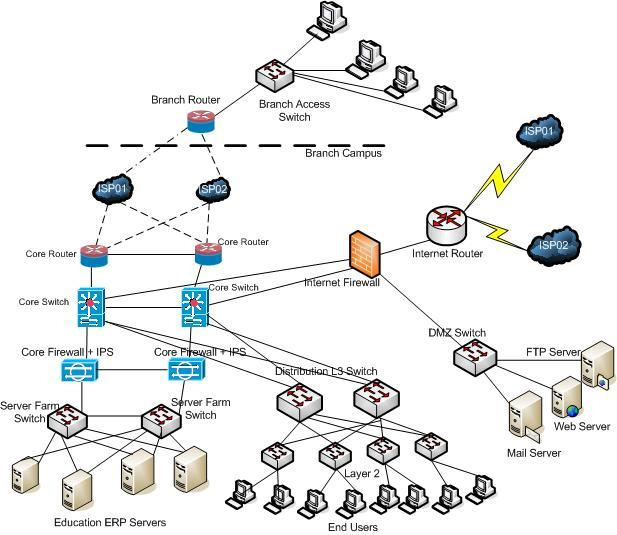
#### 1.2.1.6 Các thiết bị bảo mật bổ sung

Proxy Server: Proxy là thiết bị giúp kiểm tra và điều phối lưu lượng internet giữa người dùng và các dịch vụ trực tuyến. Proxy có thể giúp bảo vệ mạng khỏi các mối đe dọa từ web, đồng thời cải thiện hiệu suất bằng cách lưu trữ các bản sao dữ liệu.

Web Application Firewall (WAF): WAF bảo vệ các ứng dụng web khỏi các cuộc tấn công như SQL Injection, Cross-Site Scripting (XSS), và tấn công lỗ hổng của ứng dụng web. WAF giám sát và phân tích lưu lượng HTTP, xác định và ngăn chặn các yêu cầu bất hợp pháp.

Để hình dung rõ hơn, một mô hình mạng bảo mật trong doanh nghiệp có thể bao gồm các lớp bảo vệ sau:

* Mạng bên ngoài (Internet): Được bảo vệ bởi tường lửa và VPN.
* Mạng DMZ (Demilitarized Zone): Chứa các dịch vụ công cộng như web server, email server, được bảo vệ bởi WAF và IDS/IPS.
* Mạng nội bộ: Được phân đoạn thành các phân vùng khác nhau, mỗi phân vùng có chính sách bảo mật riêng. IDS/IPS và tường lửa nội bộ bảo vệ các tài nguyên quan trọng như cơ sở dữ liệu, máy chủ nội bộ.



*Hình 1.3: Một cấu trúc mạng doanh nghiệp*

Mạng và hạ tầng bảo mật doanh nghiệp là thành phần nền tảng giúp bảo vệ toàn bộ hệ thống khỏi các mối đe dọa từ bên ngoài và bên trong. Việc triển khai các thiết bị bảo mật như tường lửa, IDS/IPS, VPN, phân đoạn mạng và các công nghệ bảo mật bổ sung tạo ra một hệ thống phòng thủ đa lớp, giúp ngăn chặn các mối đe dọa và bảo vệ tài nguyên doanh nghiệp. Mô hình mạng bảo mật chặt chẽ sẽ giúp đảm bảo an toàn cho các hoạt động kinh doanh và giữ vững sự ổn định của hệ thống.

### 1.2.2 Quản lý quyền truy cập

Quản lý quyền truy cập (Identity and Access Management - IAM) là một phần quan trọng trong hệ thống bảo mật doanh nghiệp. IAM giúp đảm bảo rằng chỉ những người dùng hợp lệ và có quyền truy cập mới có thể truy cập vào các tài nguyên và thông tin nhạy cảm của tổ chức. Các chính sách và quy trình quản lý quyền truy cập đóng vai trò quyết định trong việc bảo vệ hệ thống khỏi các mối đe dọa từ việc truy cập trái phép và nâng cao tính bảo mật của doanh nghiệp.

#### 1.2.2.1 Khái niệm IAM

IAM là một hệ thống quản lý giúp tổ chức kiểm soát việc xác thực và cấp quyền truy cập của người dùng đối với các tài nguyên trong doanh nghiệp. Quản lý quyền truy cập bao gồm việc xác định ai có quyền truy cập vào tài nguyên nào, trong khoảng thời gian nào, và với mức độ quyền truy cập nào.

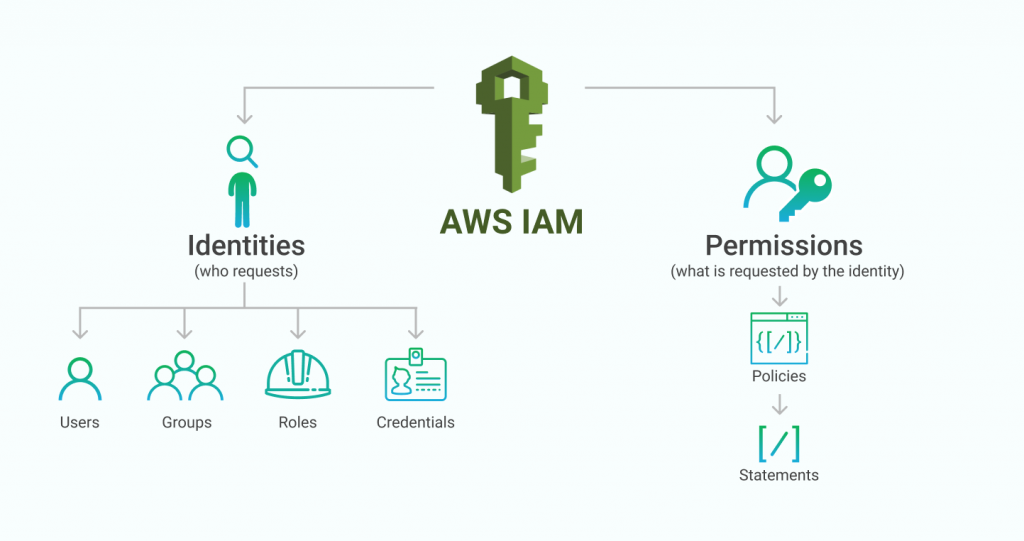
#### 1.2.2.2 Quy trình IAM

Quy trình quản lý quyền truy cập có thể được chia thành các bước cơ bản sau:

* Xác thực người dùng (Authentication): Đây là quá trình kiểm tra và xác nhận danh tính người dùng. Các phương pháp xác thực có thể bao gồm:
  + Xác thực bằng mật khẩu: Mật khẩu là phương thức xác thực phổ biến, tuy nhiên, cần có các biện pháp bổ sung như yêu cầu mật khẩu mạnh và định kỳ thay đổi mật khẩu.
  + Xác thực đa yếu tố (MFA): MFA yêu cầu người dùng phải cung cấp hai hoặc nhiều yếu tố xác thực, ví dụ như mật khẩu và mã OTP gửi qua SMS hoặc ứng dụng xác thực.
  + Xác thực sinh trắc học: Sử dụng các đặc điểm sinh trắc học của người dùng như vân tay, nhận diện khuôn mặt hoặc quét mống mắt để xác minh danh tính.
* Cấp quyền truy cập (Authorization): Sau khi xác thực, người dùng cần được cấp quyền truy cập vào các tài nguyên. Quy trình này thường được thực hiện qua các mô hình quyền truy cập như:
  + RBAC (Role-Based Access Control): Quyền truy cập được cấp dựa trên vai trò công việc của người dùng trong tổ chức. Mỗi vai trò sẽ có quyền truy cập vào các tài nguyên nhất định.
  + ABAC (Attribute-Based Access Control): Quyền truy cập được cấp dựa trên các thuộc tính của người dùng, như thời gian truy cập, địa điểm, thiết bị sử dụng, hoặc cấp bậc trong công ty.
  + DAC (Discretionary Access Control): Người sở hữu tài nguyên quyết định ai có quyền truy cập vào tài nguyên của mình.
* Giám sát và kiểm tra quyền truy cập (Access Monitoring and Auditing): Để đảm bảo tính bảo mật, việc theo dõi và kiểm tra việc sử dụng quyền truy cập là rất quan trọng. Các công cụ giám sát giúp phát hiện các hành vi bất thường hoặc xâm nhập trái phép vào hệ thống. Các hoạt động truy cập nên được ghi lại và kiểm tra định kỳ để phát hiện các vi phạm bảo mật.
* Quản lý và thu hồi quyền truy cập (Access Revocation): Khi người dùng không còn cần quyền truy cập hoặc khi họ rời khỏi tổ chức, quyền truy cập của họ cần được thu hồi ngay lập tức. Việc này giúp ngăn chặn những mối đe dọa từ những người đã rời khỏi công ty hoặc không còn có quyền truy cập.

#### 1.2.2.3 Các thành phần của IAM

IAM bao gồm nhiều thành phần quan trọng, trong đó mỗi thành phần đóng vai trò riêng biệt trong việc duy trì an ninh và kiểm soát truy cập.



*Hình 1.4: Các thành phần của IAM*

* Danh tính người dùng (Identity Management): Quản lý danh tính của người dùng, bao gồm việc tạo mới, duy trì và xóa bỏ các tài khoản người dùng. Các hệ thống IAM thường tích hợp với các dịch vụ như Active Directory hoặc LDAP để quản lý thông tin người dùng.
* Quản lý quyền hạn (Access Management): Điều này liên quan đến việc cấp, giám sát và kiểm soát quyền truy cập của người dùng đối với tài nguyên trong hệ thống. Các công cụ IAM cung cấp khả năng quản lý quyền hạn chi tiết theo từng người dùng hoặc nhóm người dùng.
* Quản lý nhóm người dùng và vai trò (Group and Role Management): Các tổ chức thường sử dụng nhóm người dùng và vai trò để đơn giản hóa việc cấp quyền. Ví dụ, một nhóm "Quản lý" có thể có quyền truy cập vào các tài nguyên cấp cao hơn so với nhóm "Nhân viên".
* Hệ thống nhận diện người dùng (User Authentication System): Đây là một thành phần quan trọng trong IAM giúp đảm bảo chỉ những người dùng hợp lệ mới có thể truy cập vào hệ thống. Nó có thể bao gồm các phương thức xác thực như mật khẩu, thẻ thông minh, hoặc xác thực sinh trắc học.

#### 1.2.2.4 Chính sách và quy định IAM

Để đảm bảo hiệu quả và an toàn trong việc quản lý quyền truy cập, doanh nghiệp cần thiết lập và tuân thủ các chính sách bảo mật nghiêm ngặt. Các chính sách này bao gồm:

* Chính sách mật khẩu: Các quy định về việc đặt mật khẩu mạnh, thay đổi mật khẩu định kỳ, và không chia sẻ mật khẩu.
* Chính sách phân quyền: Quy định rõ ràng ai có quyền truy cập vào tài nguyên nào trong hệ thống và cấp quyền theo nguyên tắc "ít quyền nhất" (least privilege).
* Chính sách MFA: Áp dụng xác thực đa yếu tố cho các tài nguyên quan trọng hoặc truy cập từ xa.
* Chính sách kiểm tra quyền truy cập: Định kỳ kiểm tra quyền truy cập của người dùng để đảm bảo quyền truy cập vẫn phù hợp với công việc hiện tại của họ.

#### 1.2.2.5 Lợi ích của IAM trong bảo mật doanh nghiệp

Giảm thiểu rủi ro xâm nhập trái phép: Quản lý quyền truy cập giúp ngăn ngừa các hành vi truy cập trái phép và hạn chế tác động của các tài khoản bị xâm nhập.

Nâng cao khả năng tuân thủ pháp lý: Việc áp dụng các quy trình IAM giúp doanh nghiệp tuân thủ các yêu cầu bảo mật và quyền riêng tư trong các quy định như GDPR hoặc HIPAA.

Cải thiện quản lý tài nguyên và người dùng: Các công cụ IAM giúp tổ chức dễ dàng quản lý và phân quyền cho hàng nghìn người dùng và tài nguyên, đặc biệt là trong môi trường doanh nghiệp lớn.

Tăng cường khả năng phục hồi sau sự cố: Khi xảy ra sự cố bảo mật, IAM giúp tổ chức nhanh chóng xác định và thu hồi quyền truy cập từ các tài khoản bị xâm nhập.

### 1.2.3 Mã hóa và bảo vệ dữ liệu

Mã hóa là một công cụ quan trọng trong bảo mật doanh nghiệp, đặc biệt khi bảo vệ dữ liệu nhạy cảm. Mã hóa giúp bảo vệ thông tin khỏi các mối đe dọa từ những người truy cập trái phép, đảm bảo rằng dữ liệu không bị rò rỉ, sửa đổi hoặc bị sử dụng vào mục đích không chính đáng. Đây là một trong những biện pháp bảo mật mạnh mẽ nhất để bảo vệ sự riêng tư và bảo mật của dữ liệu trong quá trình truyền tải và lưu trữ.

#### 1.2.3.1 Khái niệm mã hóa

Mã hóa là quá trình chuyển đổi thông tin thành một dạng không thể đọc được mà chỉ có thể giải mã được bằng một khóa (key) bảo mật. Các thuật toán mã hóa sử dụng khóa để mã hóa dữ liệu, và chỉ những người có khóa giải mã mới có thể khôi phục lại dữ liệu gốc. Mã hóa có thể được áp dụng cho dữ liệu khi đang truyền tải (data in transit) và dữ liệu khi đang lưu trữ (data at rest).

#### 1.2.3.2 Tầm quan trọng của mã hóa trong bảo mật dữ liệu

Mã hóa là công cụ không thể thiếu trong việc bảo vệ thông tin nhạy cảm, đặc biệt trong các trường hợp sau:

* Bảo vệ dữ liệu trong quá trình truyền tải: Khi dữ liệu được truyền qua mạng (như qua Internet), nếu không được mã hóa, thông tin có thể bị đánh cắp bởi các hacker. Mã hóa giúp đảm bảo rằng dữ liệu không bị đọc hoặc thay đổi trong suốt quá trình truyền tải. Ví dụ, khi một khách hàng thực hiện thanh toán trực tuyến, việc mã hóa dữ liệu như số thẻ tín dụng giúp bảo vệ thông tin cá nhân khỏi những kẻ tấn công.
* Bảo vệ dữ liệu khi lưu trữ: Dữ liệu lưu trữ trên máy chủ, cơ sở dữ liệu hoặc thiết bị di động cũng cần được mã hóa để tránh việc bị truy cập trái phép. Mã hóa dữ liệu khi lưu trữ giúp bảo vệ thông tin ngay cả khi các thiết bị hoặc hệ thống bị xâm nhập hoặc bị đánh cắp. Ví dụ, nếu một thiết bị di động chứa dữ liệu nhạy cảm bị mất hoặc bị đánh cắp, dữ liệu mã hóa sẽ không thể bị truy cập nếu không có khóa giải mã.
* Bảo vệ thông tin cá nhân và nhạy cảm: Mã hóa là một biện pháp bảo vệ mạnh mẽ đối với dữ liệu nhạy cảm như thông tin cá nhân, tài khoản ngân hàng, hồ sơ y tế, và bí mật công ty. Các tổ chức, đặc biệt là trong các ngành như tài chính và y tế, cần tuân thủ các yêu cầu bảo mật nghiêm ngặt, và mã hóa giúp bảo vệ dữ liệu khỏi các mối đe dọa tiềm tàng.

#### 1.2.3.3 Các loại mã hóa

Có hai loại mã hóa chính mà doanh nghiệp cần lưu ý khi triển khai bảo vệ dữ liệu:

* Mã hóa đối xứng (Symmetric Encryption): Đây là loại mã hóa sử dụng cùng một khóa để mã hóa và giải mã dữ liệu. Ưu điểm của mã hóa đối xứng là nhanh chóng và hiệu quả, nhưng vấn đề chính là việc truyền tải khóa an toàn. Nếu khóa bị lộ, người tấn công có thể giải mã dữ liệu. Các thuật toán mã hóa đối xứng phổ biến bao gồm AES (Advanced Encryption Standard) và DES (Data Encryption Standard).
* Mã hóa bất đối xứng (Asymmetric Encryption): Mã hóa bất đối xứng sử dụng hai khóa riêng biệt: một khóa công khai để mã hóa dữ liệu và một khóa riêng để giải mã. Loại mã hóa này thường được sử dụng trong các tình huống yêu cầu bảo mật cao, như giao dịch trực tuyến hoặc ký điện tử. Một ví dụ điển hình là thuật toán RSA, sử dụng một cặp khóa công khai và khóa riêng biệt để mã hóa và giải mã dữ liệu.
* Mã hóa kết hợp (Hybrid Encryption): Trong thực tế, mã hóa kết hợp giữa cả mã hóa đối xứng và mã hóa bất đối xứng thường được sử dụng để tận dụng ưu điểm của cả hai phương pháp. Mã hóa bất đối xứng sẽ được sử dụng để bảo mật khóa đối xứng, và sau đó mã hóa đối xứng sẽ được sử dụng để mã hóa dữ liệu. Ví dụ điển hình là giao thức SSL/TLS trong truyền tải web bảo mật.

#### 1.2.3.4 Các tiêu chuẩn mã hóa trong bảo mật doanh nghiệp

Do tính chất quan trọng của mã hóa, các tổ chức cần tuân thủ các tiêu chuẩn và quy định bảo mật để đảm bảo an toàn cho dữ liệu. Một số tiêu chuẩn mã hóa phổ biến bao gồm:

* + - AES (Advanced Encryption Standard): Là tiêu chuẩn mã hóa đối xứng được chấp nhận rộng rãi, với các độ dài khóa 128, 192 và 256 bit. AES là một trong những thuật toán mã hóa mạnh mẽ nhất hiện nay và được sử dụng trong nhiều ứng dụng bảo mật, bao gồm bảo vệ dữ liệu trong các hệ thống tài chính và chính phủ.
    - RSA (Rivest–Shamir–Adleman): Là một thuật toán mã hóa bất đối xứng phổ biến, được sử dụng trong các ứng dụng bảo mật yêu cầu mã hóa và ký số, như trong giao thức HTTPS.
    - ECC (Elliptic Curve Cryptography): Là một dạng mã hóa bất đối xứng sử dụng các đường cong elliptic. ECC cung cấp mức độ bảo mật tương đương với RSA nhưng với kích thước khóa nhỏ hơn, giúp tăng hiệu suất và giảm băng thông.
    - TLS/SSL: Giao thức bảo mật TLS/SSL sử dụng mã hóa để bảo vệ dữ liệu trong quá trình truyền tải qua mạng, đặc biệt trong các giao dịch trực tuyến và trao đổi thông tin giữa máy chủ và người dùng.

#### 1.2.3.5 Lợi ích của mã hóa trong bảo mật doanh nghiệp

Bảo vệ dữ liệu nhạy cảm: Mã hóa giúp bảo vệ thông tin quan trọng của tổ chức, bao gồm dữ liệu khách hàng, bí mật thương mại, và tài sản trí tuệ.

Tuân thủ quy định bảo mật: Các tổ chức có thể tuân thủ các quy định bảo mật và quyền riêng tư như GDPR, HIPAA, PCI-DSS thông qua việc mã hóa dữ liệu nhạy cảm.

Tăng cường sự tin tưởng của khách hàng: Khách hàng sẽ cảm thấy yên tâm khi biết rằng dữ liệu của họ được bảo vệ bằng mã hóa, từ đó củng cố uy tín và mối quan hệ của doanh nghiệp.

Ngăn chặn vi phạm bảo mật: Mã hóa giúp ngăn ngừa việc đánh cắp hoặc lạm dụng dữ liệu, ngay cả khi hệ thống bị xâm nhập.

#### 1.2.3.6 Các thách thức trong việc triển khai mã hóa

Quản lý khóa: Một trong những thách thức lớn trong mã hóa là việc quản lý và bảo vệ các khóa mã hóa. Nếu khóa bị lộ hoặc mất, dữ liệu có thể bị truy cập trái phép. Do đó, việc lưu trữ và quản lý khóa mã hóa an toàn là rất quan trọng.

Hiệu suất và tài nguyên: Mặc dù mã hóa là rất cần thiết, nhưng quá trình mã hóa và giải mã có thể làm giảm hiệu suất hệ thống, đặc biệt trong các môi trường yêu cầu xử lý dữ liệu nhanh. Do đó, cần có các chiến lược tối ưu hóa để giảm thiểu tác động này.

Khả năng tương thích: Việc triển khai mã hóa cần phải đảm bảo tính tương thích với các hệ thống và ứng dụng hiện có trong tổ chức, đặc biệt khi các hệ thống này đã cũ hoặc không hỗ trợ các phương pháp mã hóa hiện đại.

### 1.2.4 Giám sát và phát hiện sự cố

Giám sát và phát hiện sự cố là một trong những thành phần cốt lõi của hệ thống bảo mật doanh nghiệp. Việc giám sát sự kiện bảo mật trong thời gian thực không chỉ giúp phát hiện các mối đe dọa ngay từ giai đoạn đầu mà còn giảm thiểu tác động từ các cuộc tấn công. Các công cụ và phương pháp giám sát được sử dụng nhằm đảm bảo tính toàn vẹn, tính khả dụng, và tính bí mật của thông tin doanh nghiệp.

#### 1.2.4.1 Khái niệm về giám sát và phát hiện sự cố

Giám sát và phát hiện sự cố là quá trình theo dõi các hoạt động, lưu lượng và sự kiện xảy ra trong hệ thống thông tin để phát hiện các dấu hiệu bất thường hoặc các hành vi có thể dẫn đến vi phạm bảo mật. Hoạt động này thường dựa vào việc thu thập, phân tích và cảnh báo từ các công cụ bảo mật.

#### 1.2.4.2 Tầm quan trọng của giám sát và phát hiện sự cố

Phát hiện sớm các mối đe dọa: Giám sát liên tục cho phép phát hiện các hành vi bất thường hoặc các cuộc tấn công tiềm tàng ngay từ khi chúng xảy ra.

Phản ứng kịp thời: Thời gian phản ứng càng ngắn thì thiệt hại càng được giảm thiểu, đặc biệt trong các sự cố như ransomware hoặc DDoS.

Xây dựng cơ chế phòng thủ linh hoạt: Việc giám sát thường xuyên giúp cải thiện khả năng phòng thủ thông qua phân tích xu hướng và hành vi của các mối đe dọa.

#### 1.2.4.3 Các công cụ giám sát và phát hiện sự cố phổ biến

Dưới đây là các công cụ và công nghệ thường được sử dụng trong giám sát và phát hiện sự cố:

* Hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS):
  + IDS (Intrusion Detection System): Phát hiện các hành vi bất thường trong mạng hoặc hệ thống, đưa ra cảnh báo nhưng không tự động phản ứng.
  + IPS (Intrusion Prevention System): Không chỉ phát hiện mà còn tự động ngăn chặn các hành vi xâm nhập.
  + Ví dụ: Snort (một IDS mã nguồn mở), Suricata.
* SIEM (Security Information and Event Management):
* SIEM là một giải pháp kết hợp giữa quản lý thông tin bảo mật (SIM) và quản lý sự kiện bảo mật (SEM), giúp thu thập, phân tích, và quản lý dữ liệu từ nhiều nguồn khác nhau.

Ví dụ: Splunk, IBM QRadar, ArcSight.

* EDR (Endpoint Detection and Response):
  + Tập trung vào việc giám sát và phản ứng với các mối đe dọa trên các thiết bị đầu cuối như máy tính, máy chủ.
  + Ví dụ: CrowdStrike Falcon, Carbon Black.
* NDR (Network Detection and Response):
  + Giám sát mạng để phát hiện các hoạt động bất thường hoặc mối đe dọa tiềm ẩn.
  + Ví dụ: Darktrace, ExtraHop.
* SOC (Security Operations Center):
  + Trung tâm điều hành an ninh mạng là nơi các chuyên gia bảo mật giám sát và phân tích dữ liệu bảo mật 24/7 để phát hiện và phản ứng với sự cố.
* UEBA (User and Entity Behavior Analytics):
  + Phân tích hành vi của người dùng và thiết bị để phát hiện các hoạt động không bình thường hoặc đáng ngờ.

#### 1.2.4.4 Các phương pháp giám sát sự kiện bảo mật

Thu thập log và phân tích log: Log từ hệ thống, mạng, và ứng dụng được thu thập để phân tích các sự kiện xảy ra.

Phân tích lưu lượng mạng: Giám sát lưu lượng mạng để phát hiện các dấu hiệu tấn công như DDoS, brute force, hoặc truy cập bất thường.

Giám sát thời gian thực: Sử dụng các công cụ cảnh báo ngay lập tức khi phát hiện bất thường.

Phân tích hành vi bất thường: So sánh các hoạt động hiện tại với các hành vi thông thường để phát hiện các mối đe dọa.

#### 1.2.4.5 Các thách thức trong giám sát và phát hiện sự cố

Mặc dù giám sát và phát hiện sự cố là yếu tố quan trọng, nhưng doanh nghiệp vẫn phải đối mặt với nhiều thách thức lớn trong việc thực hiện hiệu quả.

* Lượng dữ liệu lớn: với khối lượng dữ liệu bảo mật khổng lồ từ nhiều nguồn, việc phân tích và lọc thông tin quan trọng đòi hỏi các công cụ mạnh mẽ và chuyên gia có kinh nghiệm. Trong vụ tấn công SolarWinds (2020), lượng dữ liệu log khổng lồ từ các hệ thống bị xâm nhập đã khiến việc phát hiện mã độc bị chậm trễ, dẫn đến kẻ tấn công có thời gian thực hiện hành vi đánh cắp thông tin.
* Cảnh báo giả (False Positive): một trong những thách thức lớn của hệ thống giám sát là đưa ra các cảnh báo không chính xác, gây lãng phí tài nguyên và làm giảm hiệu quả phản ứng. Trường hợp của Colonial Pipeline (2021) cho thấy rằng các cảnh báo không được xử lý kịp thời có thể tạo điều kiện cho ransomware tấn công và gây gián đoạn nghiêm trọng, làm ảnh hưởng đến nguồn cung nhiên liệu ở Hoa Kỳ.
* Thiếu nhân lực và kỹ năng chuyên môn: đội ngũ quản lý an ninh mạng cần có đủ năng lực để vận hành và tối ưu hóa các công cụ giám sát. Sự thiếu hụt này thường làm giảm khả năng phát hiện và phản ứng với các cuộc tấn công tinh vi như vụ SolarWinds, nơi mã độc được ẩn giấu trong chuỗi cung ứng phần mềm, chỉ bị phát hiện sau nhiều tháng.
* Đa dạng mối đe dọa: các mối đe dọa ngày càng tinh vi và khó phát hiện, đòi hỏi các công cụ và phương pháp phải luôn được cập nhật. Tấn công ransomware như ở Colonial Pipeline đã cho thấy sự cần thiết của việc đầu tư vào các công cụ giám sát tiên tiến để phát hiện và ngăn chặn các hành vi bất thường trước khi gây thiệt hại nghiêm trọng.

### 1.2.5 Đào tạo và nâng cao nhận thức bảo mật

Một hệ thống bảo mật chỉ thực sự hiệu quả khi toàn bộ nhân viên trong doanh nghiệp nhận thức được vai trò và trách nhiệm của mình trong việc bảo vệ tài sản và thông tin. Đào tạo và nâng cao nhận thức bảo mật là một phần không thể thiếu trong chiến lược bảo mật tổng thể, nhằm giảm thiểu rủi ro từ yếu tố con người – vốn được xem là mắt xích yếu nhất trong an ninh mạng.

#### 1.2.5.1 Tầm quan trọng của đào tạo bảo mật

Phòng ngừa các hành vi bất cẩn: nhân viên không được đào tạo có thể dễ dàng trở thành nạn nhân của các chiêu thức tấn công như lừa đảo qua email (phishing) hoặc vô tình tải xuống phần mềm độc hại. Việc đào tạo giúp họ nhận diện và tránh các hành vi nguy hiểm.

Phát hiện sớm các mối đe dọa: nhân viên có nhận thức tốt về bảo mật sẽ đóng vai trò như những "cảm biến" đầu tiên, phát hiện các dấu hiệu bất thường trong hệ thống, từ đó kịp thời báo cáo và ngăn chặn các sự cố.

Tuân thủ quy định và chính sách: đào tạo giúp nhân viên hiểu rõ các quy định pháp lý và chính sách bảo mật nội bộ, đảm bảo doanh nghiệp không vi phạm luật pháp, đồng thời tăng cường tính nhất quán trong việc thực hiện các quy trình bảo mật.

#### 1.2.5.2 Các nội dung đào tạo cần thiết

Nhận diện mối đe dọa phổ biến:

* + Lừa đảo qua email, tin nhắn.
  + Tấn công mạng xã hội.
  + Sử dụng phần mềm không an toàn.

Quy trình phản ứng khi phát hiện sự cố:

* + Báo cáo ngay lập tức với bộ phận IT hoặc an ninh mạng.
  + Cách ly hệ thống bị ảnh hưởng để hạn chế lan rộng.
  + Ghi nhận thông tin sự cố để hỗ trợ điều tra.

Sử dụng công cụ bảo mật:

* + Quản lý mật khẩu và xác thực đa yếu tố (MFA).
  + Cách nhận biết các cảnh báo bảo mật từ hệ thống.
  + Quy trình cập nhật phần mềm và bản vá.

Quy tắc làm việc an toàn:

* + Không sử dụng thiết bị cá nhân cho công việc nếu không được phép.
  + Không chia sẻ thông tin nhạy cảm qua các kênh không được bảo mật.
  + Kiểm tra nguồn gốc của tài liệu hoặc liên kết trước khi mở.

#### 1.2.5.3 Lợi ích từ chương trình đào tạo bảo mật

Giảm thiểu rủi ro từ yếu tố con người: Nhân viên có kiến thức và kỹ năng bảo mật giúp giảm nguy cơ lỗi do bất cẩn.

Tăng cường khả năng ứng phó sự cố: Đào tạo giúp nhân viên nhận diện và phản ứng nhanh với các mối đe dọa bảo mật.

Tuân thủ quy định và tiêu chuẩn: Đảm bảo doanh nghiệp đáp ứng yêu cầu về đào tạo bảo mật theo các tiêu chuẩn như ISO/IEC 27001 hoặc GDPR.

Xây dựng văn hóa bảo mật: Tạo môi trường làm việc chú trọng an toàn thông tin, nâng cao trách nhiệm cá nhân và tập thể.

Bảo vệ uy tín doanh nghiệp: Đào tạo nhân viên tốt giúp giảm thiểu sự cố vi phạm bảo mật, giữ vững niềm tin từ khách hàng và đối tác.

#### 1.2.5.4 Thách thức trong việc đào tạo và nâng cao nhận thức bảo mật

Dù đào tạo bảo mật là yếu tố thiết yếu, các doanh nghiệp vẫn đối mặt với nhiều khó khăn trong việc triển khai hiệu quả:

1. Thiếu sự ưu tiên từ ban lãnh đạo

Quan điểm "bảo mật không phải vấn đề chính": Một số lãnh đạo doanh nghiệp coi bảo mật là chi phí thay vì đầu tư, dẫn đến việc không đủ nguồn lực cho các chương trình đào tạo.

Hạn chế ngân sách: Các doanh nghiệp nhỏ và vừa thường gặp khó khăn trong việc đầu tư vào các khóa đào tạo chất lượng cao.

2. Nhân viên không quan tâm hoặc không nhận thức được rủi ro

Tâm lý chủ quan: Nhiều nhân viên cho rằng bảo mật là trách nhiệm của bộ phận IT, dẫn đến thiếu hợp tác hoặc không tham gia tích cực trong các buổi đào tạo.

Nhận thức hạn chế: Một số người không hiểu rõ mức độ nghiêm trọng của các rủi ro bảo mật và nghĩ rằng các mối đe dọa không ảnh hưởng trực tiếp đến họ.

3. Tài liệu và phương pháp đào tạo không hiệu quả

Thiếu thực tiễn: Các tài liệu đào tạo thường tập trung quá nhiều vào lý thuyết mà không cung cấp đủ ví dụ thực tế, làm giảm hiệu quả tiếp thu của nhân viên.

Phương pháp lỗi thời: Nhiều doanh nghiệp vẫn sử dụng các phương pháp đào tạo truyền thống như bài giảng đơn thuần, thay vì ứng dụng công nghệ như e-learning, mô phỏng tấn công, hoặc trò chơi hóa (gamification).

4. Khó khăn trong việc duy trì nhận thức liên tục

Đào tạo một lần rồi bỏ: Nhiều doanh nghiệp tổ chức các buổi đào tạo theo kiểu “làm cho có” mà không duy trì liên tục. Nhận thức bảo mật có thể phai nhạt theo thời gian nếu không được củng cố định kỳ.

Không bắt kịp mối đe dọa mới: Mối đe dọa bảo mật luôn thay đổi và trở nên tinh vi hơn. Việc không cập nhật kịp thời nội dung đào tạo có thể khiến nhân viên không nhận diện được các nguy cơ mới.

5. Thiếu công cụ đo lường hiệu quả đào tạo

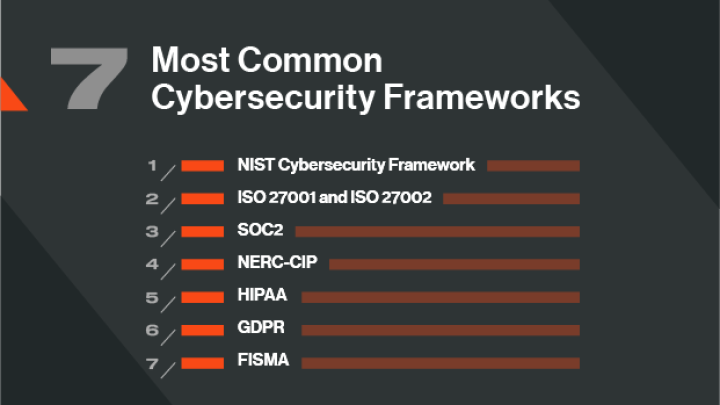
Không có thước đo cụ thể: Nhiều doanh nghiệp không có hệ thống đánh giá hiệu quả của chương trình đào tạo, dẫn đến khó khăn trong việc xác định mức độ nhận thức và cải thiện.

Khó kiểm soát hành vi thực tế: Ngay cả khi đã đào tạo, vẫn khó kiểm soát liệu nhân viên có tuân thủ đúng các quy trình bảo mật trong công việc hàng ngày hay không.

## 1.3. Các tiêu chuẩn và phương pháp bảo mật phổ biến

### 1.3.1 Tiêu chuẩn bảo mật

Các tiêu chuẩn bảo mật cung cấp khung làm việc và hướng dẫn thực hành tốt nhất để thiết lập, triển khai và quản lý hệ thống an ninh thông tin trong doanh nghiệp. Phần này sẽ giới thiệu một số tiêu chuẩn phổ biến và vai trò của chúng trong việc tăng cường bảo mật.



*Hình 1.5: Một số tiêu chuẩn bảo mật phổ biến*

#### 1.3.1.1 ISO/IEC 27001

ISO/IEC 27001 là tiêu chuẩn quốc tế cho hệ thống quản lý an ninh thông tin (ISMS), cung cấp phương pháp tiếp cận có hệ thống để quản lý thông tin nhạy cảm.

Phạm vi: Tập trung vào bảo vệ ba khía cạnh chính: tính bảo mật (confidentiality), tính toàn vẹn (integrity), và tính sẵn sàng (availability) của thông tin.

Lợi ích:

* + Giúp doanh nghiệp tuân thủ các yêu cầu pháp lý.
  + Tăng cường niềm tin từ khách hàng và đối tác.
  + Cải thiện quản lý rủi ro bảo mật.

#### 1.3.1.2 NIST Cybersecurity Framework

Được phát triển bởi Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST), khung bảo mật này hỗ trợ các tổ chức quản lý và giảm thiểu rủi ro bảo mật mạng.

Phạm vi: Gồm 5 chức năng chính: Identify (Nhận diện), Protect (Bảo vệ), Detect (Phát hiện), Respond (Phản ứng), và Recover (Phục hồi).

Lợi ích:

* + Cung cấp một khung chuẩn hóa dễ hiểu cho mọi loại hình doanh nghiệp.
  + Tăng khả năng ứng phó với sự cố và phục hồi sau tấn công.
  + Linh hoạt áp dụng tùy theo quy mô và ngành nghề.

#### 1.3.1.3 CIS Controls

Bộ kiểm soát bảo mật do Trung tâm An ninh Internet (CIS) phát triển, gồm 18 biện pháp bảo mật cụ thể nhằm giúp doanh nghiệp giảm thiểu các mối đe dọa an ninh mạng phổ biến.

Phạm vi: Bao gồm các lĩnh vực từ quản lý tài sản (Asset Management) đến giám sát liên tục (Continuous Monitoring).

Lợi ích:

* Dễ triển khai với các hướng dẫn cụ thể.
* Ưu tiên các biện pháp bảo mật có tác động lớn nhất đến rủi ro.
* Tích hợp tốt với các tiêu chuẩn khác như NIST hoặc ISO.

#### 1.3.1.4 PCI DSS (Payment Card Industry Data Security Standard)

Một tiêu chuẩn bảo mật bắt buộc dành cho các tổ chức xử lý, lưu trữ, hoặc truyền thông tin thẻ thanh toán.

Phạm vi: Gồm 12 yêu cầu chính như mã hóa dữ liệu thẻ, kiểm soát truy cập, và giám sát mạng.

Lợi ích:

* + Bảo vệ dữ liệu thanh toán khỏi tấn công mạng.
  + Giảm thiểu rủi ro bị phạt do vi phạm bảo mật thông tin thẻ.
  + Tăng niềm tin của khách hàng khi sử dụng dịch vụ thanh toán điện tử.

#### 1.3.1.5 GDPR (General Data Protection Regulation)

Quy định chung về bảo vệ dữ liệu của Liên minh Châu Âu, áp dụng cho tất cả các tổ chức thu thập hoặc xử lý dữ liệu cá nhân của công dân EU.

Phạm vi: Yêu cầu doanh nghiệp phải bảo mật dữ liệu cá nhân, đảm bảo quyền của người dùng như quyền truy cập, quyền bị lãng quên (right to be forgotten).

Lợi ích:

* + Giảm thiểu nguy cơ bị kiện tụng và phạt tiền do vi phạm quyền riêng tư.
  + Cải thiện quy trình xử lý dữ liệu và bảo vệ thông tin khách hàng.

#### 1.3.1.6 TISAX (Trusted Information Security Assessment Exchange)

Một tiêu chuẩn bảo mật thông tin được phát triển dành riêng cho ngành công nghiệp ô tô, tập trung vào việc đánh giá bảo mật thông tin giữa các nhà cung cấp và đối tác.

Phạm vi: Đảm bảo an toàn trong trao đổi dữ liệu, đặc biệt trong các chuỗi cung ứng phức tạp.

Lợi ích:

* + Tăng cường bảo mật chuỗi cung ứng.
  + Đáp ứng yêu cầu từ các đối tác lớn trong ngành ô tô.

#### 1.3.1.7 Vai trò của tiêu chuẩn bảo mật trong doanh nghiệp

Chuẩn hóa quy trình: Giúp doanh nghiệp xây dựng hệ thống bảo mật đồng bộ và nhất quán.

Quản lý rủi ro: Các tiêu chuẩn giúp xác định, đánh giá, và giảm thiểu các rủi ro bảo mật một cách hệ thống.

Tăng cường uy tín: Doanh nghiệp tuân thủ các tiêu chuẩn quốc tế sẽ tạo niềm tin lớn hơn với khách hàng và đối tác.

Hỗ trợ phát triển: Một hệ thống bảo mật mạnh mẽ và tuân thủ tiêu chuẩn tạo nền tảng vững chắc cho việc mở rộng quy mô và hội nhập quốc tế.

### 1.3.2 Các phương pháp bảo mật

Phương pháp bảo mật là tập hợp các nguyên tắc và chiến lược giúp doanh nghiệp giảm thiểu rủi ro, đối phó hiệu quả với các mối đe dọa an ninh mạng.

#### 1.3.2.1 Defense in Depth (Phòng thủ nhiều lớp)

Defense in Depth là chiến lược bảo mật dựa trên việc triển khai nhiều lớp bảo vệ trong hệ thống, nhằm tăng cường khả năng phòng thủ trước các mối đe dọa.

Nguyên tắc:

* + Lớp bảo vệ vật lý: Kiểm soát truy cập tại các khu vực chứa thiết bị CNTT, ví dụ như khóa cửa, camera giám sát.
  + Lớp bảo vệ mạng: Sử dụng tường lửa (firewall), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS).
  + Lớp bảo vệ ứng dụng: Cấu hình bảo mật trên phần mềm, kiểm tra mã nguồn, vá lỗi bảo mật thường xuyên.
  + Lớp bảo vệ dữ liệu: Mã hóa dữ liệu, quản lý quyền truy cập.
  + Lớp bảo vệ con người: Đào tạo nhận thức bảo mật cho nhân viên.

Lợi ích:

* + Tăng khả năng phát hiện và ngăn chặn các cuộc tấn công phức tạp.
  + Giảm thiểu tác động khi một lớp phòng thủ bị xâm nhập.

#### 1.3.2.2 Zero Trust Architecture (Kiến trúc Không Tin Tưởng)

Zero Trust là phương pháp bảo mật không tin tưởng vào bất kỳ thiết bị, người dùng, hay ứng dụng nào ngay cả khi chúng nằm trong mạng nội bộ.

Nguyên tắc:

* + Xác thực liên tục: Tất cả các yêu cầu truy cập phải được xác thực, bất kể nguồn gốc.
  + Quyền truy cập tối thiểu: Người dùng chỉ được cấp quyền truy cập tối thiểu cần thiết để thực hiện công việc.
  + Giám sát liên tục: Theo dõi và ghi nhận mọi hoạt động để phát hiện kịp thời các hành vi bất thường.

Lợi ích:

* + Giảm nguy cơ tấn công từ nội bộ.
  + Bảo vệ tốt hơn trước các cuộc tấn công mạng phức tạp.
  + Phù hợp với mô hình làm việc từ xa và các dịch vụ đám mây.

#### 1.3.2.3 Least Privilege (Quyền Tối Thiểu)

Chỉ cấp quyền truy cập cần thiết cho người dùng hoặc ứng dụng để thực hiện nhiệm vụ cụ thể, hạn chế quyền không cần thiết.

Lợi ích:

* + Giảm thiểu nguy cơ xâm phạm khi tài khoản bị chiếm đoạt.
  + Hạn chế phạm vi của các cuộc tấn công mạng.

#### 1.3.2.4 Segmentation (Phân đoạn mạng)

Chia mạng doanh nghiệp thành các phân đoạn nhỏ, cô lập từng vùng mạng để ngăn chặn tấn công lan rộng.

Phạm vi:

* + Phân đoạn mạng theo phòng ban hoặc chức năng (ví dụ: phân vùng mạng cho HR, IT, và khách hàng).
  + Sử dụng VLAN, VPN, hoặc các công nghệ SDN (Software-Defined Networking).

Lợi ích:

* + Tăng cường kiểm soát truy cập giữa các vùng mạng.
  + Giảm thiểu thiệt hại khi một phân đoạn bị xâm nhập.

#### 1.3.2.5 Threat Hunting (Săn lùng mối đe dọa)

Phương pháp bảo mật chủ động, tập trung vào việc tìm kiếm các mối đe dọa tiềm ẩn trong hệ thống trước khi chúng gây ra sự cố.

Quy trình:

* + Xây dựng giả thuyết dựa trên các hành vi đáng ngờ.
  + Thu thập và phân tích dữ liệu hệ thống.
  + Phát hiện và loại bỏ các mối đe dọa.

Lợi ích:

* + Phát hiện các cuộc tấn công chưa được biết đến.
  + Nâng cao khả năng phòng thủ chủ động.

#### 1.3.2.6 Multi-Factor Authentication (Xác thực đa yếu tố)

Sử dụng từ hai phương thức xác thực trở lên để đảm bảo rằng chỉ những người dùng hợp pháp mới có quyền truy cập.

Ví dụ:

* + Thông tin bạn biết (mật khẩu).
  + Thứ bạn có (OTP, thẻ bảo mật).
  + Điều bạn là (dấu vân tay, nhận diện khuôn mặt).



*Hình 1.6: Công nghệ xác thực bằng khuôn mặt- FaceID của Apple*

Lợi ích:

* + Bảo vệ tốt hơn trước các cuộc tấn công vào tài khoản người dùng.
  + Giảm nguy cơ từ các hành vi lừa đảo và đánh cắp thông tin xác thực.
  + Vai trò của các phương pháp bảo mật
  + Tăng khả năng phòng thủ: Các phương pháp bảo mật giúp xây dựng hệ thống phòng thủ nhiều lớp, giảm nguy cơ bị xâm nhập.
  + Đáp ứng các yêu cầu pháp lý và tiêu chuẩn: Các phương pháp này thường tích hợp tốt với các tiêu chuẩn bảo mật như ISO 27001, NIST.
  + Phù hợp với môi trường hiện đại: Nhiều phương pháp bảo mật, như Zero Trust và MFA, đặc biệt phù hợp với môi trường làm việc từ xa và xu hướng chuyển đổi số.

### 1.3.3 Tuân thủ và đánh giá bảo mật

Để đảm bảo rằng hệ thống bảo mật của doanh nghiệp luôn được vận hành hiệu quả và đáp ứng các yêu cầu pháp lý, việc tuân thủ và đánh giá bảo mật là yếu tố quan trọng. Dưới đây là các phương pháp và quy trình đánh giá phổ biến:

#### 1.3.3.1 Tuân thủ bảo mật

Tuân thủ bảo mật là việc áp dụng và duy trì các tiêu chuẩn, quy định, và chính sách bảo mật bắt buộc trong ngành hoặc quốc gia.

Các yêu cầu tuân thủ phổ biến:

* + GDPR (General Data Protection Regulation): Quy định về bảo vệ dữ liệu cá nhân tại Liên minh Châu Âu.
  + HIPAA (Health Insurance Portability and Accountability Act): Quy định bảo mật dữ liệu y tế tại Hoa Kỳ.
  + PCI DSS (Payment Card Industry Data Security Standard): Tiêu chuẩn bảo mật cho giao dịch thẻ tín dụng.
  + ISO/IEC 27001: Hệ thống quản lý an ninh thông tin quốc tế.

#### 1.3.3.2 Kiểm tra bảo mật (Security Testing)

Đánh giá tính an toàn của hệ thống thông qua các phương pháp kiểm tra, nhằm phát hiện các lỗ hổng và khắc phục trước khi chúng bị khai thác.

Các loại kiểm tra:

* + Kiểm tra hộp đen (Black Box Testing): Đánh giá hệ thống từ góc nhìn của kẻ tấn công không có thông tin nội bộ.
  + Kiểm tra hộp trắng (White Box Testing): Kiểm tra hệ thống với đầy đủ thông tin, như mã nguồn, cấu trúc mạng.
  + Kiểm tra hộp xám (Gray Box Testing): Kết hợp cả hai phương pháp trên, với một phần thông tin về hệ thống.
  + Penetration Testing (Kiểm thử xâm nhập): Mô phỏng các cuộc tấn công thực tế để xác định và khai thác lỗ hổng.

#### 1.3.3.3 Đánh giá nguy cơ (Risk Assessment)

Xác định, phân tích, và đánh giá các nguy cơ tiềm ẩn có thể ảnh hưởng đến an ninh thông tin của doanh nghiệp.

Quy trình:

* + Xác định tài sản (Asset Identification): Liệt kê các tài sản quan trọng như dữ liệu, phần cứng, phần mềm.
  + Xác định mối đe dọa (Threat Identification): Phân tích các mối đe dọa tiềm năng từ bên trong và bên ngoài.
  + Phân tích lỗ hổng (Vulnerability Analysis): Đánh giá các lỗ hổng trong hệ thống bảo mật.
  + Đánh giá tác động (Impact Assessment): Xác định hậu quả tiềm năng khi nguy cơ trở thành hiện thực.
  + Ưu tiên hóa nguy cơ (Risk Prioritization): Phân loại nguy cơ dựa trên mức độ nghiêm trọng và khả năng xảy ra.
  + Đề xuất biện pháp (Mitigation Strategies): Lập kế hoạch giảm thiểu nguy cơ.

#### 1.3.3.4 Đánh giá bảo mật liên tục

Đây là phương pháp giám sát và đánh giá bảo mật liên tục để đảm bảo hệ thống luôn ở trạng thái an toàn trước các mối đe dọa mới.

Công cụ hỗ trợ:

* + SIEM (Security Information and Event Management): Tích hợp và phân tích dữ liệu bảo mật từ nhiều nguồn để phát hiện sự cố.
  + Threat Intelligence: Thu thập thông tin về các mối đe dọa đang diễn ra trên toàn cầu.
  + Bảng điểm bảo mật (Security Scorecard): Đánh giá mức độ bảo mật của hệ thống bằng các chỉ số định lượng.

#### 1.3.3.5 Kiểm tra tuân thủ và kiểm toán bảo mật

Kiểm tra tuân thủ (Compliance Audit):

* + Đảm bảo hệ thống đáp ứng các yêu cầu pháp lý và tiêu chuẩn bảo mật.
  + Thường được thực hiện bởi các cơ quan hoặc đơn vị độc lập.

Kiểm toán bảo mật (Security Audit):

* + Đánh giá toàn diện các chính sách, quy trình, và công nghệ bảo mật.
  + Xác định các điểm yếu và đề xuất cải thiện.

#### 1.3.3.6 Nhận định chung

Việc tuân thủ và đánh giá bảo mật không chỉ là trách nhiệm pháp lý mà còn giúp doanh nghiệp:

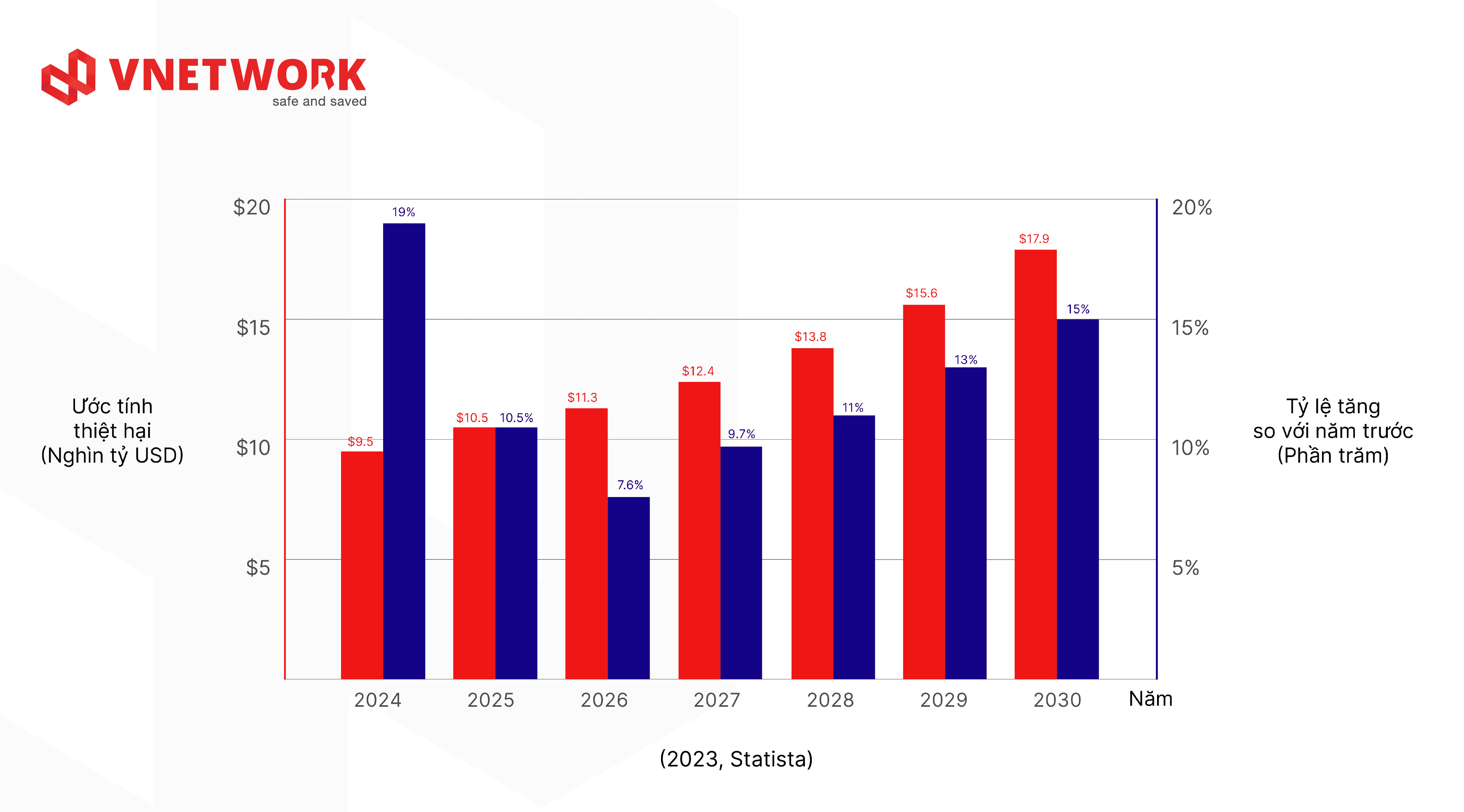
* + Nâng cao khả năng phòng thủ trước các mối đe dọa.
  + Đảm bảo niềm tin từ khách hàng, đối tác, và cổ đông.
  + Hạn chế thiệt hại tài chính và danh tiếng từ các sự cố bảo mật.

## 1.4. Các loại tấn công và lỗ hổng bảo mật phổ biến

### 1.4.1 Tấn công mạng

#### 1.4.1.1 Khái niệm

Tấn công mạng là hành động xâm nhập trái phép vào các hệ thống, mạng lưới hoặc thiết bị máy tính nhằm đánh cắp dữ liệu, gây gián đoạn hoạt động hoặc khai thác tài nguyên. Các cuộc tấn công mạng thường dựa vào lỗ hổng bảo mật hoặc sự bất cẩn trong cấu hình hệ thống.

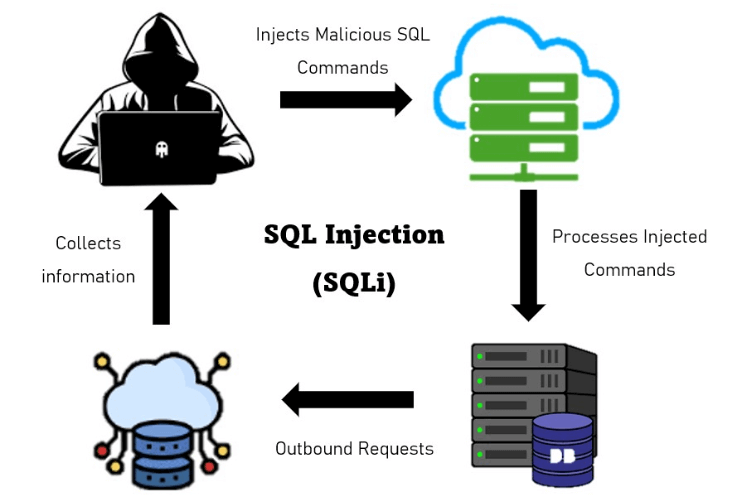


*Hình 1.7: Thiệt hại ước tính do tấn công mạng*

#### 1.4.1.2 Phân loại các loại tấn công mạng

1. SQL Injection (Tấn công chèn SQL)

Cách thức: Hacker chèn các câu lệnh SQL độc hại vào ứng dụng web thông qua các trường nhập liệu (form) hoặc URL để truy cập cơ sở dữ liệu trái phép.



*Hình 1.8: Sơ đồ tấn công SQL Injection*

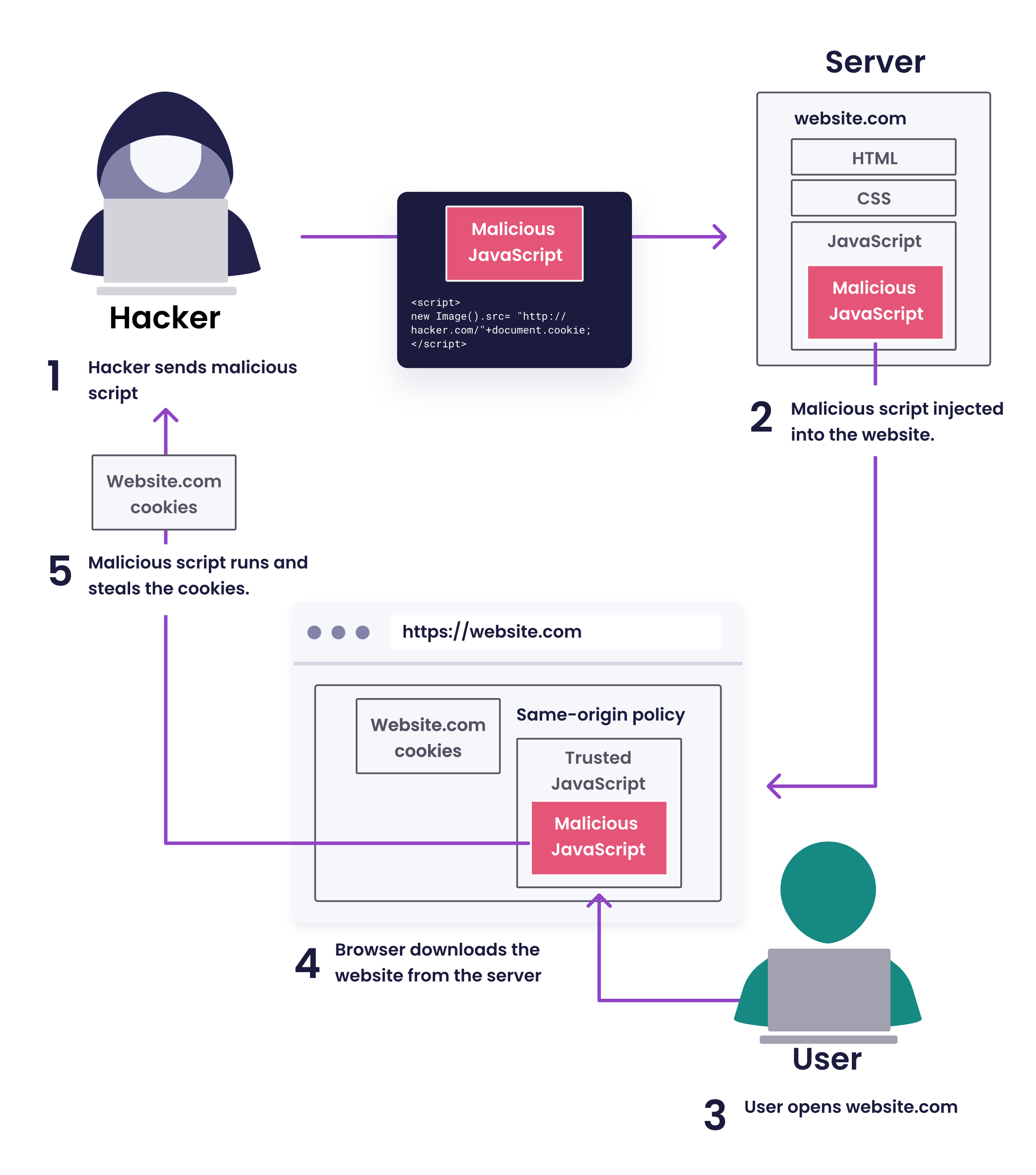
Hậu quả:

* + Lấy cắp dữ liệu nhạy cảm (thông tin khách hàng, tài khoản).
  + Xóa hoặc sửa đổi dữ liệu trong cơ sở dữ liệu.

Ví dụ: Một trang web thương mại điện tử không xác thực đầu vào có thể bị hacker khai thác để trích xuất danh sách khách hàng cùng thông tin thanh toán.

1. Cross-Site Scripting (XSS)

Cách thức: Hacker chèn mã JavaScript độc hại vào các trang web không xác thực hoặc làm sạch đầu vào, gây ra tình trạng chiếm đoạt phiên làm việc (session hijacking) hoặc tấn công người dùng khác.



*Hình 1.9: Sơ đồ tấn công XSS*

Hậu quả:

* + Đánh cắp cookie, thông tin đăng nhập.
  + Tấn công trình duyệt của người dùng, chuyển hướng đến trang web độc hại.

Ví dụ: Hacker chèn mã XSS vào phần bình luận trên một diễn đàn. Khi người dùng khác truy cập, mã độc sẽ thực thi và gửi cookie của họ đến hacker.

1. Tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS)

Cách thức: Gửi lượng lớn yêu cầu giả mạo đến hệ thống mục tiêu, làm quá tải tài nguyên và khiến dịch vụ không thể truy cập được.

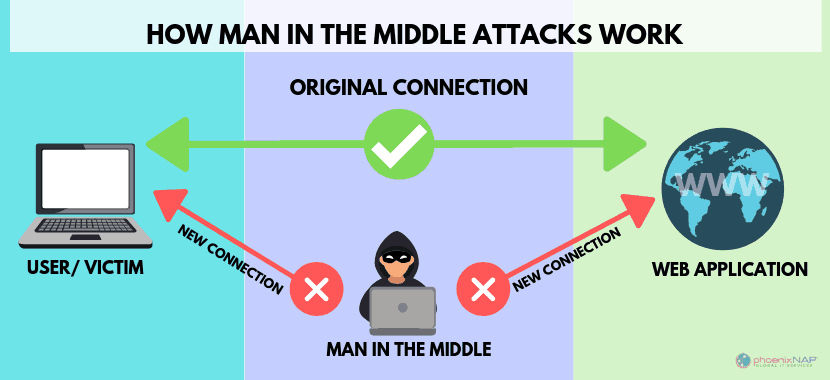
Hậu quả:

* + Gián đoạn hoạt động kinh doanh.
  + Mất doanh thu và uy tín.

Ví dụ: Một trang web thương mại bị "đánh sập" trong ngày khuyến mãi do lượng truy cập giả mạo từ một cuộc tấn công DDoS.

1. Man-in-the-Middle (MITM)

Cách thức: Kẻ tấn công chặn luồng dữ liệu giữa hai bên giao tiếp (ví dụ: giữa trình duyệt và máy chủ), sau đó đọc hoặc sửa đổi dữ liệu này.



*Hình 1.10: Sơ đồ tấn công MITM*

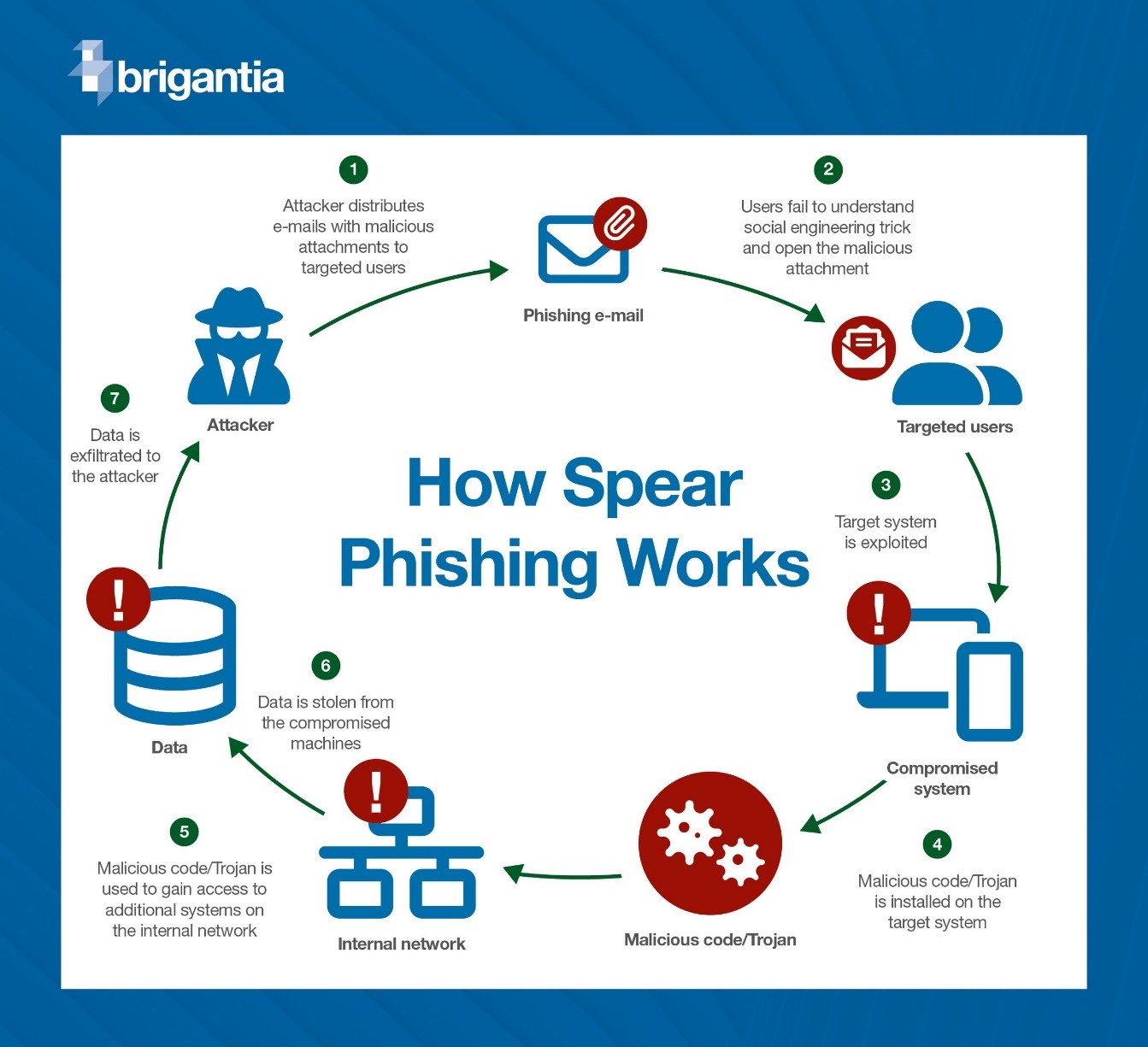
Hậu quả:

* + Đánh cắp thông tin nhạy cảm như mật khẩu hoặc chi tiết thẻ tín dụng.
  + Tấn công chuyển hướng hoặc thao túng dữ liệu.

Ví dụ: Một người dùng kết nối Wi-Fi công cộng không được mã hóa có thể bị kẻ tấn công chặn thông tin đăng nhập email.

1. Phishing và Spear Phishing

Cách thức: Gửi email, tin nhắn lừa đảo chứa liên kết độc hại hoặc tài liệu giả mạo nhằm đánh lừa nạn nhân cung cấp thông tin cá nhân.



*Hình 1.11: Sơ đồ tấn công Spear Phishing*

Hậu quả:

* + Đánh cắp thông tin đăng nhập, tài khoản ngân hàng.
  + Gây ra sự xâm nhập sâu hơn vào hệ thống doanh nghiệp.

Ví dụ: Một nhân viên nhận email giả mạo từ "bộ phận IT" yêu cầu nhập mật khẩu để "cập nhật bảo mật."

#### 1.4.1.3 Biện pháp phòng chống

Áp dụng chính sách bảo mật:

* + Xác thực và làm sạch đầu vào (Input Validation) để chống SQL Injection và XSS.
  + Sử dụng tường lửa ứng dụng web (WAF) để ngăn chặn các cuộc tấn công mạng.

Mã hóa dữ liệu:

* + Áp dụng giao thức HTTPS để bảo vệ luồng dữ liệu khỏi MITM.

Giám sát và phát hiện:

* + Sử dụng các hệ thống giám sát mạng (IDS/IPS) để phát hiện và ngăn chặn tấn công bất thường.

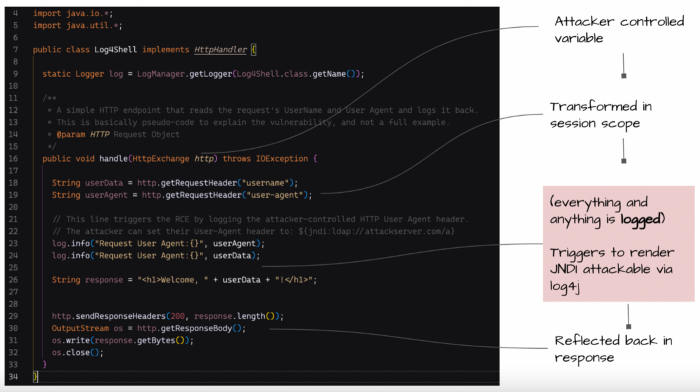
Đào tạo nhân viên:

* + Nâng cao nhận thức về các email và liên kết lừa đảo (phishing).

### 1.4.2 Lỗ hổng bảo mật trong phần mềm

#### 1.4.2.1 Khái niệm

Lỗ hổng bảo mật trong phần mềm là những yếu điểm hoặc lỗi trong mã nguồn của phần mềm, ứng dụng hoặc hệ điều hành mà kẻ tấn công có thể khai thác để thực hiện các hành vi tấn công, như xâm nhập hệ thống, đánh cắp dữ liệu hoặc gây gián đoạn hoạt động. Những lỗ hổng này có thể do lỗi lập trình, thiếu sót trong thiết kế, hoặc do sự thiếu sót trong việc cập nhật phần mềm.

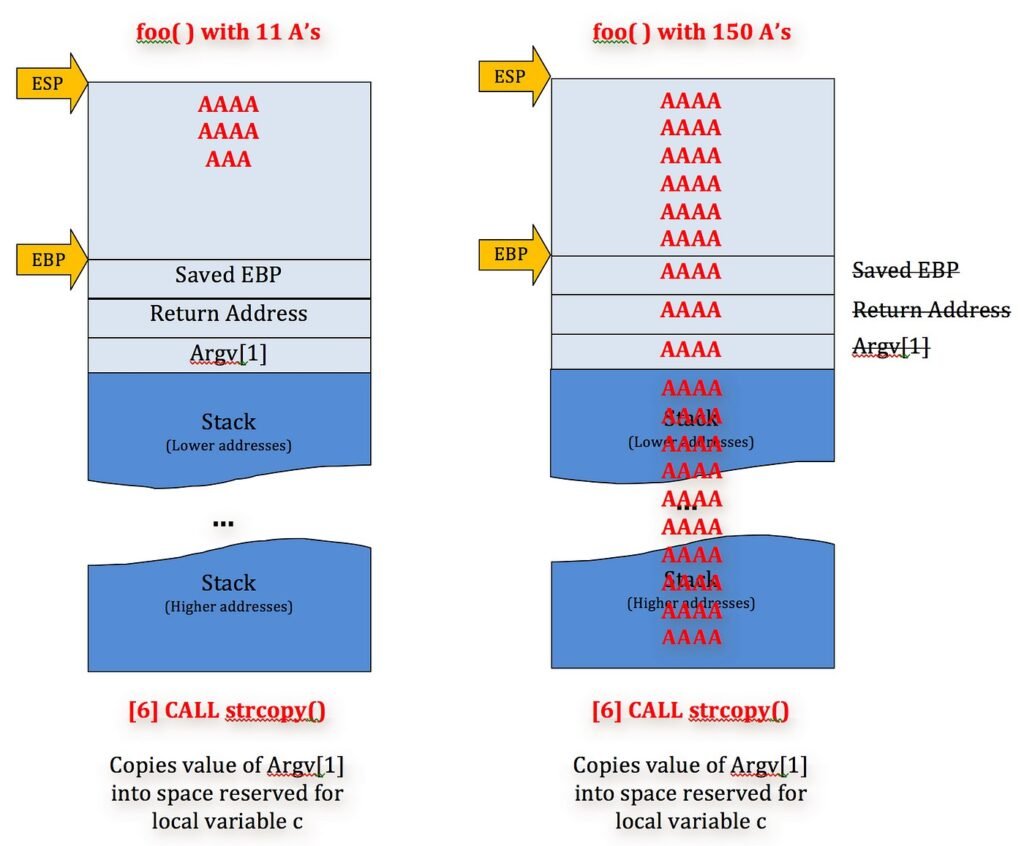


*Hình 1.12: Lỗ hổng Log4shell ảnh hưởng đến hàng triệu ứng dụng và dịch vụ*

#### Phân loại các loại lỗ hổng bảo mật trong phần mềm

1. Lỗi Buffer Overflow (Tràn bộ đệm)

Cách thức: Lỗi này xảy ra khi một chương trình cố gắng ghi dữ liệu vào bộ nhớ vượt quá phạm vi của bộ đệm đã được cấp phát. Điều này có thể khiến phần mềm thực thi mã độc hại hoặc ghi đè lên dữ liệu quan trọng.



*Hình 1.13: Mô phỏng lỗi tràn bộ đệm*

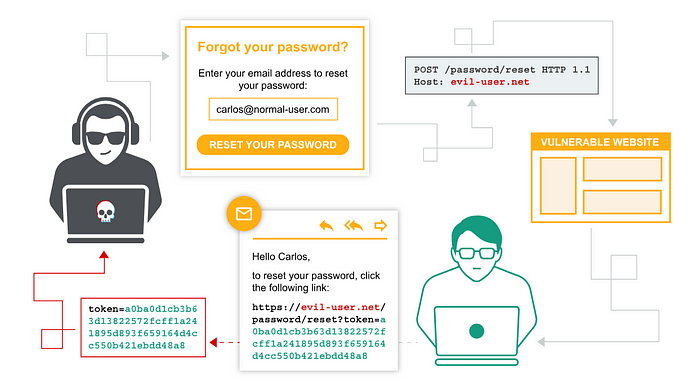
Hậu quả:

* + Chiếm quyền điều khiển của hệ thống.
  + Thực thi mã độc gây hại, thậm chí phá hủy dữ liệu.

Ví dụ: Lỗi tràn bộ đệm trong một ứng dụng cũ có thể cho phép kẻ tấn công thực thi mã từ xa, dẫn đến chiếm quyền điều khiển hệ thống.

1. Lỗi xác thực (Authentication Flaws)

Cách thức: Các lỗi xác thực có thể xuất hiện khi hệ thống không kiểm tra đầy đủ hoặc không an toàn các thông tin đăng nhập của người dùng. Điều này tạo cơ hội cho kẻ tấn công vượt qua cơ chế bảo mật mà không cần đúng thông tin.



*Hình 1.14: Sơ đồ tấn công vượt qua cơ chế xác thực*

Hậu quả:

* + Truy cập trái phép vào tài khoản người dùng hoặc hệ thống nhạy cảm.
  + Tấn công brute force hoặc dictionary attack.

Ví dụ: Hệ thống không áp dụng chính sách mật khẩu mạnh hoặc không sử dụng xác thực đa yếu tố (MFA), khiến hacker có thể dễ dàng đoán được mật khẩu và truy cập vào tài khoản.

1. Lỗi SQL Injection

Cách thức: Lỗi SQL Injection xảy ra khi một ứng dụng web không kiểm tra kỹ đầu vào của người dùng và cho phép các câu lệnh SQL độc hại được chèn vào truy vấn cơ sở dữ liệu.

Hậu quả:

* + Lấy cắp, thay đổi hoặc xóa dữ liệu trong cơ sở dữ liệu.
  + Thực thi mã độc, chiếm quyền truy cập.

Ví dụ: Một ứng dụng web có trường tìm kiếm không bảo vệ có thể bị khai thác để thực hiện SQL Injection, truy xuất thông tin người dùng hoặc dữ liệu quan trọng khác.

1. Lỗi XSS (Cross-Site Scripting)

Cách thức: Lỗi XSS xuất hiện khi ứng dụng không làm sạch đúng cách các dữ liệu đầu vào, cho phép mã JavaScript độc hại được thực thi trên trình duyệt của người dùng khác.

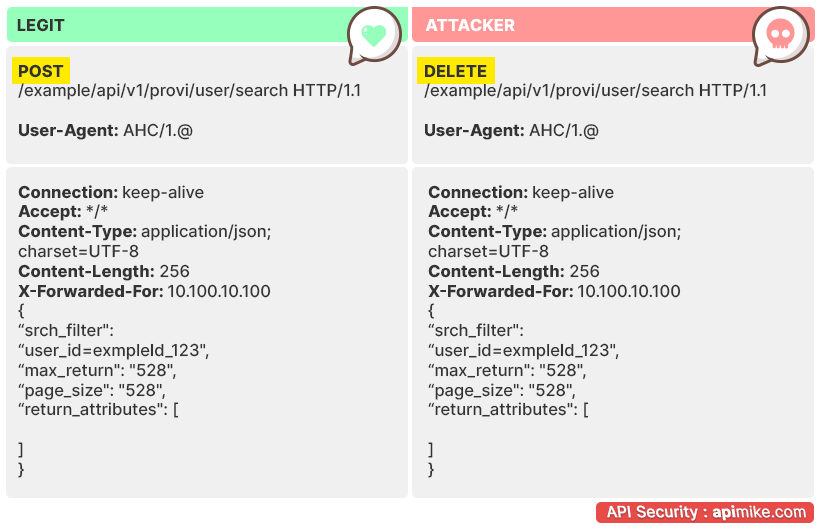
Hậu quả:

* + Đánh cắp cookie hoặc thông tin đăng nhập.
  + Thực hiện hành vi giả mạo người dùng (session hijacking).

Ví dụ: Một trang web e-commerce không lọc đúng đầu vào người dùng trong phần bình luận và bị hacker chèn mã JavaScript, khiến những người dùng truy cập trang đó bị đánh cắp thông tin tài khoản.

1. Lỗi trong API (API Flaws)

Cách thức: Các lỗi trong API xảy ra khi giao diện lập trình ứng dụng không bảo vệ tốt hoặc không thực hiện các biện pháp bảo mật như xác thực quyền truy cập, mã hóa dữ liệu.



*Hình 1.15: Ví dụ về tấn công mạng thông qua xác thực API*

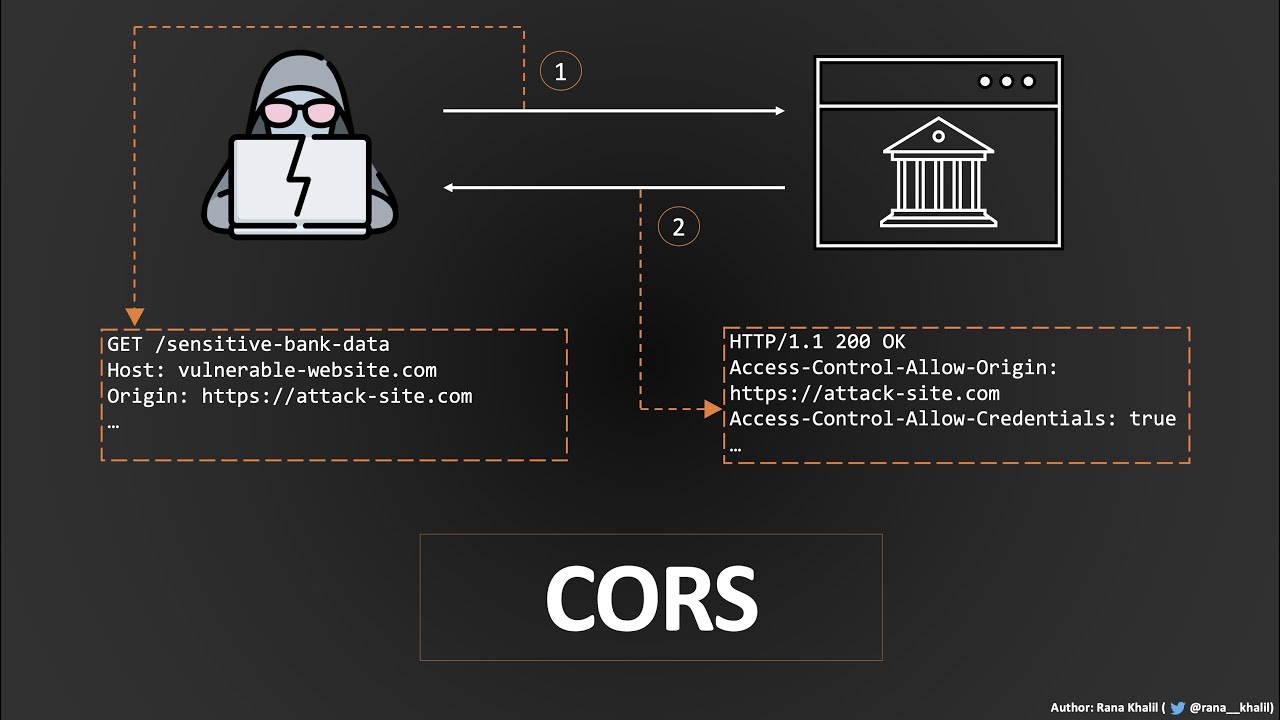
Hậu quả:

* + Truy cập trái phép vào các dịch vụ và dữ liệu qua API.
  + Tiết lộ thông tin nhạy cảm hoặc tấn công các dịch vụ web.

Ví dụ: Một API không xác thực quyền người dùng có thể cho phép hacker thực hiện thao tác không được phép, như xóa dữ liệu hoặc truy cập thông tin người dùng.

1. Lỗi CORS (Cross-Origin Resource Sharing)

Cách thức: Lỗi CORS xảy ra khi các chính sách chia sẻ tài nguyên giữa các nguồn (cross-origin) không được cấu hình chính xác, cho phép kẻ tấn công truy cập vào dữ liệu của người dùng từ một nguồn không đáng tin cậy.



*Hình 1.16: Lấy cắp dữ liệu thông qua CORS*

Hậu quả:

* + Truy cập trái phép vào thông tin người dùng từ các nguồn không đáng tin cậy.

Ví dụ: Một ứng dụng web không cấu hình CORS đúng cách có thể cho phép hacker từ một trang web độc hại gửi yêu cầu API và lấy dữ liệu của người dùng từ một trang web hợp pháp.

#### 1.4.2.3 Biện pháp phòng chống các lỗ hổng bảo mật trong phần mềm

Kiểm tra và làm sạch đầu vào (Input Validation and Sanitization): Cần kiểm tra tất cả dữ liệu đầu vào để đảm bảo không có các lệnh hoặc dữ liệu độc hại, đặc biệt là trong các trường hợp người dùng nhập liệu.

Áp dụng nguyên tắc bảo mật ngay từ khi thiết kế (Secure by Design): Xây dựng phần mềm với các nguyên tắc bảo mật ngay từ đầu, giảm thiểu các lỗ hổng có thể xuất hiện trong quá trình phát triển.

Cập nhật phần mềm thường xuyên: Thực hiện các bản vá bảo mật kịp thời để ngăn ngừa hacker khai thác các lỗ hổng đã biết.

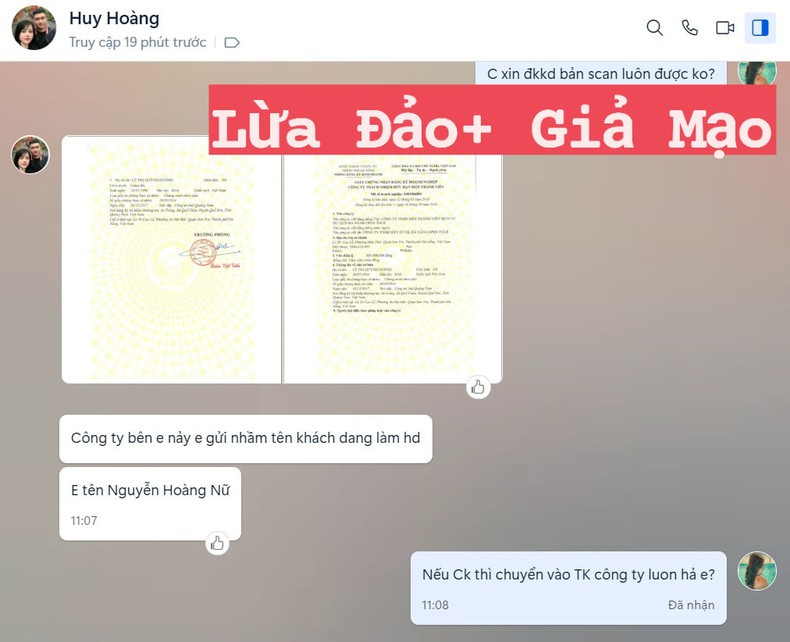
Xác thực mạnh mẽ: Triển khai xác thực đa yếu tố (MFA) và chính sách mật khẩu mạnh để bảo vệ hệ thống khỏi các cuộc tấn công truy cập trái phép.

Sử dụng các công cụ kiểm tra bảo mật: Sử dụng công cụ kiểm tra lỗ hổng tự động để phát hiện các điểm yếu trong phần mềm, giúp tăng cường khả năng phòng thủ.

### 1.4.3 Tấn công xã hội (Social Engineering)

#### 1.4.3.1 Khái niệm

Tấn công xã hội (Social Engineering) là hình thức tấn công dựa trên việc thao túng tâm lý con người để xâm nhập hệ thống, lấy cắp thông tin, hoặc thực hiện các hành vi phi pháp mà không cần trực tiếp phá vỡ các cơ chế bảo mật kỹ thuật. Đây là một trong những hình thức tấn công phổ biến nhất, lợi dụng yếu tố con người – mắt xích yếu nhất trong hệ thống bảo mật.



*Hình 1.17: Lừa đảo tour du lịch giá rẻ qua mạng xã hội*

#### 1.4.3.2 Các phương pháp tấn công xã hội phổ biến

1. Phishing (Lừa đảo qua email)

Cách thức: Tin tặc gửi email giả mạo từ nguồn đáng tin cậy để lừa nạn nhân cung cấp thông tin nhạy cảm như mật khẩu, thông tin thẻ tín dụng, hoặc tải xuống mã độc.

Ví dụ: Một email giả danh ngân hàng yêu cầu xác minh thông tin tài khoản, dẫn đến trang web giả mạo để thu thập thông tin đăng nhập.

1. Spear Phishing (Lừa đảo có mục tiêu)

Cách thức: Phishing nhắm mục tiêu vào một cá nhân hoặc tổ chức cụ thể bằng cách cá nhân hóa nội dung tấn công để tăng tính thuyết phục.

Ví dụ: Email gửi đến một nhân viên cấp cao, giả danh CEO yêu cầu chuyển khoản gấp với lý do khẩn cấp.

1. Vishing (Voice Phishing – Lừa đảo qua điện thoại)

Cách thức: Tin tặc gọi điện giả danh các tổ chức như ngân hàng, cơ quan chính phủ hoặc nhà cung cấp dịch vụ để lừa nạn nhân cung cấp thông tin nhạy cảm.

Ví dụ: Một cuộc gọi giả danh công an yêu thông báo rằng bạn đang liên quan đến một vụ án hoặc chưa hoàn thiện hồ sơ và yêu cầu cài đặt ứng dụng độc hại nhằm đánh cắp thông tin ngân hàng hoặc chuyển tiền để ứng trước thủ tục pháp lý.

1. Tailgating (Theo đuôi)

Cách thức: Kẻ tấn công lợi dụng sự lịch sự hoặc bất cẩn của nhân viên để theo đuôi vào các khu vực được bảo vệ mà không có quyền truy cập hợp lệ.

Ví dụ: Một người mang theo đồ giao hàng đi theo nhân viên vào khu vực kiểm soát ra vào mà không cần trình thẻ.

1. Pretexting (Dựng tình huống giả)

Cách thức: Kẻ tấn công tạo ra một câu chuyện giả mạo để giành được lòng tin của nạn nhân, sau đó khai thác thông tin hoặc thực hiện các hành vi trái phép.

Ví dụ: Giả danh nhân viên hỗ trợ CNTT gọi đến yêu cầu cung cấp mật khẩu để sửa lỗi hệ thống.

1. Baiting (Nhử mồi)

Cách thức: Kẻ tấn công cung cấp một "mồi nhử" hấp dẫn, như ổ USB chứa mã độc hoặc một file tải về miễn phí, để dụ người dùng tự nguyện thực hiện hành vi gây hại.

Ví dụ: Một ổ USB có nhãn "Thông tin lương nhân viên" bị bỏ quên tại văn phòng khiến nhân viên tò mò cắm vào máy tính của họ.

#### 1.4.3.3 Hậu quả của tấn công xã hội

Đánh cắp thông tin nhạy cảm: Các cuộc tấn công xã hội thường nhằm lấy cắp mật khẩu, thông tin cá nhân hoặc dữ liệu tài chính.

Gây tổn thất tài chính: Các giao dịch gian lận hoặc lừa đảo tài chính thông qua phishing hoặc vishing có thể gây thiệt hại lớn.

Làm gián đoạn hoạt động: Việc lây nhiễm mã độc thông qua nhử mồi hoặc phishing có thể làm hỏng hệ thống và gây gián đoạn hoạt động kinh doanh.

Ảnh hưởng uy tín: Sự vi phạm bảo mật liên quan đến con người có thể làm suy giảm lòng tin của khách hàng và đối tác.



*Hình 1.18: Mất cả tỷ đồng vì “Lệnh bắt có dấu mộc đỏ”*

#### 1.4.3.4 Biện pháp phòng chống tấn công xã hội

Đào tạo nâng cao nhận thức bảo mật: Tổ chức các chương trình đào tạo định kỳ để nhân viên nhận diện và xử lý các hình thức tấn công xã hội.

Xác thực đa yếu tố (MFA): Triển khai MFA để ngăn chặn truy cập trái phép, ngay cả khi thông tin đăng nhập bị đánh cắp.

Chính sách bảo mật rõ ràng: Xây dựng các chính sách bảo mật nội bộ, bao gồm hướng dẫn xử lý các tình huống như yêu cầu xác minh qua điện thoại hoặc email.

Giám sát và phát hiện hành vi bất thường: Sử dụng công cụ giám sát để phát hiện và cảnh báo các hành vi bất thường liên quan đến truy cập hoặc giao dịch.

Kiểm tra thường xuyên: Tổ chức các bài kiểm tra tấn công xã hội (Social Engineering Testing) để đánh giá khả năng phản ứng của nhân viên và hệ thống.

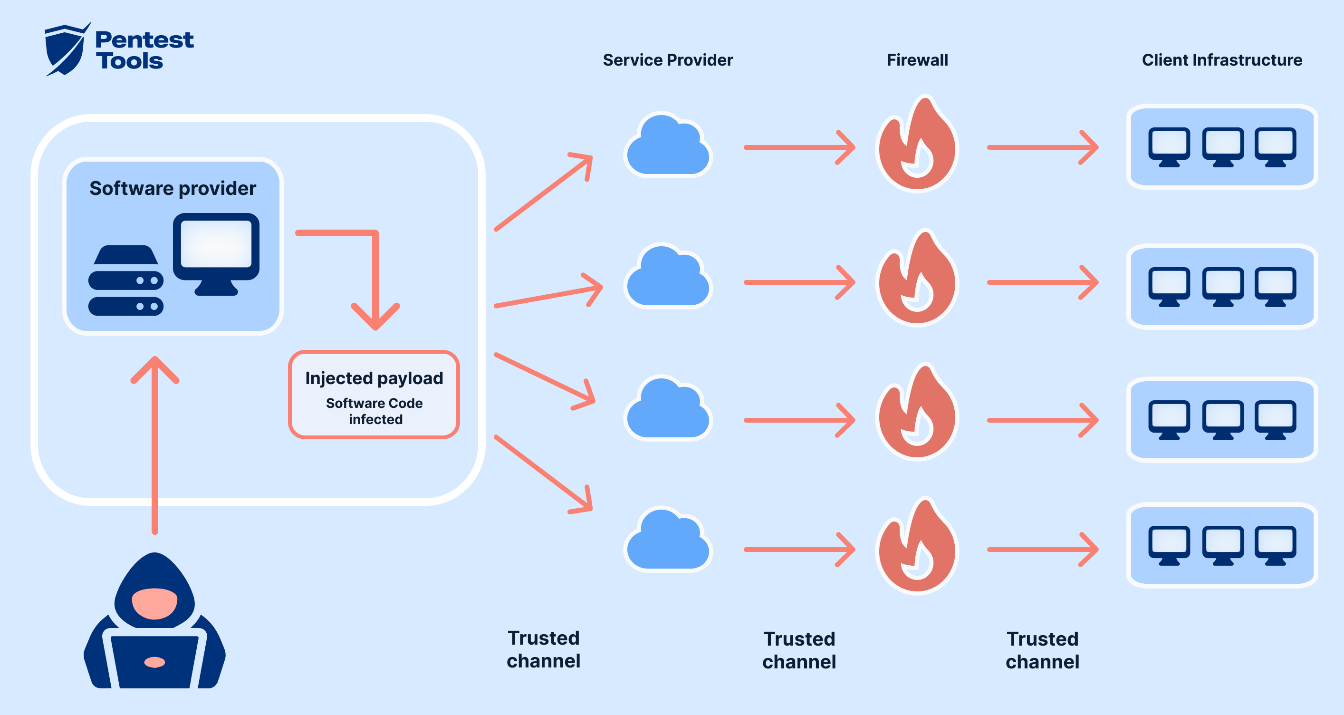
### 1.4.4 Xu hướng tấn công và lỗ hổng mới

Với sự phát triển nhanh chóng của công nghệ, các hình thức tấn công và lỗ hổng bảo mật cũng không ngừng tiến hóa. Xu hướng mới không chỉ mở rộng quy mô và độ phức tạp mà còn nhắm vào các mục tiêu mới như trí tuệ nhân tạo, IoT, và chuỗi cung ứng.

#### 1.4.4.1 Các xu hướng tấn công mới nổi

1. Tấn công chuỗi cung ứng (Supply Chain Attack)

Kẻ tấn công nhắm vào các nhà cung cấp phần mềm hoặc dịch vụ của tổ chức để cài mã độc hoặc khai thác lỗ hổng từ gốc.



*Hình 1.19: Mô phỏng tấn công chuỗi cung ứng*

Ví dụ: Vụ tấn công SolarWinds năm 2020 đã cho thấy nguy cơ từ các phần mềm quản lý bị nhiễm mã độc, gây ảnh hưởng nghiêm trọng đến hàng nghìn tổ chức.

1. Tấn công trí tuệ nhân tạo (AI Attack)

AI bị sử dụng để tự động hóa các cuộc tấn công, hoặc ngược lại, kẻ tấn công nhắm vào các hệ thống AI để làm sai lệch dữ liệu hoặc kết quả dự đoán.

Ví dụ: Deepfake được sử dụng để giả mạo danh tính hoặc lừa đảo tài chính, hoặc tấn công vào mô hình AI nhằm phá hoại hệ thống.

1. Tấn công vào Internet of Things (IoT)

Các thiết bị IoT thường thiếu bảo mật mạnh mẽ, dễ bị xâm nhập và sử dụng làm nền tảng cho các cuộc tấn công lớn.

Ví dụ: Cuộc tấn công Mirai Botnet đã biến hàng triệu thiết bị IoT thành mạng lưới botnet, gây ra sự cố DDoS lớn.

1. Ransomware-as-a-Service (RaaS)

Các nền tảng RaaS cho phép bất kỳ ai, kể cả không có kỹ năng cao, thuê hoặc sử dụng mã độc ransomware để thực hiện tấn công.

Ví dụ: RaaS đã tạo ra hàng loạt cuộc tấn công đòi tiền chuộc nhắm vào doanh nghiệp trên toàn cầu.

#### 1.4.4.2 Xu hướng lỗ hổng mới nổi

1. Lỗ hổng trong công nghệ đám mây (Cloud Vulnerabilities)

Sự chuyển đổi sang công nghệ đám mây dẫn đến nhiều rủi ro từ cấu hình sai, quyền truy cập không an toàn, và lỗ hổng API.

Ví dụ: Các dịch vụ lưu trữ đám mây bị cấu hình công khai, dẫn đến rò rỉ dữ liệu nhạy cảm.

1. Lỗ hổng trong Blockchain và DeFi

Blockchain và các nền tảng tài chính phi tập trung (DeFi) đang trở thành mục tiêu với các lỗ hổng trong hợp đồng thông minh.

Ví dụ: Vụ hack Ronin Network năm 2022 khiến hơn 600 triệu USD bị đánh cắp qua lỗi hợp đồng thông minh.

1. Lỗ hổng Zero-Day

Đây là các lỗ hổng chưa được phát hiện và khắc phục, thường bị khai thác ngay khi được tìm thấy.

Ví dụ: Các cuộc tấn công sử dụng zero-day như vụ khai thác lỗ hổng Microsoft Exchange năm 2021.

1. Tấn công dữ liệu lớn (Big Data Breaches)

Các lỗ hổng trong hệ thống lưu trữ dữ liệu lớn hoặc cấu hình sai của cơ sở dữ liệu mở rộng có thể gây ra vi phạm dữ liệu diện rộng.

Ví dụ: Các vụ rò rỉ thông tin khách hàng từ Facebook hoặc LinkedIn.

#### 1.4.4.3 Hướng đối phó

Tăng cường bảo mật chuỗi cung ứng bằng cách kiểm tra và giám sát chặt chẽ các đối tác cung cấp dịch vụ.

Nâng cao bảo mật cho các thiết bị IoT thông qua mã hóa và xác thực mạnh mẽ.

Áp dụng các công cụ bảo mật dựa trên AI để phát hiện và ngăn chặn tấn công thông minh.

Triển khai các chính sách giám sát và đánh giá liên tục cho hệ thống đám mây và blockchain.

## 1.5 Quy trình kiểm thử bảo mật và đánh giá rủi ro

Trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi, kiểm thử bảo mật và đánh giá rủi ro đã trở thành một quy trình không thể thiếu để bảo vệ hệ thống mạng của doanh nghiệp. Hai phương pháp này không chỉ hỗ trợ việc nhận diện lỗ hổng mà còn giúp đưa ra các biện pháp khắc phục, đảm bảo sự ổn định và an toàn cho hệ thống

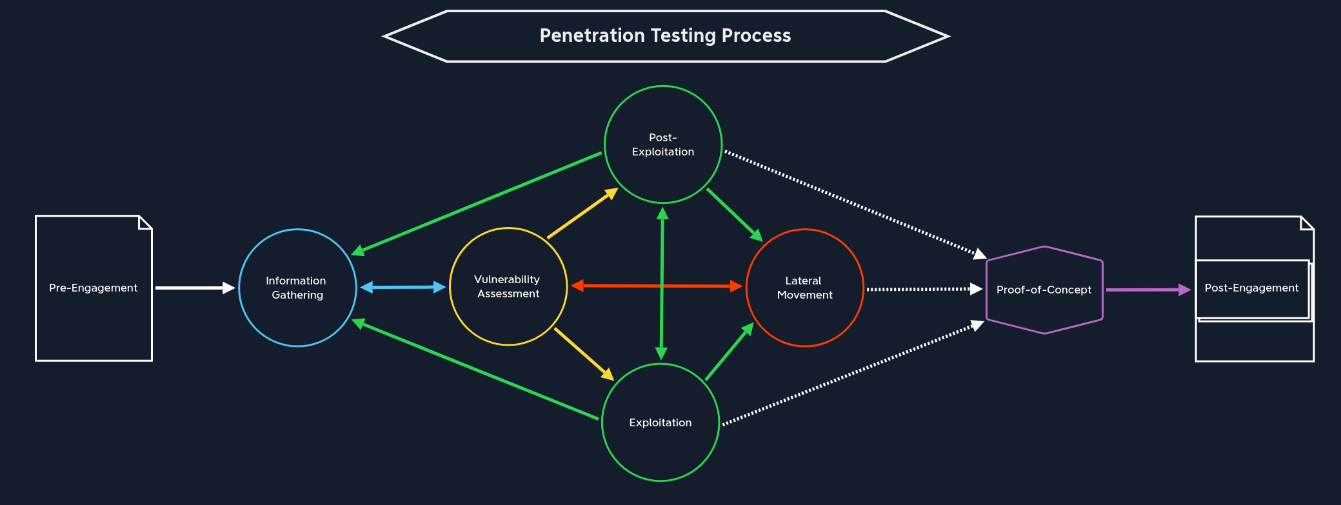
### Kiểm thử xâm nhập (Pentesting)

### 1.5.1.1 Khái niệm

Kiểm thử xâm nhập (Penetration Testing – Pentesting) là một quá trình giả lập các cuộc tấn công mạng nhằm kiểm tra tính an toàn của hệ thống. Đây là phương pháp hiệu quả để xác định và khai thác các lỗ hổng tiềm ẩn trước khi kẻ tấn công thực sự lợi dụng chúng.

#### 1.5.1.2 Quy trình kiểm thử xâm nhập

1. Thu thập thông tin (Reconnaissance)
   * Sử dụng công cụ như Nmap, Shodan để tìm kiếm các cổng mở, dịch vụ và hệ điều hành của mục tiêu.
   * Ví dụ: Một hệ thống mạng với cổng 80 mở có thể gợi ý một máy chủ web, trong khi cổng 445 thường liên quan đến dịch vụ SMB.
2. Phân tích lỗ hổng (Vulnerability Analysis)
   * Áp dụng công cụ như Nessus, OpenVAS để quét và xác định lỗ hổng.
   * Ví dụ: Một hệ thống chạy OpenSSL cũ có thể dễ dàng bị khai thác bởi lỗ hổng Heartbleed.
3. Tấn công khai thác (Exploitation)
   * Sử dụng công cụ như Metasploit để khai thác các lỗ hổng phát hiện được.
   * Ví dụ: Kẻ tấn công có thể sử dụng payload để thực hiện Remote Code Execution (RCE) qua lỗ hổng trên máy chủ web.
4. Di chuyển ngang (Lateral Movement)
   * Sau khi khai thác thành công, kẻ tấn công di chuyển qua các hệ thống khác trong mạng. BloodHound là một công cụ phổ biến để vẽ sơ đồ quyền hạn trong Active Directory.
5. Báo cáo kết quả
   * Tất cả lỗ hổng được ghi nhận kèm mức độ rủi ro và cách khai thác. Báo cáo này là cơ sở để doanh nghiệp cải thiện hệ thống.



*Hình 1.20: Quy trình kiểm thử xâm nhập*

### 1.5.3 Đánh giá rủi ro

#### 1.5.3.1 Khái niệm

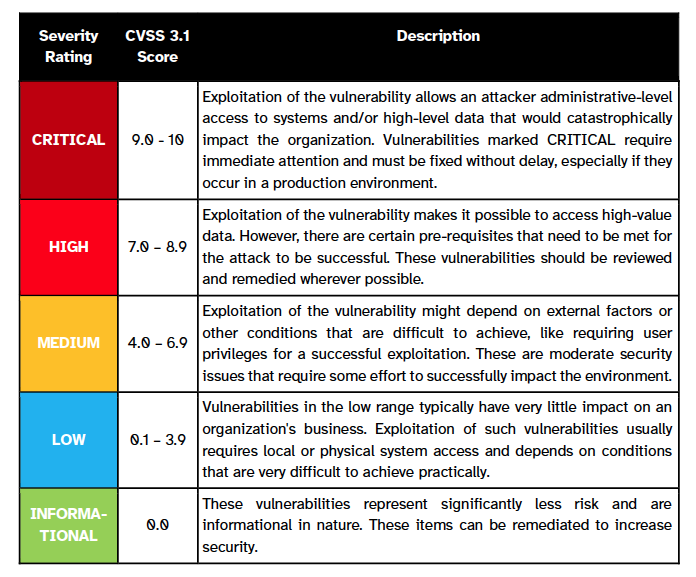
Đánh giá rủi ro là một quy trình tiếp nối kiểm thử xâm nhập nhằm đo lường mức độ ảnh hưởng của các lỗ hổng đã phát hiện và xác định các biện pháp giảm thiểu rủi ro.

#### 1.5.3.2 Quy trình đánh giá rủi ro

1. Xác định tài sản quan trọng

* Liệt kê các tài sản (hệ thống, dữ liệu, người dùng) cần bảo vệ.
* Ví dụ: Hệ thống quản lý khách hàng (CRM) chứa thông tin nhạy cảm như hợp đồng, địa chỉ và tài khoản ngân hàng.

1. Phân loại mức độ rủi ro
   * Sử dụng các phương pháp như CVSS (Common Vulnerability Scoring System) để đánh giá mức độ nghiêm trọng của từng lỗ hổng.
   * Ví dụ: Lỗ hổng có CVSS 9.8 thuộc nhóm nguy cơ cao (Critical).
2. Phân tích khả năng bị khai thác
   * Đánh giá xác suất lỗ hổng bị lợi dụng, dựa trên tần suất tiếp xúc của hệ thống với mạng bên ngoài.
3. Đề xuất biện pháp giảm thiểu
   * Các biện pháp khắc phục có thể bao gồm vá lỗi phần mềm, cấu hình lại hệ thống hoặc tăng cường giám sát.
4. Đánh giá lại sau khắc phục
   * Thực hiện lại kiểm thử xâm nhập để đảm bảo các biện pháp đã áp dụng mang lại hiệu quả.



*Hình 1.21: Điểm số CVSS đánh giá mức độ nguy hiểm của các lỗ hổng*

Ví dụ tổng thể: Một doanh nghiệp nhỏ sử dụng máy chủ web với phiên bản PHP lỗi thời. Trong quá trình kiểm thử, phát hiện lỗ hổng RCE (CVE-2021-12345). Sau khi vá lỗi và cập nhật phần mềm, doanh nghiệp tiến hành kiểm tra lại và xác nhận rằng lỗ hổng đã được khắc phục hoàn toàn, giảm thiểu rủi ro tấn công.

## 1.6 Bảo mật trong môi trường đám mây

Trong kỷ nguyên số, điện toán đám mây đã trở thành một phần không thể thiếu trong hạ tầng công nghệ thông tin của các doanh nghiệp, đặc biệt là doanh nghiệp nhỏ. Sự linh hoạt, khả năng mở rộng và chi phí thấp của đám mây đã giúp các doanh nghiệp giảm thiểu rào cản về công nghệ và nhanh chóng thích nghi với sự thay đổi. Tuy nhiên, song song với lợi ích, bảo mật đám mây cũng đối mặt với nhiều thách thức, đòi hỏi các doanh nghiệp phải áp dụng các biện pháp bảo vệ nghiêm ngặt.

### 1.6.1 Lợi ích và thách thức của bảo mật đám mây

Lợi ích:

* Khả năng mở rộng linh hoạt: Các doanh nghiệp có thể mở rộng hoặc thu nhỏ hạ tầng CNTT của mình tùy thuộc vào nhu cầu, chỉ cần trả tiền cho những gì họ sử dụng.
* Khả năng truy cập toàn cầu: Nhân viên có thể làm việc từ bất kỳ đâu, chỉ cần có kết nối Internet.
* Tích hợp bảo mật sẵn có: Các nhà cung cấp dịch vụ đám mây (CSP) như AWS, Azure, Google Cloud thường cung cấp các giải pháp bảo mật tích hợp như mã hóa, giám sát lưu lượng và phát hiện xâm nhập.

Thách thức:

* Mất quyền kiểm soát dữ liệu: Khi dữ liệu được lưu trữ trên đám mây, doanh nghiệp phụ thuộc vào nhà cung cấp dịch vụ để bảo vệ dữ liệu.
* Rủi ro truy cập trái phép: Tài khoản đám mây bị tấn công hoặc cấu hình sai có thể dẫn đến rò rỉ dữ liệu nhạy cảm.
* Tuân thủ quy định: Đảm bảo tuân thủ các tiêu chuẩn và luật pháp quốc tế (như GDPR, HIPAA) thường là một bài toán phức tạp khi sử dụng đám mây.

### 1.6.2 Các giải pháp bảo mật đám mây

* Mã hóa dữ liệu
  + Dữ liệu phải được mã hóa cả khi lưu trữ (at-rest) và khi truyền tải (in-transit).
  + Ví dụ: AWS cung cấp tính năng mã hóa tự động cho S3 Buckets, trong khi Azure sử dụng TLS để bảo vệ dữ liệu truyền tải.
* Quản lý quyền truy cập (IAM)
  + Sử dụng các hệ thống Quản lý danh tính và quyền truy cập (IAM) để kiểm soát ai được phép truy cập vào tài nguyên nào.
  + Ví dụ: Azure Active Directory cung cấp khả năng tích hợp MFA (Multi-Factor Authentication) để tăng cường bảo mật.
* Giám sát và ghi nhật ký
  + Doanh nghiệp cần triển khai các công cụ giám sát lưu lượng, phát hiện hành vi bất thường và ghi lại nhật ký hệ thống.
  + Ví dụ: AWS CloudTrail ghi lại mọi sự kiện trong tài khoản đám mây, giúp theo dõi các hoạt động đáng ngờ.
* Phòng chống tấn công và rủi ro
  + Sử dụng tường lửa ứng dụng web (WAF) để bảo vệ các ứng dụng đám mây khỏi các cuộc tấn công như SQL Injection, Cross-Site Scripting (XSS).
  + Sử dụng các dịch vụ DDoS Protection từ nhà cung cấp để ngăn chặn tấn công từ chối dịch vụ.

### 1.6.3 Hệ thống bảo mật nhiều lớp trong đám mây

Một hệ thống đám mây an toàn cần áp dụng mô hình bảo mật nhiều lớp.

* Lớp dữ liệu: Mã hóa dữ liệu bằng các thuật toán hiện đại như AES-256.
* Lớp ứng dụng: Triển khai cơ chế kiểm tra mã nguồn, phát hiện mã độc trong ứng dụng trước khi triển khai lên đám mây.
* Lớp mạng: Sử dụng VPN hoặc Virtual Private Cloud (VPC) để cô lập tài nguyên.
* Lớp người dùng: Áp dụng Zero Trust để yêu cầu xác thực mọi truy cập, không phân biệt nội bộ hay bên ngoài.

### 1.6.4 Bài học từ các sự cố bảo mật đám mây

Sự cố Capital One (2019): Hacker đã khai thác cấu hình sai trong AWS S3 Bucket, dẫn đến việc rò rỉ dữ liệu cá nhân của hơn 100 triệu khách hàng. Bài học: Đảm bảo cấu hình bảo mật đúng, định kỳ kiểm tra các chính sách truy cập.

Sự cố Dropbox (2012): Rò rỉ tài khoản người dùng do sử dụng mật khẩu yếu. Bài học: Tăng cường các biện pháp bảo mật danh tính như MFA và chính sách mật khẩu mạnh.

## 1.7. Các xu hướng bảo mật doanh nghiệp hiện nay

Trong bối cảnh an ninh mạng không ngừng thay đổi, các tổ chức và doanh nghiệp đang phải đối mặt với những mối đe dọa ngày càng tinh vi. Để thích ứng, các xu hướng bảo mật hiện đại đã được phát triển nhằm cung cấp các giải pháp hiệu quả và tối ưu hơn. Những xu hướng này không chỉ giúp doanh nghiệp bảo vệ tốt hơn tài sản kỹ thuật số mà còn đảm bảo tính linh hoạt và bền vững trong một môi trường công nghệ phát triển nhanh chóng.

### 1.7.1 Tăng cường sử dụng AI và học máy trong bảo mật

#### 1.7.1.1 Vai trò của AI trong an ninh mạng

AI và học máy (Machine Learning) giúp tự động hóa việc giám sát, phân tích và phát hiện các mối đe dọa an ninh mạng trong thời gian thực.

Các thuật toán AI có thể nhận diện hành vi bất thường, chẳng hạn như một lượng lớn yêu cầu truy cập từ một IP đáng ngờ hoặc hành vi lạ của tài khoản người dùng.



*Hình 1.22: Ứng dụng của AI trong an ninh mạng*

#### 1.7.1.2 Triển khai cụ thể

Phát hiện xâm nhập thông minh (IDS/IPS): Các hệ thống như Darktrace và Palo Alto Networks sử dụng AI để phát hiện và ngăn chặn các cuộc tấn công mạng trước khi chúng gây thiệt hại.

Phân tích hành vi người dùng (UEBA): Công cụ như Splunk hoặc Exabeam sử dụng AI để theo dõi hành vi của người dùng và cảnh báo khi phát hiện bất thường.

#### 1.7.1.3 Thách thức

Chi phí triển khai: Công nghệ AI thường đòi hỏi đầu tư lớn và đội ngũ chuyên môn cao.

Rủi ro từ AI đảo ngược: Tin tặc có thể lợi dụng AI để phát hiện các lỗ hổng bảo mật và thực hiện các cuộc tấn công tinh vi hơn.

### 1.7.2 Zero Trust: Triết lý bảo mật không tin cậy

#### 1.7.2.1 Khái niệm Zero Trust

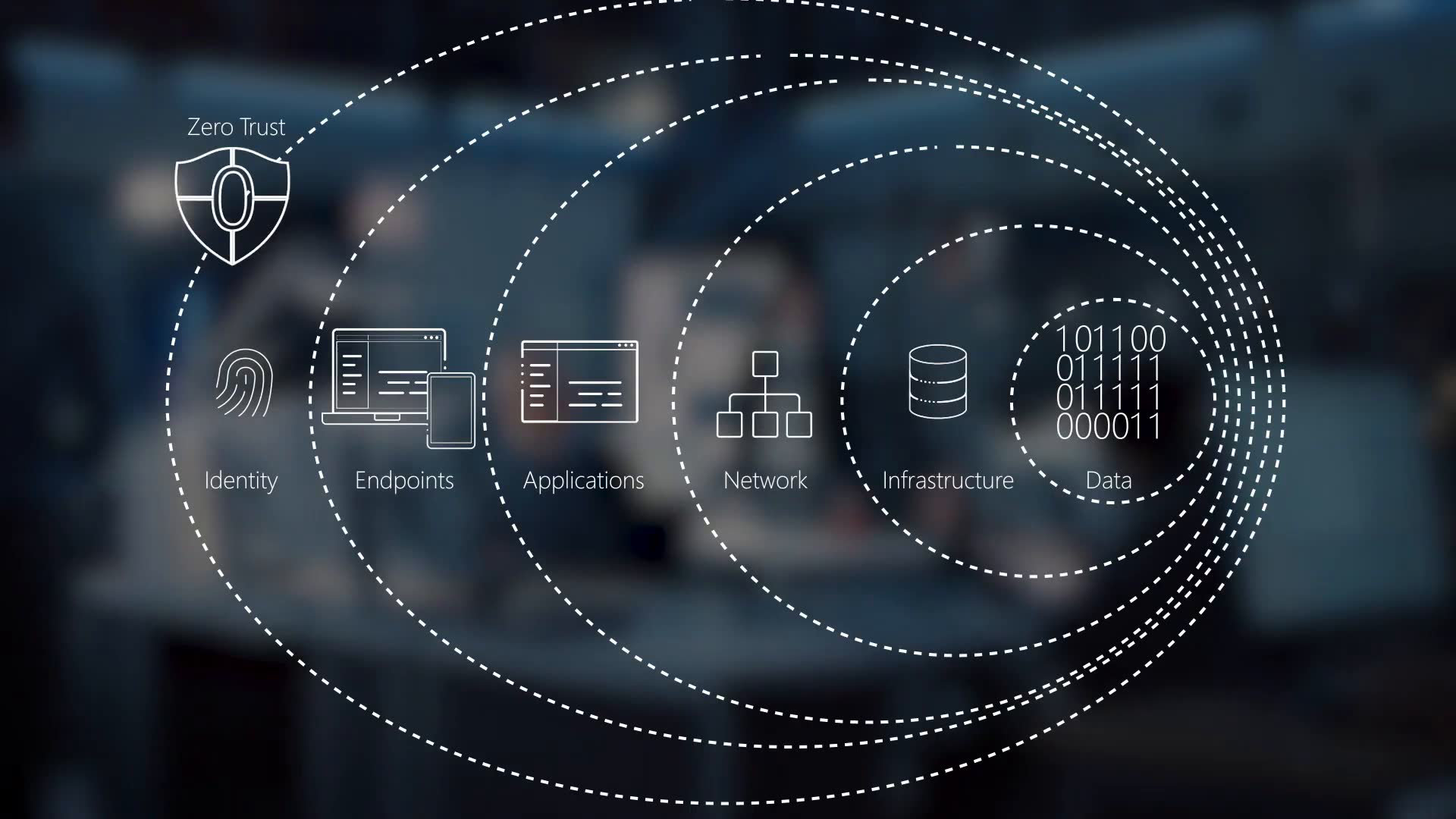
"Không tin tưởng bất kỳ ai, luôn xác thực mọi thứ" – triết lý Zero Trust yêu cầu xác thực và ủy quyền liên tục cho tất cả các đối tượng truy cập, bất kể chúng đến từ bên trong hay bên ngoài mạng doanh nghiệp.

#### 1.7.2.2 Các nguyên tắc chính

Xác thực liên tục (Continuous Verification): Không tin tưởng bất kỳ người dùng hay thiết bị nào mà không xác thực danh tính rõ ràng.

Giới hạn quyền truy cập (Least Privilege): Chỉ cấp quyền truy cập tối thiểu cần thiết cho người dùng và ứng dụng.

Cô lập mạng (Micro-Segmentation): Chia nhỏ hệ thống mạng thành các phân đoạn nhỏ hơn để giảm thiểu tác động nếu xảy ra xâm nhập.



*Hình 1.23: Cấu trúc và chiến lược của Zero Trust*

#### 1.7.2.3 Triển khai cụ thể

Microsoft Azure AD Conditional Access: Xác thực đa yếu tố (MFA) và điều kiện dựa trên vị trí, thiết bị.

Zscaler Zero Trust Exchange: Hỗ trợ bảo mật không gian làm việc từ xa và kiểm soát truy cập mạng.

### 1.7.3 Bảo mật không gian làm việc từ xa (Remote Work Security)

#### 1.7.3.1 Thách thức của làm việc từ xa

Môi trường làm việc từ xa, phổ biến sau đại dịch COVID-19, tạo ra các điểm yếu bảo mật mới, chẳng hạn như thiết bị cá nhân không được quản lý hoặc kết nối qua mạng Wi-Fi công cộng.

#### 1.7.3.2 Giải pháp bảo mật

VPN an toàn: Triển khai VPN để mã hóa dữ liệu truyền tải giữa nhân viên và hệ thống công ty.

Endpoint Detection and Response (EDR): Giám sát và bảo vệ các thiết bị đầu cuối (như máy tính cá nhân) trước các mối đe dọa.

Giải pháp SASE (Secure Access Service Edge): Tích hợp bảo mật mạng và quản lý truy cập từ xa trên nền tảng đám mây, giúp đảm bảo an toàn khi làm việc từ xa.

### 1.7.4 Bảo mật dữ liệu thông qua mã hóa hiện đại

Mã hóa đồng nhất (Homomorphic Encryption): Cho phép tính toán trên dữ liệu đã mã hóa mà không cần giải mã, bảo vệ dữ liệu ngay cả khi bị đánh cắp.

Quản lý khóa mã hóa (Key Management): Sử dụng các công cụ như HashiCorp Vault hoặc AWS KMS để quản lý khóa mã hóa một cách an toàn.

### 1.7.5 Tích hợp bảo mật dựa trên đám mây (Cloud-Native Security)

Bảo mật container: Với sự phát triển của công nghệ container như Docker và Kubernetes, các công cụ như Aqua Security giúp phát hiện và vá lỗ hổng trong môi trường container.

Giám sát serverless: Các dịch vụ không máy chủ (serverless) như AWS Lambda yêu cầu bảo mật để theo dõi và kiểm soát truy cập.

Hiệu quả trong thực tế:

* AI và học máy trong phát hiện tấn công mạng: Công cụ Darktrace đã phát hiện và ngăn chặn một cuộc tấn công bằng ransomware bằng cách nhận diện hành vi bất thường trong lưu lượng mạng.
* Ứng dụng Zero Trust: Một ngân hàng lớn ở Mỹ đã triển khai Zero Trust kết hợp với phân đoạn mạng (Micro-Segmentation), giảm 70% nguy cơ bị xâm nhập.

## 1.8 Tổng kết và hướng phát triển

### 1.8.1 Tổng kết nội dung

Chương 1 đã trình bày tổng quan về an ninh mạng doanh nghiệp, tập trung vào các khía cạnh chính như tầm quan trọng của an ninh mạng, các thách thức đặc thù đối với doanh nghiệp nhỏ, và các giải pháp bảo mật hiện hành. Những nội dung này không chỉ làm sáng tỏ thực trạng an ninh mạng mà còn đặt nền móng lý thuyết vững chắc cho các chương tiếp theo.

Trong bối cảnh các mối đe dọa an ninh mạng không ngừng gia tăng, các doanh nghiệp cần tập trung vào việc xây dựng một hệ thống mạng an toàn, đồng thời áp dụng các xu hướng bảo mật tiên tiến như AI, Zero Trust, và bảo mật không gian làm việc từ xa. Bên cạnh đó, việc tận dụng các giải pháp bảo mật dựa trên đám mây và quản lý rủi ro một cách hiệu quả cũng đóng vai trò then chốt để bảo vệ tài sản kỹ thuật số.

Các nội dung về kiểm thử bảo mật và đánh giá rủi ro đã nhấn mạnh tầm quan trọng của việc xác định và khắc phục lỗ hổng trước khi kẻ tấn công có cơ hội khai thác. Những thông tin này không chỉ có giá trị trong lý thuyết mà còn là bước đệm để thực hiện các phần kiểm thử thực tế trong các chương sau.

### 1.8.2. Hướng phát triển trong tương lai

An ninh mạng là một lĩnh vực không ngừng thay đổi, đòi hỏi sự sáng tạo và thích ứng với những công nghệ mới. Dựa trên những nội dung đã trình bày trong chương này, một số hướng phát triển quan trọng trong lĩnh vực bảo mật doanh nghiệp bao gồm:

1. Ứng dụng công nghệ bảo mật lượng tử (Quantum Security):

Với khả năng tính toán vượt trội, máy tính lượng tử có thể làm suy yếu các thuật toán mã hóa truyền thống. Vì vậy, việc nghiên cứu và áp dụng các thuật toán mã hóa lượng tử là một xu hướng tất yếu trong tương lai để đảm bảo dữ liệu an toàn trước các cuộc tấn công lượng tử.

1. Blockchain trong an ninh mạng:

Công nghệ blockchain không chỉ được sử dụng trong lĩnh vực tài chính mà còn có tiềm năng lớn trong việc bảo vệ dữ liệu và xác thực giao dịch. Blockchain có thể được sử dụng để xây dựng các hệ thống bảo mật phi tập trung, giảm nguy cơ tấn công từ một điểm duy nhất (Single Point of Failure).

1. Tăng cường bảo mật dựa trên hành vi (Behavioral Security):

Thay vì chỉ dựa vào các quy tắc và chữ ký cố định, bảo mật dựa trên hành vi tập trung vào việc phân tích hành động của người dùng và thiết bị để phát hiện các dấu hiệu bất thường. Điều này đặc biệt hiệu quả trong việc ngăn chặn các cuộc tấn công chưa được ghi nhận trước đó.

1. Tích hợp bảo mật trong IoT (Internet of Things):

Sự phát triển mạnh mẽ của IoT đã mở ra cơ hội nhưng cũng tạo ra nhiều rủi ro bảo mật. Trong tương lai, các doanh nghiệp cần tập trung phát triển các giải pháp bảo mật tích hợp cho thiết bị IoT, bao gồm mã hóa, quản lý danh tính và kiểm soát truy cập.

1. Bảo mật dựa trên đám mây thế hệ tiếp theo:

Với sự chuyển đổi của nhiều doanh nghiệp sang mô hình làm việc từ xa và dựa trên đám mây, các dịch vụ bảo mật đám mây thế hệ tiếp theo, như CASB (Cloud Access Security Broker) và XDR (Extended Detection and Response), sẽ tiếp tục là một hướng phát triển quan trọng.

1. Tăng cường giáo dục và nhận thức về an ninh mạng:

Bên cạnh việc triển khai công nghệ, con người vẫn là yếu tố quyết định trong bảo mật. Do đó, cần đầu tư mạnh mẽ hơn vào các chương trình đào tạo, nâng cao nhận thức về an ninh mạng cho nhân viên, đặc biệt là ở các doanh nghiệp nhỏ.

# CHƯƠNG 2: THIẾT KẾ VÀ TRIỂN KHAI MÔ HÌNH MẠNG AN TOÀN

## 2.1. Khảo sát hiện trạng tại SkyTech Solutions

### 2.1.1. Giới thiệu doanh nghiệp

SkyTech Solutions là một doanh nghiệp nhỏ chuyên cung cấp các dịch vụ tư vấn công nghệ thông tin và giải pháp chuyển đổi số cho các doanh nghiệp vừa và nhỏ. Hiện tại, SkyTech Solutions có quy mô 15 nhân viên, được chia thành 4 phòng ban:

* Phòng Kinh doanh (5 người): Phụ trách tiếp cận khách hàng, tư vấn dịch vụ.
* Phòng Kỹ thuật (5 người): Quản lý và triển khai các dự án công nghệ.
* Phòng Kế toán & Nhân sự (3 người): Xử lý tài chính, nhân sự, quy trình nội bộ.
* Quản lý cấp cao (2 người): Điều hành và lên chiến lược phát triển.

### 2.1.2. Hiện trạng hệ thống mạng

#### 2.1.2.1 Tài nguyên hiện có

|  |  |
| --- | --- |
| **Thành phần** | **Tình trạng** |
| Router | Router phổ thông (TP-Link Archer C6), không hỗ trợ tường lửa nâng cao. |
| Switch | Switch unmanaged, 16 cổng, không hỗ trợ VLAN. |
| Máy chủ chính | Windows Server 2016, các dịch vụ Web Server và lưu trữ cơ bản. |
| Email | Sử dụng Gmail miễn phí, không có kiểm soát bảo mật và lưu trữ email. |
| Máy trạm nhân viên | Intel Core i3/i5, RAM 8GB, SSD 500GB, kết nối qua LAN. |

*Bảng 2.1: Tài nguyên hiện có của SkyTech Solutions*

#### 2.1.2.2 Dịch vụ và cấu hình hiện tại

* Web Server:
  + Chạy Apache trên Windows Server 2016.
  + Không hỗ trợ giao thức HTTPS (truyền tải HTTP dễ bị tấn công Man-in-the-Middle).
* Email:
  + Sử dụng Gmail miễn phí cho toàn bộ nhân viên.
  + Không có kiểm soát dữ liệu email nội bộ.
* Bảo mật:
  + Không có Active Directory (AD) hay xác thực tập trung.
  + Chưa triển khai tường lửa hoặc phân vùng mạng.

#### 2.1.2.3 Lỗ hổng bảo mật

* Cấu trúc mạng:
  + Không phân vùng mạng (VLAN), dễ bị tấn công lateral movement.
  + Toàn bộ thiết bị nội bộ đều nằm trong một lớp mạng duy nhất.
* Web Server:
  + Không sử dụng HTTPS, tài liệu truyền tải qua giao thức HTTP không được mã hóa.
  + Phiên bản Apache lỗi thời.
* Quản lý truy cập:
  + Nhân viên chia sẻ tài khoản qua email, không có xác thực đa yếu tố (MFA).
  + Không có công cụ kiểm soát tài liệu nội bộ.
* Giám sát:
  + Không có hệ thống ghi nhật ký (logging) hoặc giám sát mạng.

### 2.1.3. Đánh giá tổng quát

Dựa trên phân tích hiện trạng, hệ thống mạng của SkyTech Solutions đang đối mặt với nhiều vấn đề nghiêm trọng cần được cải thiện, cụ thể như sau:

* An ninh bảo mật:
  + Thiếu các cơ chế bảo vệ phân vùng mạng, tăng nguy cơ di chuyển ngang (lateral movement) trong hệ thống.
  + Web Server và email không đảm bảo tính bảo mật, đặc biệt là việc truyền tải thông tin qua HTTP không được mã hóa.
* Hiệu năng hoạt động:
  + Hạ tầng mạng hiện tại sử dụng thiết bị cơ bản (router phổ thông, switch unmanaged), không đáp ứng được yêu cầu phân vùng hoặc kiểm soát lưu lượng mạng.
  + Máy chủ và dịch vụ cũ hoạt động dưới mức tối ưu, làm tăng nguy cơ lỗi hệ thống.
* Quản lý và giám sát:
  + Không có hệ thống quản lý danh tính tập trung (Active Directory), dẫn đến việc chia sẻ tài khoản không an toàn và không có kiểm soát quyền truy cập.
  + Thiếu công cụ giám sát mạng và nhật ký bảo mật, gây khó khăn trong việc phát hiện các hành vi bất thường.

Hệ thống hiện tại của SkyTech Solutions chưa đáp ứng được các yêu cầu cơ bản về bảo mật và hiệu năng cho một doanh nghiệp trong thời đại số. Do đó, việc thiết kế và triển khai một mô hình mạng an toàn là cần thiết để cải thiện khả năng bảo vệ, quản lý, và mở rộng của hệ thống.

## 2.2 Phân tích yêu cầu thiết kế

### 2.2.1. Nhu cầu của hệ thống

Dựa trên kết quả khảo sát tại SkyTech Solutions (đã được trình bày trong mục 2.1), có thể nhận thấy những nhu cầu sau là cần thiết để hệ thống mạng có thể đáp ứng được yêu cầu bảo mật và hiệu năng:

1. Quản lý danh tính và quyền truy cập
   * Hệ thống cần được tổ chức tập trung, cho phép quản lý tài khoản người dùng, quyền truy cập tài nguyên một cách hiệu quả.
   * Tích hợp các cơ chế xác thực đa yếu tố (MFA) để tăng tính an toàn.
2. Bảo mật dịch vụ công khai
   * Dịch vụ Web Server cần hỗ trợ HTTPS để đảm bảo tính bảo mật cho dữ liệu truyền tải.
   * Dịch vụ Mail Server cần hỗ trợ giao thức SMTP với TLS để mã hóa email nội bộ và khách hàng.
3. Phân vùng mạng
   * Tạo DMZ (Demilitarized Zone) để tách biệt dịch vụ công khai (Web Server) khỏi mạng nội bộ (LAN).
   * Sử dụng VLAN để cách ly máy trạm nhân viên, thiết bị quản trị và dịch vụ mạng.
4. Giám sát và bảo vệ
   * Tích hợp firewall (tường lửa) để lọc luồng dữ liệu đối với DMZ và LAN.
   * Tích hợp hệ thống ghi nhật ký (logging) và giám sát luông truy cập.

### 2.2.2. Mục tiêu thiết kế

Dựa trên các nhu cầu đã xác định, các mục tiêu thiết kế được đề xuất như sau:

1. Tăng cường bảo mật
   * Sử dụng giao thức HTTPS cho Web Server và giao thức TLS cho Mail Server.
   * Triển khai Active Directory để quản lý danh tính tập trung và giới hạn quyền truy cập.
2. Phân vùng mạng hiệu quả
   * Thiết lập VLAN:
     + VLAN 10: DMZ (Web Server).
     + VLAN 20: LAN (máy trạm nhân viên).
     + VLAN 30: Quản lý (DC01 và Mail Server).
   * Tăng cường tương tác giữa các VLAN qua firewall.
3. Hỗ trợ mở rộng
   * Thiết kế linh hoạt để hệ thống có thể mở rộng quy mô trong tương lai, bao gồm thêm người dùng và dịch vụ.
4. Triển khai firewall
   * Sử dụng pfSense để phân vùng mạng, quản lý NAT và chặn truy cập trái phép.

### 2.2.3. Phạm vi và giới hạn

1. Phạm vi

* Triển khai hệ thống mạng cho SkyTech Solutions bao gồm các thành phần:
  + Active Directory (DC01).
  + Web Server (DMZ01).
  + Mail Server (MS01).
  + Firewall (pfSense).
* Các thiết bị và dịch vụ sẽ được triển khai trên máy ảo (VMware Workstation).

1. Giới hạn

* Hệ thống được thiết kế dành cho quy mô doanh nghiệp nhỏ (15 người dùng).
* Chưa tích hợp các dịch vụ cao cấp như hệ thống IDS/IPS.

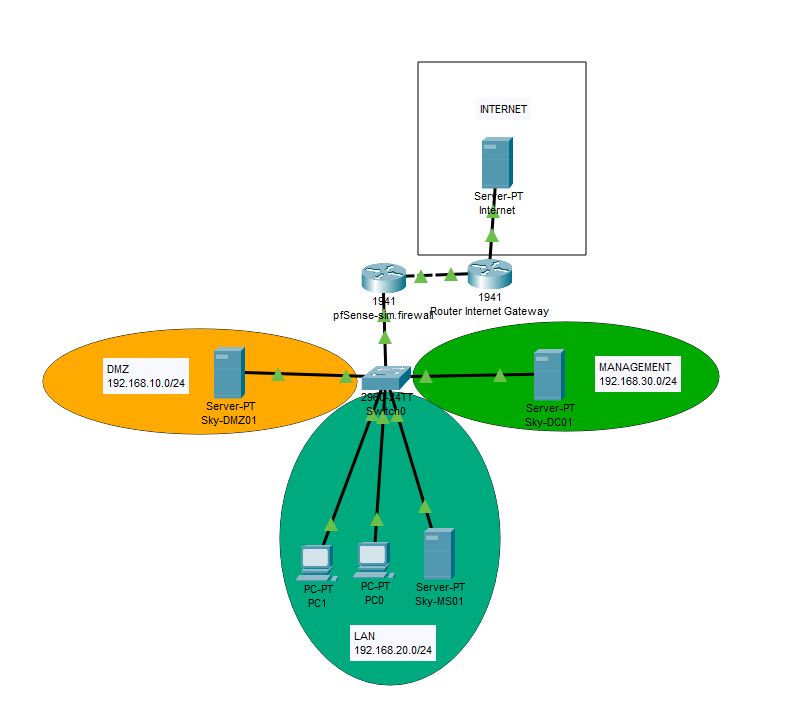
## 2.3. Thiết kế mô hình mạng an toàn

### 2.3.1. Sơ đồ mô hình mạng

Hệ thống mạng của SkyTech Solutions được thiết kế dựa trên nguyên tắc phân vùng mạng rõ ràng, nhằm bảo đảm tính bảo mật và tăng hiệu quả quản lý. Mô hình bao gồm ba phân vùng chính:

* DMZ (Demilitarized Zone):
  + Chứa Web Server (DMZ01) cung cấp dịch vụ truy cập công khai qua Internet.
  + Tách biệt với mạng nội bộ (để ngăn chặn tấn công lateral movement).
* LAN (Local Area Network):
  + Chứa các máy trạm nhân viên và Mail Server (MS01).
  + Cung cấp kênh giao tiếp nội bộ và lưu trữ tài liệu.
* Quản lý (Management VLAN):
  + Chứa Domain Controller (DC01) quản lý danh tính và quyền truy cập.
  + Khu vực bảo mật cao, chỉ cho phép truy cập từ các thiết bị quản trị.

Sơ đồ mô hình mạng:



*Hình 2.1: Sơ đồ mạng dự kiến của SkyTech Solutions*

### 2.3.2. Các thành phần hệ thống

1. Active Directory Server (DC01)

* Chức năng:
  + Quản lý danh tính người dùng và quyền truy cập.
  + Làm DNS Server cho máy chủ nội bộ.
* Cấu hình:
  + Hệ điều hành: Windows Server 2022.
  + Tên miền: skytech.tp.
  + IP: 192.168.30.2/24.

1. Web Server (DMZ01)

* Chức năng:
  + Cung cấp dịch vụ truy cập web công khai qua Internet.
  + Tích hợp HTTPS để đảm bảo truyền tải an toàn.
* Cấu hình
  + Hệ điều hành: Ubuntu Server 22.04.
  + Dịch vụ: Apache/Nginx.
  + IP: 192.168.10.2/24.

1. Mail Server (MS01)

* Chức năng:
  + Xử lý email nội bộ và giao tiếp với khách hàng qua SMTP.
  + Mã hóa email bằng TLS.
* Cấu hình:
  + Hệ điều hành: Ubuntu Server 22.04.
  + Dịch vụ: Postfix hoặc Zimbra.
  + IP: 192.168.20.2/24.

1. Tường lửa (pfSense)

* Chức năng:
  + Quản lý luồng dữ liệu giữa các phân vùng (DMZ, LAN, MANAGEMENT, WAN).
  + Thực thi các chính sách NAT và ACL.
* Cấu hình:
  + IP WAN: 203.0.113.1.
  + IP LAN: 192.168.20.1/24.
  + IP DMZ: 192.168.10.1/24.
  + IP MANAGEMENT: 192.168.30.1/24

### 2.3.3. Chính sách bảo mật

1. Phân vùng mạng

* VLAN 10 (DMZ): Các dịch vụ công khai, tách biệt hoàn toàn khỏi LAN.
* VLAN 20 (LAN): Các máy trạm và Mail Server.
* VLAN 30 (Management): Chỉ dành cho thiết bị quản trị như DC01.

1. Tường lửa

* Cấm tất cả luồng truy cập từ DMZ sang LAN.
* Cho phép luồng truy cập từ WAN vào DMZ qua cổng 443 (HTTPS).
* Cho phép SMTP và IMAP qua TLS từ WAN vào MS01.

1. Quản lý danh tính

* Triển khai Group Policy (GPO) trên Active Directory để bảo vệ máy trạm nhân viên:
  + Tự động khoá màn hình sau 5 phút không sử dụng.
  + Hạn chế quyền truy cập tập tin nhạy cảm.

### 2.3.4. Cấu hình máy ảo

| **Thành phần** | **Hệ điều hành** | **CPU** | **RAM** | **Dung lượng ổ cứng** | **Địa chỉ IP** |
| --- | --- | --- | --- | --- | --- |
| Domain Controller (DC01) | Windows Server 2022 | 2 cores | 4GB | 100GB | 192.168.30.2/24 |
| Web Server (DMZ01) | Ubuntu Server 22.04 | 2 cores | 2GB | 50GB | 192.168.10.2/24 |
| Mail Server (MS01) | Ubuntu Server 22.04 | 2 cores | 2GB | 50GB | 192.168.20.2/24 |
| Firewall (pfSense) | pfSense | 1 core | 1GB | 10GB | 203.0.113.1 (WAN), 192.168.10.1 (DMZ), 192.168.20.1 (LAN) |

*Bảng 2.2: Chi tiết cấu hình các thành phần*

# CHƯƠNG 3:



# Tài liệu tham khảo

**Tiếng anh**

[1] <https://academy.hackthebox.com/preview/certifications/htb-certified-penetration-testing-specialist/certification-steps>

[2] <https://academy.hackthebox.com/course/preview/active-directory-enumeration--attacks>

[3] <https://academy.hackthebox.com/course/preview/attacking-enterprise-networks>

[4]<https://www.youtube.com/playlist?list=PLbK3lpDL_g6ChnJ9E8LB30dezPfuzgaBI>

[5] <https://nored0x.github.io/red-teaming/active-directory-domain-enumeration-part-1/>

[6] <https://nored0x.github.io/red-teaming/active-directory-domain-enumeration-part-2/>

[7] <https://www.hackingarticles.in/active-directory-enumeration-powerview/>

[8] <https://portswigger.net/web-security/authentication#vulnerabilities-in-third-party-authentication-mechanisms>

**Tiếng Việt**

[1] <https://thietbimanggiare.com/mo-hinh-mang-cho-doanh-nghiep/>

[2] <https://antoanthongtin.vn/an-toan-thong-tin/10-vu-vi-pham-du-lieu-dang-chu-y-dau-the-ky-21-107368>

[3] <https://cmcts.com.vn/vi/bao-mat-thong-tin-doanh-nghiep.html>

[4] <https://www.bitdefender.vn/post/security-for-small-business/>

[5] <https://whitehat.vn/>

[6] <https://giaiphapmangh3t.com>