Bài thảo luận Atbmtt N21

An toàn bảo mật (Trường Đại học Thương mại)

TRƯỜNG ĐẠI HỌC THƯƠNG MẠI

KHOA HỆ THỐNG THÔNG TIN KINH TẾ & THƯƠNG MẠI ĐIỆN TỬ

BÀI THẢO LUẬN NHÓM 21

HỌC PHẦN AN TOÀN VÀ BẢO MẬT THÔNG TIN

Đề tài:

NGUY CƠ VÀ GIẢI PHÁP ĐẢM BẢO AN TOÀN ĐỐI VỚI HỆ THỐNG NGƯỜI DÙNG TRONG CÁC MẠNG DOANH NGHIỆP

LỚP HP: 232_ECIT0921_02

GIẢNG VIÊN: NGUYỄN THỊ HỘI

Hà Nội, năm 2024

BẢNG PHÂN CÔNG NHIỆM VỤ

STT	Họ và tên	Nhiệm vụ	Nhóm tự đánh giá	Giảng viên đánh giá
36	Vũ Thị Thu Hiền	Nhóm trưởng + Thuyết trình + Nội dung III		
40	Lê Thị Huế	Word + Nội dung III		
45	Văn Thị Huyền	Powerpoint + Nội dung II/2.1 + IV		
60	Quách Hoàng Ly	Powerpoint + Nội dung III		
65	Phạm Thị Mai	Thuyết trình + Nội dung I + II/2.2		

MỤC LỤC

LỜI MỞ ĐẦU

Trong thời đại công nghệ thông tin ngày một phát triển nhanh chóng và mạnh mẽ, với sự xuất hiện của Internet cùng máy vi tính, các tài liệu văn bản và giấy tờ, những thông tin quan trọng đều được số hóa và xử lý một cách dễ dàng, sau đó được truyền đi trong một môi trường mà mặc định là không an toàn. Chính vì lý do đó, yêu cầu về việc có một cơ chế, giải pháp nhằm bảo vệ sự an toàn và bảo mật cả thông tin ngày càng trở nên cấp thiết.

Đặc biệt là đối với các doanh nghiệp trong thời đại số, an toàn thông tin là một trong những yếu tố then chốt giúp đảm bảo sự hoạt động hiệu quả, bền vững và phát triển của các doanh nghiệp. Ngày nay, đi đôi với sự phát triển đa dạng của công là việc các doanh nghiệp đang phải đối mặt với nhiều thách thức và rủi ro về an toàn thông tin, từ việc bị tấn công mạng, xâm nhập hệ thống, đánh cắp dữ liệu, lừa đảo, mã độc, đến việc mất uy tín, thiệt hại kinh tế và pháp lý. Do đó, việc nâng cao nhận thức, triển khai các giải pháp và biện pháp bảo vệ an toàn thông tin mạng là một nhiệm vụ cấp thiết và bắt buộc đối với các doanh nghiệp. Việc bảo vệ thông tin và dữ liệu của tổ chức không chỉ là vấn đề kỹ thuật mà còn là một phần quan trọng của chiến lược kinh doanh.

Hiểu và nhận biết được tầm quan trọng của vấn đề trên, nhóm 21 chúng em xin đưa ra bài thảo luận với mục tiêu nhấn mạnh tầm quan trọng của an toàn thông tin đối với hệ thống người dùng trong các mạng doanh nghiệp, đồng thời đề xuất các giải pháp cần thiết để bảo vệ thông tin và dữ liệu, cũng như đề xuất một số giải pháp và khuyến nghị để cải thiện và nâng cao an toàn thông tin mạng cho các doanh nghiệp.

Bài thảo luận sẽ đi sâu vào các khía cạnh của an toàn thông tin, bao gồm: tìm hiểu sơ lược về thực trạng của việc đảm bảo an toán đối với hệ thống của người dùng trong doanh nghiệp Việt Nam hiện nay, phát hiện được nguyên nhân cũng như nguy cơ và tổn thất do việc mất an toàn hệ thống của người dùng; từ đó sẽ trình bày các biện pháp cụ thể để đảm bảo an toàn thông tin trong môi trường doanh nghiệp. Đồng thời, bài thảo luận cũng sẽ phân tích các xu hướng mới trong lĩnh vực an toàn thông tin và đề xuất các chiến lược tiếp cận đáng chú ý để đối phó với những thách thức ngày càng phức tạp trong việc bảo vệ thông tin doanh nghiệp.

Trong quá trình thực hiện bài thảo luận sẽ khó tránh khỏi những sai xót, chúng em mong sẽ nhận được sự đánh giá cũng như góp ý để nhóm có thể hoàn thiện bài một cách tốt hơn. Chúng em xin chân thành cảm ơn!

PHẦN NỘI DUNG

I. GIỚI THIỆU CHUNG

Trong thời điểm công nghệ và nhu cầu sử dụng Intenet ngày một tăng cao hiện nay, đòi hỏi các doanh nghiệp phải có một hệ thống mạng hoạt động thật tốt phục vụ công việc kinh doanh cũng như quản lý nội bộ. Mạng doanh nghiệp chuyên dụng là vấn đề thiết yếu mà từ doanh nghiệp vừa và nhỏ cho đến doanh nghiệp lớn cần phải quan tâm đặc biệt. Hệ thống mạng văn phòng có ảnh hưởng rất lớn đến hiệu suất làm việc, duy trì kết nối và đặc biệt là vấn đề mang tính bảo mật.

1.1. Hệ thống mạng doanh nghiệp

1.1.1. Khái niệm

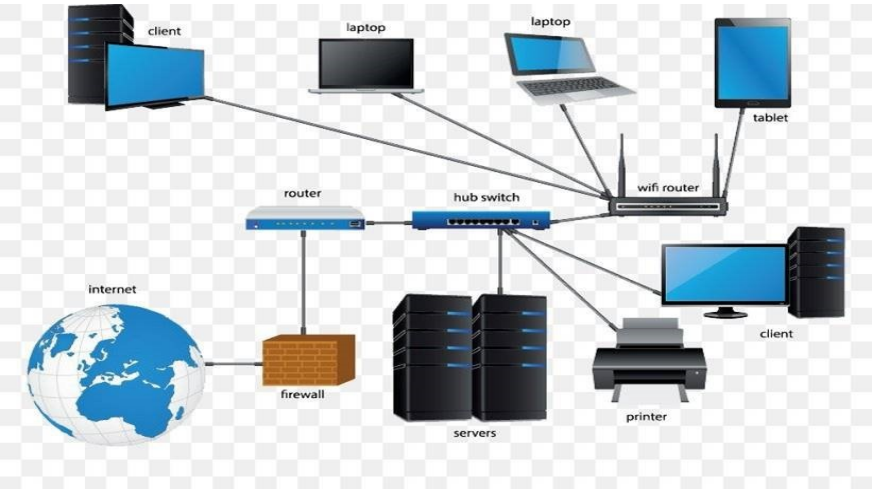
Hệ thống mạng doanh nghiệp còn được biết đến với tên gọi là mạng nội bộ công ty. Hệ thống mạng cho doanh nghiệp là hệ thống kết nối máy tính và những thiết bị khác để trao đổi, chia sẻ thông tin, dữ liệu trong quá trình làm việc. Hệ thống mạng bao gồm những loại mạng khác nhau như mạng LAN hay mạng WAN.

Mạng LAN

LAN là viết tắt của Local Area Network tạm dịch là mạng máy tính nội bộ, giao tiếp này cho phép các máy tính kết nối với nhau để cùng làm việc và chia sẻ dữ liệu. Kết nối này được thực hiện thông qua sợi cáp LAN hoặc Wifi (không dây) trong không gian hẹp, chính vì thế nó chỉ có thể sử dụng được trong một phạm vi giới hạn như phòng làm việc, trong nhà, trường học,…

Để xây dựng hệ thống mạng LAN cho công ty sẽ bao gồm: Máy chủ (server), các máy khách (client), các loại thiết bị ghép nối, card mạng và dây cáp.

Hiện nay, hệ thống mạng nội bộ doanh nghiệp đã và đang được triển khai phổ biến tại nhiều địa điểm như: Nội bộ một phòng ban, văn phòng trong công ty, trường học, bệnh viện,...



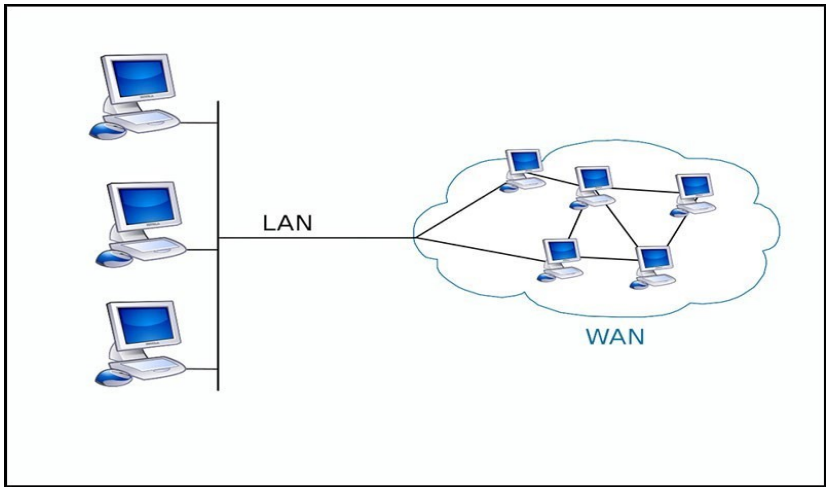
Hình 1: Mạng LAN

Mạng WAN

Mạng WAN (Wide Area Network) hay còn gọi là mạng diện rộng được kết hợp giữa mạng MAN và mạng LAN thông qua thiết bị vệ tinh, cáp quang, cáp dây điện.

Trong WAN giao thức sử dụng chủ yếu là giao thức TCP/IP, đường truyền băng thông thay đổi phụ thuộc vị trí lắp đặt. Mạng diện rộng WAN mang lại khả năng kết nối rộng lớn cả một quốc gia hoặc toàn cầu.

So với thiết kế hệ thống mạng LAN cho công ty, mạng WAN kết nối được các thiết bị ở khu vực rộng hơn, không gặp rào cản về vấn đề địa lý. Chúng tạo ra hệ thống mạng doanh nghiệp quốc gia phủ rộng giữa nhiều thành phố hoặc tỉnh thành. Mạng WAN được thiết kế để trở thành một mạng riêng của tổ chức, hoặc để có kết nối rộng như vậy sẽ cần thông qua một hạ tầng mạng công cộng hay một công ty viễn thông.



Hình 2: Mạng WAN

Ngoài ra, trong hệ thống mạng doanh nghiệp, có ba mô hình mạng phổ biến nhất hiện nay là:

- Mô hình mạng trạm – chủ (Client – Server): Có hai loại thiết bị là máy chủ (Server) và máy trạm (Client).

- Mô hình mạng ngang hàng (Peer to Peer): Không có sự phân biệt giữa máy chủ và máy trạm.

- Mô hình mạng lai (Hybrid): Kết hợp các yếu tố của cả hai mô hình trên.

Tùy thuộc vào quy mô và nhu cầu cụ thể của doanh nghiệp, mỗi loại mạng đều có những đặc điểm và ứng dụng riêng biệt, phục vụ cho các mục đích khác nhau trong môi trường doanh nghiệp.

1.1.2. Vai trò

Hệ thống mạng doanh nghiệp đóng vai trò rất quan trọng như:

- *Phát triển cộng đồng mạng doanh nghiệp:* Lắp đặt hệ thống mạng sẽ giúp phát triển cộng đồng mạng xã hội cho doanh nghiệp. Điều này giúp tăng độ nhận diện, phủ sóng thương hiệu đồng thời giúp doanh nghiệp dễ dàng hơn khi tìm kiếm khách hàng trung thành và tương tác với họ một cách nhanh chóng nhất.

- *Hỗ trợ quá trình quản lý và giám sát nhân viên:* Thiết kế hệ thống hạ tầng mạng cho doanh nghiệp sẽ hỗ trợ ban quản lý công ty giám sát và theo dõi hiệu quả làm việc của nhân viên một cách đơn giản và tiết kiệm thời gian hơn. Nhờ vậy, doanh nghiệp không chỉ tăng hiệu quả làm việc mà còn tiết kiệm được một khoản chi phí nhất định.

- *Hỗ trợ mở rộng thị trường:* Hệ thống mạng doanh nghiệp là cần thiết trong việc mở rộng thị trường, tiếp cận đối tượng khách hàng tiềm năng và tăng doanh thu cho doanh nghiệp. Bạn có thể quảng cáo trực tuyến trên mạng xã hội để đưa tên tuổi của doanh nghiệp đến gần hơn với khách hàng đồng thời tăng tỷ lệ chuyển đổi doanh thu cho doanh nghiệp.

- *Đo lường, theo dõi qua trình kinh doanh của doanh nghiệp:* Thiết kế hệ thống mạng cho doanh nghiệp là cách tốt nhất giúp doanh nghiệp đo lường và theo dõi quá trình kinh doanh. Với hệ thống mạng lưới rộng khắp, các công việc được theo dõi và đo lường kết quả bằng những phần mềm, dịch vụ trực tuyến thông minh.

- *Tăng sự hợp tác giữa các phòng ban trong nội bộ doanh nghiệp:* Nhờ hệ thống mạng nội bộ, các phòng ban trong doanh nghiệp sẽ dễ dàng hơn trong việc kết nối với nhau, chia sẻ tài liệu và hỗ trợ nhau trong công việc. Việc kết nối giữa các phòng ban là điều cần thiết giúp công việc diễn ra suôn sẻ và dễ dàng hơn rất nhiều.

- *Tăng hiệu quả kinh doanh tối đa:* Xây dựng hệ thống mạng cho doanh nghiệp sẽ giúp hỗ trợ chủ doanh nghiệp tăng hiệu quả kinh doanh lên tối đa. Với hệ thống mạng doanh nghiệp, bạn có thể đo lường, theo dõi kết quả kinh doanh bằng công cụ phân tích, giám sát. Đồng thời, bạn có thể xử lý nhiều đầu việc cùng một lúc và kết hợp quảng cáo trực tiếp bằng cách sử dụng các nền tảng tiếp thị số.

- *Tiếp thị toàn cầu:* Các doanh nghiệp xây dựng hệ thống mạng giúp hoạt động kinh doanh diễn ra tốt hơn, tiết kiệm thời gian, chi phí và nhân lực. Ngoài ra, hệ thống mạng rộng khắp cũng giúp doanh nghiệp dễ dàng tiếp thị toàn cầu vượt qua mọi rào cản về ngôn ngữ, văn hoá và địa lý.

1.2. Hệ thống người dùng trong các mạng doanh nghiệp

1.2.1. Khái niệm

Hệ thống người dùng trong mạng doanh nghiệp là một cơ chế quản lý thông tin về những người được phép truy cập và sử dụng tài nguyên của mạng. Hệ thống này có nhiệm vụ:

- Quản lý người dùng: Tạo, xóa, sửa đổi và vô hiệu hóa tài khoản người dùng.

- Phân quyền truy cập: Cấp hoặc thu hồi quyền truy cập vào các tài nguyên mạng khác nhau cho từng người dùng.

- Theo dõi hoạt động: Theo dõi và ghi lại hoạt động của người dùng trên mạng để phát hiện các hành vi đáng ngờ hoặc lạm dụng.

- Thực thi chính sách: Đảm bảo người dùng tuân thủ chính sách bảo mật và sử dụng tài nguyên mạng của doanh nghiệp.

- Tích hợp với các hệ thống khác: Tích hợp với các hệ thống khác như Active Directory và hệ thống email để tự động hóa quản lý người dùng và chia sẻ thông tin.

1.2.2. Cấu trúc

Hệ thống người dùng mạng doanh nghiệp bao gồm:

- Nhân viên: Người dùng được uỷ quyền truy cập vào các tài nguyên và ứng dụng của công ty.

- Đối tác: Nhà cung cấp, khách hàng và các thực thể bên ngoài khác có mối quan hệ kinh doanh với công ty.

- Khách hàng: Người dùng bên ngoài truy cập vào các dịch vụ hoặc cổng thông tin của công ty.

- Quản trị viên hệ thống: Người dùng có quyền truy cập nâng cao vào hệ thống để quản lý, giám sát và bảo trì.

- Nhóm hỗ trợ kỹ thuật: Người dùng chịu trách nhiệm khắc phục sự cố, cung cấp hỗ trợ kỹ thuật và bảo trì hệ thống.

- Nhà thầu: Người dùng được thuê ngoài để thực hiện các nhiệm vụ hoặc dự án cụ thể.

1.2.3. Phân loại

Mạng doanh nghiệp, người dùng được phân loại thành các cấp độ truy cập khác nhau, tuỳ thuộc vào nhu cầu và cấp độ bảo mật bắt buộc của họ. Dưới đây là một phân loại hệ thống phổ biến:

Người dùng tiêu chuẩn: Là người dùng cơ bản với các đặc quyền hạn chế, được cấp quyền truy cập vào các ứng dụng và tài nguyên cần thiết để hoàn thành nhiệm vụ công việc và thường có các biện pháp bảo mật được cấu hình sẵn để hạn chế rủi ro.

Ví dụ: Nhân viên văn phòng, bộ phân tiếp tân, …

Người dùng nâng cao: Là những người dùng có nhu cầu truy cập rộng hơn, được cấp quyền truy cập vào các ứng dụng chuyên dụng hoặc tài nguyên nhạy cảm hơn và có thể thực hiện các tác vụ quản trị hạn chế.

Ví dụ: quản trị viên hệ thống cấp thấp, trưởng nhóm, …

Người dùng đặc quyền: Là người dùng có quyền truy cập và kiểm soát toàn diện đối với hệ thống, đồng thời có thể tạo người dùng cuối - người sử dụng các ứng dụng và dịch vụ mạng.

Người quản trị hệ thống:

- Quản trị viên mạng: Quản lý hệ thống mạng tổng thể

- Quản trị viên hệ thống: Quản trị các máy chủ, dịch vụ và tài nguyên hệ thống

- Quản trị viên bảo mật: Đảm bảo bảo mật của hệ thống mạng

- Quản trị viên cơ sở dữ liệu: Quản lý và bảo trì cơ sở dữ liệu

Nhà phát triển ứng dụng:

- Nhà phát triển ứng dụng: Phát triển và bảo trì các ứng dụng mạng

- Nhà phân tích kinh doanh: Thù nhập và phân tích các yêu cầu kinh doanh để thiết kế các ứng dụng.

Người hỗ trợ IT:

- Đội ngũ hỗ trợ IT cấp 1: Cung cấp hỗ trợ kỹ thuật cơ bản cho người dùng cuối

- Đội ngũ hỗ trợ IT cấp 2 hoặc cấp 3: giaiir quyết các vấn đề kỹ thuật sửa đổi hoặc xoá người dùng, nhóm và tài nguyên.

- Thường được yêu cầu xác thực bổ sung đẻ đảm bảo tính toàn vẹn của hệ thống

Ví dụ: quản trị viên mạng, quản trị viên hệ thống, …

Người dùng khách: Là người dùng tạm thời không thuộc tổ chức, được cấp quyền truy cập có giới hạn vào các tài nguyên nhất định và thường được phân bổ tài khoản riêng biệt hoặc truy cập mạng khách.

Ví dụ: Khách hàng đối tác, nhà thầu, …

Người dùng hệ thống: Là tài khoản đặc biệt được tạo để thực thi các tác vụ tự động hoặc dịch vụ nền, không có tương tác trực tiếp với người dùng và thường được sử dụng cho các dịch vụ như sao lưu, giám sát hoặc quản lý cập nhật.

Ví dụ: Tài khoản dịch vụ, Daemon, …

Người dùng bị vô hiệu hoá: Là tài khoản không còn hoạt động hoặc đã bị vô hiệu hoá, không thể đăng nhập hoặc truy cập bất kỳ tài nguyên nào và được giữ lại cho mục đích kiểm toán hoặc tuân thủ.

Người dùng từ xa:

- Người dùng di động: Truy cập mạng doanh nghiệp từ các thiết bị di động

- Người dùng từ xa: Truy cập mạng doanh nghiệp từ các vị trí bên ngoài

Nhà thầu:

- Nhà thầu bên thứ ba: Cung cấp các dịch vụ và hỗ trợ chuyên môn cho hệ thống mạng.

- Đối tác kinh doanh: Truy cập mạng doanh nghiệp để trao đổi dữ liệu và cộng tác

Khách truy cập:

- Khách truy cập nội bộ: Những người không phải là nhân viên nhưng cần truy cập vào mạng doanh nghiệp.

- Khách truy cập bên ngoài: Những người không thuộc doanh nghiệp nhưng cần truy cập vào một số tài nguyên mạng giới hạn.

II. THỰC TRẠNG VỀ VIỆC ĐẢM BẢO AN TOÀN ĐỐI VỚI HỆ THỐNG NGƯỜI DÙNG TRONG CÁC MẠNG DOANH NGHIỆP

2.1. Thực trạng về việc đảm bảo an toàn đối với hệ thống người dùng trong các mạng doanh nghiệp hiện nay ở Việt Nam.

Hiện nay, việc đảm bảo an toàn cho hệ thống người dùng trong các mạng doanh nghiệp tại Việt Nam đang đối mặt với những thách thức lớn. Các cuộc tấn công mạng ngày càng trở nên phức tạp và tinh vi hơn, đặc biệt là các hình thức tấn công như khai thác lỗ hổng bảo mật, tấn công dò quét mạng và tấn công APT.

Các loại cuộc tấn công mạng trong mạng doanh nghiệp rất đa dạng và phức tạp có thể kể đến:

- Tấn công bằng phần mềm độc hại (Malware attack): Bao gồm spyware, ransomware, virus và worm.

- Tấn công giả mạo (Phishing attack): Sử dụng email giả mạo hoặc trang web lừa đảo để đánh cắp thông tin.

- Tấn công trung gian (Man-in-the-middle attack): Hacker chen vào giữa giao tiếp của hai bên để đánh cắp dữ liệu.

- Tấn công từ chối dịch vụ (DoS và DDoS): Làm quá tải hệ thống để ngăn chặn dịch vụ từ việc hoạt động bình thường.

- Tấn công cơ sở dữ liệu (SQL injection): Khai thác lỗ hổng trong cơ sở dữ liệu để truy cập hoặc phá hủy dữ liệu.

- Khai thác lỗ hổng Zero-day (Zero-day attack): Tận dụng lỗ hổng chưa được biết đến hoặc chưa được vá trong phần mềm.

Khi một doanh nghiệp trở thành mục tiêu của một cuộc tấn công, hậu quả không chỉ dừng lại ở việc thông tin bảo mật của doanh nghiệp bị lộ ra ngoài mà còn có thể làm ảnh hưởng đến thông tin cá nhân của nhân viên. Việc thông tin cá nhân bị đánh cắp có thể dẫn đến nhiều vấn đề nghiêm trọng như lừa đảo, mạo danh, hoặc thậm chí là vi phạm quy định về bảo vệ dữ liệu cá nhân.

Các số liệu thống kê cho thấy:

Trong những năm gần đây, Việt Nam đã chứng kiến việc tăng số lượng các cuộc tấn công mạng vào các doanh nghiệp. Theo báo cáo của Bộ Thông tin và Truyền thông, số lượng cuộc tấn công mạng tại Việt Nam đã tăng đáng kể từ 9.159 lần vào năm 2018 lên đến 13.382 vào năm 2020. Các cuộc tấn công thường nhắm vào thông tin quan trọng của doanh nghiệp như dữ liệu khách hàng, thông tin tài chính hoặc thông tin bí mật.

Ngoài ra, theo báo cáo của BKAV, một công ty bảo mật Việt Nam, hơn 90% các doanh nghiệp tại Việt Nam đã bị tấn công mạng ít nhất một lần trong năm 2020. Các phương thức tấn công phổ biến bao gồm tấn công phần mềm độc hại, tấn công mạng xã hội và tấn công phishing. Để bảo vệ thông tin và dữ liệu của mình, các doanh nghiệp cần đầu tư vào các giải pháp bảo mật mạng hiệu quả và nâng cao nhận thức về an ninh mạng cho nhân viên.

Theo tổng kết của công ty Công nghệ An ninh mạng quốc gia Việt Nam (NCS) năm 2023, Việt Nam đã ghi nhận tổng cộng 13.900 vụ tấn công mạng vào các tổ chức, tăng 9,5% so với năm 2022, trung bình mỗi tháng 1.160 vụ. Trong đó, có 550 trang thông tin bị xâm nhập, chèn mã quảng cáo cờ bạc, cá độ và 83.000 máy tính, máy chủ bị mã độc mã hoá dữ liệu tống tiền tấn công. Điều này cho thấy mức độ nghiêm trọng và tần suất cao của các cuộc tấn công mạng đối với mạng doanh nghiệp tại Việt Nam. Các mục tiêu chịu nhiều cuộc tấn công nhất là các cơ quan chính phủ, hệ thống ngân hàng, tổ chức tài chính và công nghiệp, đồng thời cũng ảnh hưởng lớn đến hệ thống người dùng trong mạng doanh nghiệp.

Ngoài ra, trong năm 2021, có tới 100 triệu lượt dữ liệu về người dùng internet và tổ chức doanh nghiệp Việt Nam bị lộ lọt, và hơn 100 nghìn tài khoản, mật khẩu được rao bán trên các nền tảng chợ đen. Điều này cho thấy nguy cơ mất an toàn thông tin mạng ở

Việt Nam là rất cao và đòi hỏi các biện pháp phòng ngừa và ứng phó mạnh mẽ hơn từ phía các doanh nghiệp và cơ quan chức năng.

=> Từ các dữ liệu trên cho thấy, tình trạng an toàn bảo mật thông tin hệ thống người dùng trong mạng doanh nghiệp đang gây ra lo ngại. Mặc dù nhiều doanh nghiệp đã cố gắng tăng cường bảo mật hệ thống, nhưng vẫn còn tồn tại một số tổ chức chưa đảm bảo an toàn hệ thống mạng một cách chặt chẽ. Việc thông tin của người dùng trong mạng doanh nghiệp bị rò rỉ có thể gây ra những hậu quả nghiêm trọng như mất an toàn thông tin và ảnh hưởng đến uy tín của doanh nghiệp.

Trong thời đại công nghệ thông tin hiện nay, việc bảo vệ an toàn mạng trở thành vấn đề cực kỳ quan trọng đối với các doanh nghiệp. Tuy nhiên, nhiều người dùng vẫn chưa nhận thức đầy đủ về nguy cơ từ các cuộc tấn công mạng. Việc lướt web, check mail và nhấp vào các đường link không rõ nguồn gốc đều tạo cơ hội cho các hacker tấn công và đánh cắp thông tin quan trọng của cá nhân và doanh nghiệp một cách dễ dàng. Sự thiếu cảnh giác này có thể dẫn đến hậu quả nghiêm trọng không chỉ cho cá nhân mà còn cho toàn bộ doanh nghiệp.

Tại Việt Nam, việc nhấp vào đường link lạ có thể dẫn đến nhiều hậu quả nghiêm trọng, đặc biệt là trong môi trường doanh nghiệp. Các cuộc tấn công mạng thông qua đường link lừa đảo (phishing) có thể gây ra mất thông tin khách hàng và dữ liệu quan trọng. Theo một nghiên cứu, 59% doanh nghiệp vừa và nhỏ tại Việt Nam đã gặp sự cố mạng trong năm qua, và 86% trong số đó đã bị mất thông tin khách hàng.

Cùng với sự phát triển mạnh mẽ về số lượng người dùng Internet, đặc biệt là mua sắm online, các vụ tấn công mạng gia gia tăng, kể cả về số lượng, quy mô; các hình thức tấn công tinh vi hơn. Trung tâm ứng cứu khẩn cấp máy tính Việt Nam đã ghi nhận và xử lý gần 10.000 vụ tấn công website. Trong đó, gần 50% các sự cố đến từ phát tán mã độc thông qua những lỗ hổng bảo mật.

Trong giới kinh doanh ngày nay, việc bảo vệ thông tin dữ liệu của người dùng mạng doanh nghiệp trở nên ngày càng quan trọng và khó khăn hơn bao giờ hết. Một thực tế đáng lo ngại là thông tin dữ liệu có thể bị đánh cắp bởi những bộ phận nội bộ trong doanh nghiệp, gây ra rủi ro đáng kể cho hệ thống an toàn thông tin. Việc sử dụng chung một mạng cũng tạo điều kiện thuận lợi cho những kẻ xấu tấn công từ bên trong mạng, đe dọa tính bảo mật của doanh nghiệp.

Theo các số liệu thống kê gần đây, vấn đề dữ liệu bị đánh cắp bởi nhân viên nội bộ trong các doanh nghiệp tại Việt Nam đang ngày càng trở nên nghiêm trọng. Một số điểm đáng chú ý từ các báo cáo bao gồm:

- Có hơn 11.000 tài khoản giáo dục và hơn 30.000 tài khoản ngân hàng đã bị xâm nhập và đánh cắp trong năm 2023.

- Tổng thiệt hại về tài chính do việc đánh cắp dữ liệu gây ra lên đến hơn 16 tỉ đồng.

- Số lượng bản ghi thông tin cá nhân bị lộ lọt tăng gần gấp đôi so với năm trước.

- Đa số hacker sử dụng tài khoản nội bộ đánh cắp để trích xuất dữ liệu sau đó rao bán, gây ra thiệt hại lớn cho doanh nghiệp.

Những số liệu này chỉ ra rằng việc quản lý và bảo mật thông tin nội bộ là một yếu tố quan trọng mà các doanh nghiệp cần phải chú trọng để bảo vệ dữ liệu của mình khỏi những rủi ro an ninh mạng.

Một vấn đề quan trọng về an toàn của hệ thống người dùng mạng doanh nghiệp hiện nay là sự cần thiết phải bảo vệ thông tin quan trọng của doanh nghiệp khỏi các cuộc tấn công mạng. Để đảm bảo an toàn, một số doanh nghiệp đã áp dụng biện pháp giám sát chặt chẽ các thiết bị mà nhân viên sử dụng. Tuy nhiên, việc theo dõi thông tin cá nhân hay lịch sử truy cập của người dùng cũng có thể dẫn đến việc thông tin bị lộ hoặc rò rỉ, gây mất niềm tin và ảnh hưởng đến quyền riêng tư của nhân viên.

Theo các số liệu thống kê, việc theo dõi thông tin cá nhân và lịch sử truy cập của người dùng tại Việt Nam có thể dẫn đến các vấn đề về bảo mật và quyền riêng tư:

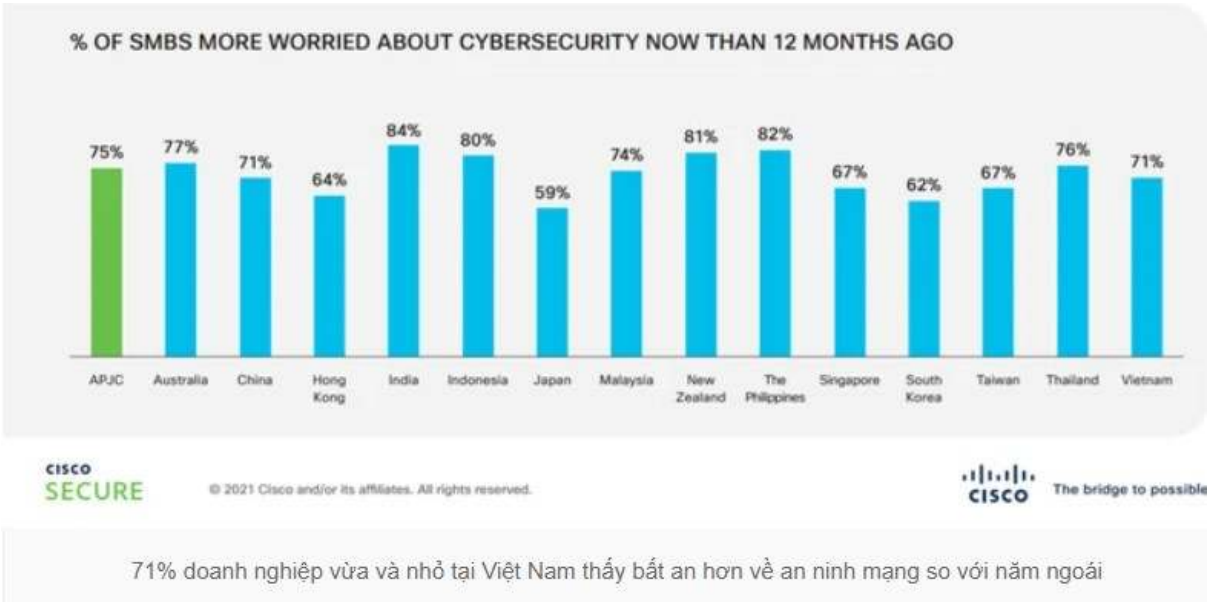
Việt Nam có 77 triệu người dùng Internet và 70 triệu người tham gia mạng xã hội, với tổng số kết nối di động hoạt động là 161,6 triệu. Sự gia tăng này trong việc sử dụng Internet và mạng xã hội đồng nghĩa với việc tăng khả năng rủi ro về an ninh mạng và việc theo dõi thông tin cá nhân.

Các hệ thống như website, ứng dụng hoặc email doanh nghiệp trở thành mục tiêu hấp dẫn cho các tấn công và vi phạm bảo mật, làm tăng nguy cơ thông tin bị lộ hoặc rò rỉ.

Theo nghiên cứu mới của Cisco, các doanh nghiệp vừa và nhỏ tại Việt Nam đang bị lộ thông tin, bị tấn công và có nhiều mối đe dọa an ninh mạng hơn so với trước đây:

88% doanh nghiệp vừa và nhỏ Việt Nam bị tấn công mạng mất thông tin khách hàng năm 2021; theo kết quả nghiên cứu, 59% doanh nghiệp vừa và nhỏ tại Việt Nam gặp sự cố mạng trong năm qua. Hậu quả của những sự cố này là 86% số doanh nghiệp bị mất thông tin khách hàng vào tay của những kẻ xấu. Bên cạnh việc mất dữ liệu khách hàng, các doanh nghiệp vừa và nhỏ tại Việt Nam gặp sự cố mạng còn bị mất dữ liệu nhân viên (67%), email nội bộ (61%), thông tin tài chính (58%), sở hữu trí tuệ (56%) và thông tin kinh doanh nhạy cảm (51%). Ngoài ra, 61% doanh nghiệp thừa nhận sự cố mạng tác động tiêu cực đến danh tiếng của họ.

Những sự cố này đang ảnh hưởng đáng kể đến tình hình kinh doanh. 30% doanh nghiệp vừa và nhỏ tại Việt Nam bị tấn công mạng cho biết họ tổn thất khoảng 500.000 USD hoặc nhiều hơn, trong đó 4% cho rằng họ tổn thất tầm một triệu đô la Mỹ hoặc hơn.



71% doanh nghiệp vừa và nhỏ tại Việt Nam thấy bất an hơn về an ninh mạng so với năm ngoái

=> Trong thế giới công nghệ hiện đại, việc đảm bảo an toàn cho hệ thống người dùng trong các mạng doanh nghiệp ở Việt Nam đang trở thành một vấn đề cực kỳ quan trọng. Với sự phát triển của internet và các công nghệ thông tin, các mối đe dọa từ các cuộc tấn công mạng ngày càng phức tạp và nguy hiểm hơn. Để bảo vệ thông tin quan trọng và dữ liệu của doanh nghiệp, sự nhận thức về an ninh mạng cần được nâng cao và đầu tư vào các giải pháp công nghệ hiện đại là điều không thể phủ nhận.

2.2. Một số nguyên nhân chính gây mất an toàn thông tin đối với hệ thống người dùng trong các mạng doanh nghiệp.

Có rất nhiều nguyên nhân khác nhau dẫn đến việc mất an toàn thông tin, chúng được chia thành hai loại như sau:

Nguyên nhân chủ quan (từ phía người dùng trong doanh nghiệp):

- *Nhận thức an toàn thông tin chưa tốt:* Thiếu tính kiến thức cơ bản về an ninh mạng có thể dẫn đến việc nhân viên không nhận biết được các mối đe doạ, từ đó trở thành nạn nhân của các cuộc tấn công như lừa đảo qua email hoặc social engineering.

- *Không phân quyền rõ ràng trong quản lý:* Khi người quản trị không phân quyền rõ ràng cho thành viên, nhân viên nội bộ có thể đánh cắp hoặc thay đổi thông tin quan trọng của nội bộ doanh nghiệp.

- *Lỗ hổng tồn tại trên thiết bị:* Việc tải và cài đặt phần mềm hoặc ứng dụng không rõ nguồn gốc có thể chứa lỗ hổng bảo mật, tạo cơ hội cho hacker tấn công vào hệ thống.

- *Sự lơ là trong việc cập nhật và bảo trì hệ thống, phần mềm bảo mật:* Khi không cập nhật các bản vá bảo mật mới nhất cho hệ thống và phần mềm, doanh nghiệp có thể để lộ các lỗ hổng bảo mật đã được khắc phục, mở cửa cho các cuộc tấn công từ phía hacker. Và nếu không thực hiện đúng quy trình bảo trì hệ thống và phần mềm, có thể dẫn đến việc thiếu sót trong việc kiểm tra, sửa chữa và bảo trì các thành phần quan trọng, tạo điều kiện cho các mối đe dọa xâm nhập.

Nguyên nhân khách quan:

- *Cuộc tấn công từ Hacker, virus, malware hoặc các đối thủ tiềm năng khác:* Các cuộc tấn công từ các thế lực xấu có thể dẫn đến việc xâm nhập vào hệ thống mạng của doanh nghiệp, đánh cắp thông tin quan trọng hoặc gây hỏng hóc hệ thống làm gián đoạn hoạt động kinh doanh.

- *Sự phức tạp và đa dạng, ngày càng tinh vi của các mối đe doạ mạng hiện nay:* Với sự phát triển của công nghệ, các mối đe dọa mạng ngày càng phức tạp và đa dạng chẳng hạn như phần mềm tống tiền, tấn công lừa đảo và các chiến thuật lừa đảo qua mạng, gây ra rủi ro đáng kể cho các doanh nghiệp, có thể không có sẵn các biện pháp phòng vệ cần thiết.

- *Sự thiếu hụt về cơ sở hạ tầng bảo mật của doanh nghiệp:* Nếu hệ thống bảo mật của doanh nghiệp không được xây dựng và duy trì một cách chặt chẽ, có thể dễ dàng bị tấn công và thông tin quan trọng bị đánh cắp.

- *Yêu cầu tuân thủ quy định:* Việc không tuân thủ các quy định bảo vệ dữ liệu và tiêu chuẩn ngành có thể dẫn đến hậu quả pháp lý và thiệt hại về danh tiếng cho doanh nghiệp.

- *Chiến thuật kỹ thuật xã hội:* Những kẻ tấn công có thể sử dụng các kỹ thuật xã hội để thao túng nhân viên tiết lộ thông tin nhạy cảm hoặc cấp quyền truy cập vào các hệ thống an toàn.

III. NGUY CƠ, TỔN THẤT VÀ CÁCH PHÒNG TRÁNH ĐỂ ĐẢM BẢO AN TOÀN ĐỐI VỚI HỆ THỐNG NGƯỜI DÙNG TRONG CÁC MẠNG DOANH NGHIỆP

Về phía người dùng: Người dùng là những người sử dụng các thiết bị, ứng dụng, dịch vụ của doanh nghiệp để thực hiện các công việc, giao dịch, trao đổi thông tin.	
Nguy cơ và tổn thất	**Cách phòng tránh**
1. Bị tấn công xâm nhập mạng từ bên trong nội bộ: Tấn công xâm nhập mạng từ bên trong nội bộ là một trong những hình thức tấn công mạng nguy hiểm và khó phát hiện nhất. Đây là trường hợp một người dùng khác trong cùng mạng doanh nghiệp có ý định xấu, lợi dụng các lỗ hổng bảo mật để truy cập vào hệ thống của người dùng mục tiêu, đánh cắp, thay đổi, xóa bỏ các dữ liệu quan trọng. **Nguyên nhân:** - Sự bất mãn, thù hận, đố kỵ, cạnh tranh của nhân viên đối với công ty hoặc đồng nghiệp. - Sự dụ dỗ, hối lộ, đe dọa, tống tiền của bên thứ ba đối với nhân viên. - Sự thiếu kiến thức, kỹ năng, chủ quan, cẩu thả, bất cẩn của nhân viên trong việc bảo vệ thông tin. - Sự lợi dụng, chiếm đoạt, mượn danh tính của hacker đối với nhân viên. **Tổn thất:** - Tổn thất về riêng tư, bảo mật: Người	- *Đào tạo và nâng cao nhận thức về an toàn thông tin cho nhân viên:* Đào tạo nhân viên về các mối đe dọa từ bên trong và cách phát hiện các hoạt động không bình thường. Nhân viên nên được thông báo cũng như huấn luyện về các biện pháp cần thiết để bảo vệ thông tin quan trọng và hệ thống. - *Giám sát hoạt động:* Thực hiện giám sát đối với các hoạt động mạng và hệ thống để phát hiện các hoạt động không bình thường hoặc đáng ngờ, bao gồm việc theo dõi lưu lượng mạng và sự hoạt động của người dùng. - *Phát hiện và ứng phó nhanh chóng:* Sử dụng các giải pháp phát hiện xâm nhập (IDS) và phòng thủ xâm nhập (IPS) để phát hiện và ngăn chặn các hoạt động không mong muốn trên mạng nội bộ; đồng thời đáp ứng nhanh chóng khi phát hiện các sự cố bằng cách có kế hoạch ứng phó sẵn có. - *Thiết lập mật khẩu mạnh:* Khuyến khích

dùng có thể bị xâm phạm quyền riêng tư, bị theo dõi, nghe lén, quay lén, bị tiết lộ các thông tin cá nhân, gia đình, công việc, học tập. - Bị thay đổi, xóa, hỏng, hoặc mất dữ liệu quan trọng trên hệ thống hoặc website. - Bị lợi dụng tài nguyên máy tính hoặc hệ thống mạng để thực hiện các hành vi phạm pháp khác. Điều này có thể làm chậm hoặc làm hỏng máy tính, cũng như gây ra những rắc rối pháp lý cho người dùng. **VD:** Một nhân viên có quyền truy cập vào cơ sở dữ liệu của công ty có thể lợi dụng điều đó để sao chép, xóa hoặc thay đổi dữ liệu quan trọng, hoặc cài đặt một chương trình gián điệp để theo dõi hoặc điều khiển các thiết bị khác trong mạng.	việc sử dụng mật khẩu mạnh và thay đổi định kỳ. Bên cạnh đó, sử dụng các biện pháp bảo mật bổ sung như xác minh hai yếu tố để bảo vệ tài khoản cũng là một trong số những giải pháp hữu hiệu. - *Cập nhật và bảo trì:* Đảm bảo rằng tất cả các hệ thống và phần mềm được cập nhật phiên bản mới nhất đầy đủ và định kỳ. Lỗ hổng bảo mật có thể được khai thác bởi các tác nhân xâm nhập, do đó việc duy trì hệ thống an toàn là rất quan trọng. - *Kiểm tra thiết bị ngoại vi:* Đảm bảo rằng tất cả các thiết bị ngoại vi như USB và đĩa cứng di động được kiểm tra trước khi được kết nối vào hệ thống. - *Xác thực và ủy quyền:* Sử dụng các phương tiện xác thực mạnh mẽ và các phương pháp ủy quyền an toàn để đảm bảo rằng chỉ các người dùng được ủy quyền mới có thể truy cập vào các tài nguyên quan trọng. - *Kiểm soát quyền truy cập:* Hạn chế quyền truy cập của nhân viên chỉ đến các tài nguyên và thông tin cần thiết cho công việc của họ, "Nguyên tắc ít nhất là đủ" nên được áp dụng ở mức độ rộng rãi.
2. Bị đánh cắp dữ liệu, bị mất, hỏng, sửa đổi thông tin: Đây là trường hợp một bên thứ ba ngoài mạng doanh nghiệp, thường là các hacker, tin tặc, có khả năng chiếm quyền kiểm soát hệ thống của người dùng, lấy đi các thông tin cá nhân,	- *Sao lưu và lưu trữ dữ liệu:* Thực hiện sao lưu dữ liệu quan trọng, và lưu trữ ở nhiều nơi khác nhau, như ổ cứng ngoài, đĩa CD, USB, hoặc đám mây dữ liệu định kỳ là một biện pháp quan trọng để đảm bảo rằng có thể khôi phục lại dữ liệu nếu

tài khoản, mật khẩu, số thẻ, số tài khoản ngân hàng, thông tin giao dịch, thông tin bí mật nhà nước. Nguy hiểm hơn, tin tặc có thể đánh cắp toàn bộ dữ liệu rồi ép nạn nhân trả tiền chuộc. **Nguyên nhân:** Các hacker, tin tặc có thể tấn công hệ thống của người dùng bằng nhiều cách, như: khai thác các lỗ hổng bảo mật, sử dụng các phần mềm độc hại, giả mạo các trang web, email, tin nhắn đáng tin cậy, lợi dụng sự thiếu hiểu biết, cẩu thả, bất cẩn của người dùng. Mục đích của các hacker, tin tặc có thể là: kiếm tiền, trả thù, chứng tỏ khả năng, đánh cắp thông tin bí mật, gây rối loạn, phá hoại. **Tổn thất:** Khi hệ thống của người dùng bị tấn công, các hacker, tin tặc có thể lấy đi các thông tin cá nhân, tài khoản, mật khẩu, số thẻ, số tài khoản ngân hàng, thông tin giao dịch, thông tin bí mật nhà nước. Những thông tin này có thể bị sử dụng để: mua sắm, thanh toán trái phép, lừa đảo, chiếm đoạt tài sản, bôi nhọ, đe dọa, tống tiền, tiết lộ, phát tán, xâm phạm quyền riêng tư, an ninh, bảo mật. Nguy hiểm hơn, các hacker, tin tặc có thể đánh cắp toàn bộ dữ liệu trên hệ thống của người dùng, mã hóa chúng và đòi tiền chuộc để giải mã. Đây là một hình thức tấn công mạng bằng ransomware, có thể gây ra những tổn thất nghiêm trọng về tài chính, thời gian, công sức, dữ liệu.	xảy ra sự cố. - *Sử dụng phần mềm bảo vệ dữ liệu:* Cài đặt và sử dụng các phần mềm bảo mật, bao gồm phần mềm chống virus, firewall, và phần mềm chống malware để bảo vệ dữ liệu của bạn khỏi các mối đe dọa trực tuyến. - *Mã hóa dữ liệu:* Việc mã hóa dữ liệu nhằm mục đích bảo vệ những dữ liệu quan trọng, đặc biệt là khi chuyển dữ liệu qua mạng hoặc lưu trữ trên các thiết bị di động. - *Quản lý quyền truy cập:* Đảm bảo rằng chỉ có những người cần thiết mới có quyền truy cập vào dữ liệu nhạy cảm, cũng như thiết lập các cơ chế xác thực và kiểm soát quyền truy cập dữ liệu một cách cẩn thận. - *Thực hiện các biện pháp bảo mật vật lý:* Bảo vệ các thiết bị lưu trữ dữ liệu và hệ thống máy chủ bằng cách sử dụng các biện pháp an ninh vật lý như khóa, hệ thống kiểm soát truy cập và camera an ninh. - *Tuân thủ chính sách an ninh:* Tuân thủ tất cả các chính sách an ninh thông tin và hướng dẫn của tổ chức, bao gồm việc giữ bí mật thông tin và tuân thủ các quy định về bảo mật; cũng giúp hạn chế một phần việc dữ liệu bị đánh cắp, bị mất hay hỏng hóc.

VD: Một nhân viên của một công ty bảo hiểm bị lừa bởi một email giả mạo từ người quản lý, yêu cầu cung cấp danh sách khách hàng và thông tin bảo hiểm của họ. Sau đó, nhân viên này nhận ra rằng email đó là của một hacker, và dữ liệu của họ đã bị đánh cắp và bán trên web đen.	
3. Bị tấn công bởi các phần mềm độc hại, bị chèn mã độc, virus vào trong phần mềm, công cụ: Đây là trường hợp người dùng tải về hoặc cài đặt các phần mềm, ứng dụng, plug-in trình duyệt từ các nguồn không đáng tin cậy, có thể chứa các mã độc, virus, trojan, worm, ransomware, spyware, adware, keylogger, rootkit, botnet. **Nguyên nhân:** - Sử dụng các phần mềm crack, tải về các phần mềm lạ, không rõ nguồn gốc, hoặc từ các trang web giả mạo hoặc web đen. - Mở hoặc trả lời các email, tin nhắn, hoặc cuộc gọi nghi ngờ, đặc biệt là những yêu cầu cung cấp thông tin cá nhân, tài khoản, mật khẩu, hoặc dữ liệu quan trọng. - Bấm vào các quảng cáo, đường dẫn, file đính kèm có chứa mã độc, virus, hoặc dẫn đến các trang web độc hại. - Sử dụng các thiết bị lưu trữ di động như USB, thẻ nhớ, ổ cứng ngoài, hoặc các thiết bị IoT (Internet of Things) bị nhiễm mã độc.	- *Sử dụng phần mềm phòng thủ mạng:* Triển khai các giải pháp phòng thủ mạng như Firewalls, Intrusion Detection Systems (IDS) và Intrusion Prevention Systems (IPS) để phát hiện/phòng ngừa xâm nhập để ngăn chặn các truy cập không mong muốn vào hệ thống, cũng như phát hiện và chặn các hoạt động không bình thường. Bên cạnh đó, việc cài đặt các phần mềm chống virus cũng như việc cập nhật định kỳ các phần mềm an ninh để bảo vệ khỏi các mã độc hay virus cũng là một biện pháp hiệu quả. - *Cập nhật và bảo mật phần mềm:* Nên yêu cầu người dùng cập nhật phần mềm và hệ điều hành của họ đến phiên bản mới nhất để khắc phục các lỗ hổng bảo mật đã được khắc phục và ngăn chặn các cuộc tấn công từ những lỗ hổng này. - *Kiểm tra e-mail và tệp đính kèm:* Cần cẩn thận khi mở email từ nguồn không xác định, không mở các tập tin đính kèm từ nguồn không tin cậy, và kiểm tra URL trước khi nhấp vào liên kết để hạn chế

- Không cập nhật hệ điều hành, phần mềm, ứng dụng, hoặc không bảo mật hệ thống mạng, máy tính, thiết bị của mình. **Tổn thất:** - Tổn thất về công nghệ: Người dùng có thể bị ảnh hưởng bởi các sự cố kỹ thuật, như hệ thống bị lỗi, mất kết nối, bị tấn công bởi các phần mềm độc hại, virus, mã độc, v.v. khi sử dụng các thiết bị, phần mềm, ứng dụng trong mạng doanh nghiệp. - Các mã độc, virus này có thể làm hỏng hệ thống, làm chậm máy, gửi thông tin về hacker, mã hóa dữ liệu đòi tiền chuộc, hiển thị quảng cáo phiền phức, ghi lại các thao tác bàn phím, đánh cắp quyền truy cập, biến máy tính thành một phần của mạng lưới tấn công. Hacker có thể sử dụng nhiều kỹ thuật tấn công khác nhau để xâm nhập vào bên trong hệ thống như: Phishing, virus, phần mềm gián điệp, man in middle. **<u>VD:</u>** Vào năm 2017, mã độc tống tiền WannaCry tấn công hơn 200.000 máy tính trên 150 quốc gia, yêu cầu thanh toán tiền chuộc để giải mã dữ liệu bị mã hóa.	việc bị tấn công bởi mã độc hay virus. - *Kiểm tra phần mềm bên thứ ba:* Trước khi cài đặt hoặc sử dụng phần mềm bên thứ ba, hãy đảm bảo rằng nó được tải xuống từ nguồn tin cậy và đã được kiểm tra kỹ lưỡng để tránh sự bùng nổ mã độc.
4. Bị tấn công qua các thiết bị IoT (Internet of Things): Đây là trường hợp người dùng sử dụng các thiết bị thông minh kết nối internet, như camera, cảm biến, đồng hồ, thiết bị đeo, thiết bị y tế, thiết bị gia dụng…. Các thiết bị IoT cũng tiềm ẩn nhiều nguy cơ và rủi ro về an ninh	- *Giám sát và phát hiện:* Triển khai các giải pháp giám sát mạng và hệ thống để phát hiện các hoạt động bất thường từ các thiết bị IoT. Các công cụ giám sát mạng và hệ thống như IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) có thể giúp phát hiện các hoạt

mạng, khiến người dùng có thể bị tấn công qua các thiết bị này. **Nguyên nhân:** - Thiếu bảo mật: Nhiều thiết bị IoT không được thiết kế với bảo mật là ưu tiên, mà chỉ tập trung vào tính năng và hiệu năng. Do đó, chúng có thể có các lỗ hổng bảo mật, như mật khẩu mặc định, giao thức truyền thông không mã hóa, cập nhật phần mềm không đều, v.v. Điều này giúp cho các hacker có thể dễ dàng xâm nhập và kiểm soát các thiết bị IoT. - Thiếu nhận thức: Nhiều người dùng không có đủ kiến thức và kỹ năng về an ninh mạng, cũng như không quan tâm đến việc bảo vệ các thiết bị IoT của mình. Họ có thể không thay đổi mật khẩu mặc định, không kiểm tra nguồn gốc của các thiết bị, không cập nhật phần mềm, không sử dụng các phần mềm bảo mật, v.v. Điều này khiến cho các thiết bị IoT trở thành mục tiêu dễ bị tấn công. - Thiếu quản lý: Nhiều doanh nghiệp không có một chính sách và quy trình quản lý các thiết bị IoT một cách hiệu quả, nhất là khi số lượng thiết bị IoT ngày càng tăng. Họ có thể không kiểm tra và đánh giá an ninh mạng của các thiết bị, không phát hiện và xử lý kịp thời các sự cố, không có kế hoạch phòng ngừa và khắc phục hậu quả, v.v. Điều này khiến cho các thiết bị IoT có thể bị lợi dụng để thực hiện	động không bình thường và ngăn chặn các cuộc tấn công. - *Sử dụng giải pháp bảo mật IoT:* Xem xét triển khai các giải pháp bảo mật IoT chuyên biệt, bao gồm cả giải pháp phát hiện xâm nhập và giải pháp quản lý thiết bị để tăng cường bảo vệ cho mạng và thiết bị IoT. - *Xác định và quản lý thiết bị IoT:* Tổ chức cần thiết lập một quy trình để xác định và quản lý tất cả các thiết bị IoT được kết nối vào mạng của họ. Có thể là việc sử dụng phần mềm quản lý thiết bị (device management software) để giúp kiểm soát, cập nhật và theo dõi các thiết bị IoT trong mạng. - *Tách mạng VLAN:* Sử dụng các mạng VLAN (Virtual Local Area Network) để tách các thiết bị IoT khỏi mạng chính của doanh nghiệp có thể giúp giảm thiểu rủi ro từ các cuộc tấn công trên mạng IoT đến hệ thống chính của doanh nghiệp. - *Sử dụng firewall và mạng riêng ảo (VPN):* Triển khai các giải pháp tường lửa (firewall) và mạng riêng ảo (VPN) để kiểm soát và bảo vệ dữ liệu truyền qua mạng, cũng như từ các thiết bị IoT. - *Theo dõi và đánh giá liên tục:* Liên tục theo dõi và đánh giá tình trạng bảo mật của mạng và các thiết bị IoT để có thể phát hiện sớm và đối phó với các mối đe dọa mới.

các cuộc tấn công mạng. **Tổn thất:** - Các thiết bị này có thể bị hacker khai thác lỗ hổng bảo mật để truy cập vào hệ thống của người dùng, đánh cắp dữ liệu, điều khiển thiết bị, gây ra các hậu quả nguy hiểm cho sức khỏe, an toàn, riêng tư của người dùng. - Tổn thất về an toàn, sức khỏe: Người dùng có thể bị gây ra các tai nạn, chấn thương, ngộ độc, bệnh tật do hacker điều khiển các thiết bị IoT. **VD:** Vào năm 2016, một cuộc tấn công DDoS (từ chối dịch vụ phân tán) lớn nhất từ trước đến nay đã sử dụng hàng triệu thiết bị IoT bị lây nhiễm để làm tê liệt các trang web như Twitter, Netflix và PayPal.	
5. Mã độc lây nhiễm bắt nguồn từ Plug-in trình duyệt: Plug-in trình duyệt là các phần mở rộng hoặc tiện ích được cài đặt vào trình duyệt để tăng cường chức năng hoặc trải nghiệm của người dùng. Tuy nhiên, một số plug-in trình duyệt có thể chứa mã độc, virus, hoặc được tạo ra bởi các hacker để theo dõi hoặc điều khiển các thiết bị của người dùng. **Nguyên nhân:** - Cài đặt các plug-in trình duyệt không rõ nguồn gốc, không đáng tin cậy, hoặc từ các trang web giả mạo hoặc web đen. - Không cập nhật các plug-in trình duyệt, hoặc không kiểm tra các quyền truy cập	- *Hạn chế cài đặt plug-in không cần thiết:* Cần xác định các plug-in cần thiết cho công việc hàng ngày và hạn chế sự cài đặt của các plug-in không được phép. Bên cạnh đó cũng cần xem xét và cập nhật chính sách cài đặt trình duyệt để ngăn chặn việc cài đặt plug-in mà không có sự phê duyệt từ phía quản trị. - *Sử dụng giải pháp bảo mật tiên tiến:* Sử dụng phần mềm chống virus và phần mềm chống độc hại Anti- Malware có khả năng phát hiện và chặn các mã độc từ plug-in; đồng thời cập nhật định kỳ các phần mềm an ninh để bảo vệ khỏi các mối đe dọa mới.

và cài đặt của chúng. - Không sử dụng các phần mềm bảo mật, hoặc không bảo mật hệ thống mạng, máy tính, thiết bị của mình. **Tổn thất:** - Người dùng có thể bị đánh cắp hoặc tiết lộ thông tin cá nhân, tài khoản, mật khẩu, dữ liệu nhạy cảm, bản quyền, tài chính, bị đòi tiền chuộc. - Bị thay đổi, xóa, hỏng, hoặc mất dữ liệu quan trọng. - Bị lợi dụng tài nguyên máy tính hoặc hệ thống mạng để thực hiện các hành vi phạm pháp khác. - Bị ảnh hưởng đến hoạt động kinh doanh, uy tín, khả năng cạnh tranh, và mối quan hệ với khách hàng, đối tác, nhà cung cấp.	- *Quản lý và theo dõi các cập nhật:* Đảm bảo rằng tất cả các plug-in được cài đặt đều được cập nhật định kỳ với các phiên bản an toàn nhất cũng như thực hiện quá trình giám sát và theo dõi các thông báo cập nhật của nhà sản xuất plug-in, loại bỏ những plug-in không cần thiết hoặc có nguy cơ bảo mật. - *Giới hạn quyền truy cập của plug-in:* Hạn chế quyền truy cập của plug-in để giảm thiểu rủi ro nếu nó bị lợi dụng; thực hiện theo dõi và xác minh các yêu cầu quyền truy cập từ plug-in để phát hiện các hành vi bất thường. - *Sử dụng công cụ giám sát và phát hiện xâm nhập (IDS/IPS):* Triển khai các công cụ giám sát và phát hiện xâm nhập để theo dõi hoạt động của mạng và phát hiện các hoạt động bất thường. Việc thiết lập các quy tắc lọc lưu lượng mạng để ngắn chặn truy cập đến các trang web có nguy cơ hoặc lưu lượng từ các plug-in không an toàn cũng vô cùng quan trọng và hữu hiệu trong việc phòng tránh mã độc.
Về phía doanh nghiệp: Các nguy cơ mất an toàn thông tin từ phía doanh nghiệp là những yếu tố có thể gây ra sự cố, rủi ro, thiệt hại cho hệ thống thông tin của doanh nghiệp, cũng như cho các đối tác, khách hàng, nhân viên và bên thứ ba liên quan.	
Nguy cơ và tổn thất	**Cách phòng tránh**
1. Gian lận thanh toán: Là hình thức mà kẻ gian hoặc hacker lợi dụng lỗi của hệ thống thanh toán để thực hiện những giao dịch ảo dẫn tới thất thoát lớn cho doanh	- *Đào tạo và nâng cao nhận thức an ninh cho nhân viên:* Đào tạo nhân viên về các biện pháp an ninh thông tin, nhận diện các dấu hiệu của gian lận thanh toán và hướng

nghiệp. **Nguyên nhân:** - Sự phát triển của công nghệ thanh toán, tạo ra nhiều lỗ hổng bảo mật và cơ hội cho kẻ gian. - Sự thiếu nhận thức, kỹ năng, thói quen bảo vệ thông tin của người dùng. - Sự thiếu kiểm soát, giám sát, phát hiện, ngăn chặn gian lận của các tổ chức thanh toán. - Sự tham lam, độc ác, tinh vi, sáng tạo của kẻ gian. **Tổn thất:** - Tổn thất về tài chính: Các doanh nghiệp có thể bị mất doanh thu, bị bồi thường thiệt hại, bị phạt tiền, bị đòi tiền chuộc. - Tổn thất về uy tín, danh tiếng: Các doanh nghiệp có thể bị mất khách hàng, bị mất tin cậy, bị bôi nhọ, bị đe dọa, tống tiền. - Chi phí pháp lý và điều tra: Doanh nghiệp có thể phải chi trả chi phí đáng kể cho việc điều tra gian lận và các thủ tục pháp lý liên quan. - Gián đoạn hoạt động kinh doanh: Gian lận có thể gây ra sự gián đoạn trong hoạt động kinh doanh hàng ngày và quy trình thanh toán. - Mất niềm tin của khách hàng: Khách hàng có thể mất niềm tin vào khả năng bảo mật của doanh nghiệp, dẫn đến việc giảm sự trung thành và doanh số.	dẫn cách xử lý khi phát hiện. - *Xây dựng hệ thống theo dõi và sử dụng công nghệ phát hiện gian lận (Fraud detection technology):* Doanh nghiệp cần có hệ thống giám sát và phát hiện gian lận để theo dõi các giao dịch, phát hiện các hoạt động bất thường và cảnh báo kịp thời. - *Sử dụng hệ thống thanh toán an toàn:* Sử dụng các cổng thanh toán an toàn, có mã hóa dữ liệu và tuân thủ các tiêu chuẩn bảo mật như PCI-DSS (Payment Card Industry Data Security Standard) để đảm bảo thông tin thanh toán được bảo vệ. - *Thực hiện kiểm tra bên thứ ba:* Đối với các bên thứ ba có liên quan đến quy trình thanh toán, doanh nghiệp nên thực hiện kiểm tra để đảm bảo rằng họ tuân thủ các tiêu chuẩn an toàn thông tin. - *Theo dõi các xu hướng và phát triển mới:* Theo dõi các xu hướng mới trong gian lận thanh toán, đồng thời từ đó có cái nhìn tổng quan để đưa ra giải pháp hiệu quả nhất, giúp tối thiểu hóa việc gian lận trong thanh toán. - *Xác thực hai yếu tố (Two-factor authentication):* Yêu cầu người dùng cung cấp hai thông tin xác thực khác nhau để truy cập vào hệ thống thanh toán nhằm tăng cường được tính bảo mật và giảm nguy cơ về việc truy cập trái phép. - *Kiểm tra định kỳ và kiểm soát quy trình*

- Tăng chi phí bảo mật: Doanh nghiệp có thể phải đầu tư thêm vào hệ thống an ninh mạng và các biện pháp phòng chống gian lận để ngăn chặn các sự cố tương tự trong tương lai. - Ảnh hưởng đến cổ đông và giá cổ phiếu: Cổ đông có thể mất niềm tin vào quản lý doanh nghiệp, và giá cổ phiếu có thể giảm sút do những lo ngại về rủi ro tài chính và quản trị.	*thanh toán:* Thiết lập các quy trình kiểm tra nội bộ để phát hiện các hoạt động không bình thường trong hệ thống thanh toán, như việc theo dõi giao dịch, kiểm tra số tiền, người nhận thanh toán, và mẫu giao dịch. - *Tuân thủ các tiêu chuẩn bảo mật:* Đảm bảo rằng hệ thống thanh toán tuân thủ các tiêu chuẩn bảo mật quốc tế như PCI DSS (Payment Card Industry Data Security Standard) hoặc các tiêu chuẩn bảo mật khác cũng là cách hạn chế được tình trạng gian lận thanh toán. - *Thúc đẩy văn hóa công ty trung thực và minh bạch*
2. Rủi ro về dữ liệu **Nguyên nhân:** - Thiếu bảo mật: Doanh nghiệp không có các biện pháp bảo mật cơ bản, như mật khẩu, mã hóa, tường lửa, phần mềm bảo mật, cập nhật phần mềm, v.v. để ngăn chặn các cuộc tấn công từ bên ngoài hoặc bên trong nội bộ. - Thiếu nhận thức: Doanh nghiệp không có đủ kiến thức và kỹ năng về an ninh mạng, cũng như không quan tâm đến việc bảo vệ dữ liệu của mình. Họ có thể không thay đổi mật khẩu thường xuyên, không kiểm tra nguồn gốc của các dữ liệu, không cẩn thận khi sử dụng các dịch vụ thương mại điện tử. - Thiếu quản lý: Doanh nghiệp không có	- *Sao lưu và lưu trữ dữ liệu:* Thực hiện sao lưu dữ liệu quan trọng, và lưu trữ ở nhiều nơi khác nhau, như ổ cứng ngoài, đĩa CD, USB, hoặc đám mây dữ liệu định kỳ là một biện pháp quan trọng để đảm bảo rằng có thể khôi phục lại dữ liệu nếu xảy ra sự cố. - *Thiết lập chính sách bảo mật dữ liệu:* Đây được xem là bước đầu tiên quan cũng như quan trong nhất trong việc hạn chế và phòng tránh các rủi ro. Bởi lẽ, doanh nghiệp cần phát triển và thi hành các chính sách bảo mật dữ liệu rõ ràng, trong đó quy định các biện pháp an ninh mạng cần thiết, cũng như quy định về việc sử dụng và truy cập vào dữ liệu. - *Bảo vệ dữ liệu và đường truyền dữ liệu:*

một chính sách và quy trình quản lý dữ liệu một cách hiệu quả, nhất là khi số lượng và loại dữ liệu ngày càng tăng. Họ có thể không kiểm tra và đánh giá chất lượng dữ liệu, không phát hiện và xử lý kịp thời các sự cố, không có kế hoạch phòng ngừa và khắc phục hậu quả. **Tổn thất:** - Gây thiệt hại cho dữ liệu của doanh nghiệp, như bị đánh cắp, rò rỉ, thay đổi, xóa, hỏng, hoặc mất. - Ảnh hưởng đến hoạt động kinh doanh, uy tín, khả năng cạnh tranh, và mối quan hệ với khách hàng, đối tác, nhà cung cấp, v.v. của doanh nghiệp. - Dữ liệu bị rò rỉ có thể gây ra thất thoát tài sản trí tuệ. Việc này có thể do một nhân viên không tốt của một công ty sao chép và mang đi các dữ liệu quan trọng hoặc tài sản trí tuệ của doanh nghiệp mà không được phép.	Sử dụng mã hóa (encryption) để bảo vệ dữ liệu trên đường truyền, đặc biệt là khi dữ liệu được truyền qua mạng Internet hoặc các kết nối không an toàn. Doanh nghiệp cần có các biện pháp bảo mật dữ liệu hiệu quả, bao gồm mã hóa, kiểm soát truy cập, và cơ chế xác thực mạnh mẽ. - *Cập nhật hệ thống an toàn thông tin:* Đảm bảo rằng tất cả các phần mềm và hệ điều hành đều được cập nhật với các bản vá bảo mật mới nhất để ngăn chặn các lỗ hổng bảo mật. - *Sử dụng các giải pháp bảo mật chuyên sâu:* Doanh nghiệp nên xem xét việc sử dụng các giải pháp bảo mật chuyên sâu như tường lửa, phần mềm chống virus, phát hiện xâm nhập, và các công nghệ bảo mật tiên tiến khác. - *Tuân thủ các quy định pháp lý:* Việc thực hiện tuân thủ các quy định pháp lý về bảo vệ dữ liệu, như GDPR (Nghị định về bảo vệ dữ liệu chung của Liên minh châu Âu) hoặc các quy định bảo mật dữ liệu khác áp dụng tại khu vực hoạt động của doanh nghiệp cũng là một biện pháp quan trong giúp tối thiểu hóa được rủi ro về dữ liệu.
3. Rủi ro về công nghệ **Nguyên nhân:** - Lỗi phần cứng và phần mềm: Đây có thể gây mất dữ liệu và gián đoạn hoạt động của hệ thống.	- *Hợp tác với các chuyên gia bảo mật:* Hợp tác với các chuyên gia bảo mật hoặc tổ chức bảo mật để có được sự tư vấn và hỗ trợ trong việc phòng tránh và ứng phó với các rủi ro công nghệ.

- Tấn công mạng: Các sự kiện như VnDirect bị tấn công mạng cho thấy năng lực phòng thủ kém của doanh nghiệp và dự báo tấn công mạng sẽ tiếp tục gia tăng. - Thiếu hụt ngân sách: Điều này khiến các CISOs phải đấu tranh để thu hẹp khoảng cách giữa nhu cầu thực tế và kinh phí cần thiết cho việc đảm bảo an toàn thông tin. **Tổn thất:** - Các rủi ro này có thể ảnh hưởng đến hoạt động kinh doanh, uy tín, khả năng cạnh tranh, và mối quan hệ với khách hàng, đối tác, nhà cung cấp, v.v. của doanh nghiệp. - Tổn thất về thời gian, công sức: Doanh nghiệp có thể bị mất nhiều thời gian, công sức để khắc phục các sự cố, phục hồi dữ liệu, sửa chữa máy móc, bồi thường thiệt hại, giải quyết các vấn đề pháp lý.	- *Thực hiện biện pháp bảo mật cơ bản:* Đảm bảo rằng các biện pháp bảo mật cơ bản được triển khai, bao gồm cài đặt và cập nhật phần mềm bảo mật, sử dụng mật khẩu mạnh, mã hóa dữ liệu quan trọng, và thiết lập các quy trình kiểm soát truy cập. - *Tạo lập chính sách bảo mật:* Xây dựng và thực hiện chính sách bảo mật mạng cho doanh nghiệp, như các quy định về việc sử dụng internet và thiết bị công nghệ thông tin, quản lý dữ liệu nhạy cảm, và các biện pháp phòng chống tấn công mạng cũng giúp hạn chế được các rủi ro không đáng có về phía công nghệ. - *Hợp tác và chia sẻ thông tin:* Doanh nghiệp có thể tham gia các cộng đồng an ninh mạng và công nghệ để chia sẻ thông tin về các mối đe dọa cũng như các biện pháp phòng ngừa với các doanh nghiệp và tổ chức khác.
4. Rủi ro về tin tặc **Nguyên nhân:** - Truy cập không an toàn: Sử dụng mạng di động hoặc wifi công cộng không an toàn có thể làm tăng nguy cơ bị tấn công. - Phần mềm độc hại: Việc cài đặt vô tình các phần mềm độc hại có thể mở cửa cho tin tặc xâm nhập vào hệ thống. - Tấn công từ chối dịch vụ (DoS và DDoS): Các cuộc tấn công này nhằm làm quá tải hệ thống, khiến cho dịch vụ không thể truy cập được.	- *Sử dụng HTTPS và chứng chỉ SSL:* Doanh nghiệp cũng nên chú trọng vào việc sử dụng HTTPS và chứng chỉ SSL để giúp mã hóa dữ liệu truyền giữa người dùng và website, làm giảm khả năng bị tin tặc đánh cắp thông tin. - *Chống xâm nhập, tấn công từ dịch vụ DDOS:* Việc cài đặt các hệ thống phòng thủ để ngăn chặn các cuộc tấn công từ chối dịch vụ phân tán là một biện pháp mà doanh nghiệp có thể sử dụng nhằm hạn chế được những rủi ro về tin tặc.

- Thiếu hiểu biết về an ninh mạng: Nhiều doanh nghiệp không nhận thức đầy đủ về mức độ nguy hiểm của các cuộc tấn công mạng và không đầu tư đủ vào biện pháp bảo mật. **Tổn thất:** - Tổn thất về tài chính: Doanh nghiệp có thể bị mất tiền, bị lừa đảo, bị chiếm đoạt tài sản, bị đòi tiền chuộc. Doanh nghiệp phải chi trả phí phạt pháp lý và chi phí để phục hồi hệ thống và dữ liệu sau một cuộc tấn công mạng có thể làm suy giảm lợi nhuận của doanh nghiệp và gây ra tổn thất về tài chính. - Các rủi ro này có thể ảnh hưởng đến hoạt động kinh doanh, uy tín, khả năng cạnh tranh, và mối quan hệ với khách hàng, đối tác, nhà cung cấp của doanh nghiệp.	- *Bảo mật website và máy chủ:* Doanh nghiệp cũng nên nghiêm ngặt trong việc thực hiện các biện pháp bảo mật để ngăn chặn các lỗ hổng có thể bị khai thác. - *Áp dụng các phương pháp bảo mật khác:* Bên cạnh những biện pháp nên trên, các biện pháp bảo mật khác cũng nên được áp dụng như rà quét website thường xuyên để phát hiện mã độc, sao lưu dữ liệu, và sử dụng các phần mềm, tính năng bảo mật website,…cũng giúp ích trong công cuộc bảo vệ hệ thống mạng doanh nghiệp khỏi những rủi ro về tin tặc.

VD:

- Năm 2021, một vụ tấn công mạng đã làm cho hệ thống máy tính của Công ty TNHH Sản xuất Thép Hòa Phát bị tê liệt, gây ra thiệt hại ước tính khoảng 400 tỷ đồng. Doanh nghiệp đã bị mất doanh thu, bị giảm năng suất, bị ảnh hưởng đến uy tín, danh tiếng và phải bồi thường cho các đối tác, khách hàng.
- Năm 2022, một vụ tấn công mạng bằng ransomware đã gây ra sự cố cho hệ thống y tế của Việt Nam, khiến hàng nghìn bệnh nhân không thể khám chữa bệnh, lấy kết quả xét nghiệm, đặt lịch hẹn. Nhiều người dùng đã bị ảnh hưởng đến sức khỏe, an toàn và phải mất nhiều thời gian, công sức để giải quyết các vấn đề phát sinh.
- Năm 2023, một vụ đánh cắp dữ liệu lớn xảy ra tại Công ty TNHH Thương mại điện tử Lazada, khiến hơn 1,1 triệu tài khoản người dùng bị lộ thông tin cá nhân, thẻ tín dụng và lịch sử mua hàng. Nhiều người dùng đã bị mất tiền, bị lừa đảo, bị xâm phạm quyền riêng tư và bị ảnh hưởng đến uy tín, danh tiếng.

IV. XU HƯỚNG CÔNG NGHỆ

Vào năm 2024, các tác nhân đe dọa mạng chủ yếu tập trung vào các cuộc tấn công tinh vi đã chứng tỏ tỷ lệ thành công và lợi tức đầu tư (ROI) cao trong quá khứ. Và các xu hướng an ninh mạng hàng đầu thường được lấy cảm hứng từ sự kết hợp của các phản ứng đối với các mối đe dọa mạng hàng đầu, công nghệ mới và các mục tiêu bảo mật dài hạn. Dưới đây là một số xu hướng và công nghệ bảo mật hàng đầu xác định không gian an ninh mạng vào năm 2024. (Theo Check Point)

4.1. Trung tâm dữ liệu lai (Hybrid Data Center)

Trung tâm dữ liệu lai là môi trường CNTT tiên tiến kết hợp các trung tâm dữ liệu tại chỗ (on-premises/on-prem) truyền thống với các ứng dụng dựa trên đám mây (cloud-based).

Kiến trúc này giúp cho doanh nghiệp tận dụng tối đa cả 2 lợi ích: tính bảo mật và khả năng kiểm soát của trung tâm dữ liệu riêng (private data center) với tính hiệu quả về chi phí, khả năng mở rộng và tính linh hoạt của các dịch vụ đám mây. Có thể thấy rõ rằng việc kết hợp trung tâm dữ liệu truyền thống (on-premises) và điện toán đám mây (cloud) mang lại nhiều lợi ích cho người dùng và doanh nghiệp trong việc bảo mật an toàn thông tin:

- *Tối ưu hóa hiệu suất và mở rộng linh hoạt:* Hybrid Data Center sử dụng khả năng điều phối để dữ liệu và ứng dụng có thể được di chuyển giữa cơ sở hạ tầng tại chỗ và cơ sở hạ tầng dựa trên đám mây qua mạng khi cần. Nó cho phép các tổ chức điều chỉnh môi trường lưu trữ dữ liệu cho phù hợp theo nhu cầu cơ sở hạ tầng và bảo mật của họ. Ví dụ: dữ liệu và ứng dụng nhạy cảm, quan trọng hơn có thể được lưu trữ trên on-prem để giữ an toàn, trong khi đó có thể mở rộng không gian lưu trữ bằng cloud để lưu những dữ liệu không nhạy cảm, không yêu cầu hiệu suất cao => tiện lợi truy cập từ bất kỳ đâu. Việc sử dụng cơ sở hạ tầng điều phối và kết nối cho phép các tài nguyên này di chuyển liền mạch giữa hai tài nguyên khi cần thiết.

- *Tăng cường bảo mật dữ liệu:* Với các vi phạm dữ liệu ngày càng gia tăng, bảo mật là mối quan tâm hàng đầu của các doanh nghiệp. Các trung tâm dữ liệu lai cung cấp một khung bảo mật kết hợp các cơ chế bảo mật như: mã hóa dữ liệu, khả năng kiểm soát truy cập nghiêm ngặt và khả năng hiển thị của on-prem với các tính năng bảo mật nâng cao được cung cấp bởi các nhà cung cấp dịch vụ đám mây. Điều này giúp người dùng và

doanh nghiệp bảo vệ dữ liệu quan trọng của họ khỏi bị đánh cắp, sửa đổi hoặc tiết lộ không mong muốn.

- *Khả năng sao lưu và phục hồi dữ liệu hiệu quả:* Hybrid data center kết hợp các giải pháp sao lưu và phục hồi dữ liệu tự động (Ví dụ, on-prem có thể được sử dụng để lưu trữ các bản sao dự phòng của dữ liệu quan trọng và nhạy cảm. Trong khi đó, dịch vụ Cloud cung cấp khả năng sao lưu và khôi phục dữ liệu nhanh chóng và dễ dàng). Điều này cho phép người dùng và doanh nghiệp khôi phục nhanh chóng dữ liệu sau các sự cố như mất dữ liệu hoặc tấn công malware.

4.2. Sử dụng AI trong các cuộc tấn công mạng

Generative AI đã nhanh chóng cất cánh vào năm 2024. Mặc dù công nghệ này lần đầu tiên đi vào ý thức cộng đồng vào cuối năm 2022 với sự trỗi dậy của ChatGPT, nhưng nhiều lựa chọn thay thế đã xuất hiện kể từ đó.

Sự trỗi dậy của AI có tác động đáng kể đến an ninh mạng cả từ góc độ tấn công và phòng thủ. Về mặt tấn công, ChatGPT và các công cụ tương tự đã được các tác nhân đe dọa mạng sử dụng để hợp lý hóa và cải thiện các cuộc tấn công mạng với sự gia tăng các cuộc tấn công trên diện rộng hàng năm. Về mặt phòng thủ, AI có nhiều ưu điểm về mặt bảo mật và vai trò của nó sẽ tiếp tục phát triển trong tương lai.

Một số lợi ích của AI đối với bảo mật bao gồm:

- *Tự động hóa các nhiệm vụ lặp đi lặp lại:* An ninh mạng đòi hỏi rất nhiều thu thập dữ liệu, phân tích, quản lý hệ thống và các nhiệm vụ lặp đi lặp lại khác tiêu tốn thời gian và nguồn lực của các nhà phân tích. AI có tiềm năng tự động hóa các hoạt động này, cho phép nhân viên an ninh tập trung nỗ lực của họ vào nơi cần thiết nhất.

- *Cải thiện khả năng phát hiện và ứng phó với mối đe dọa:* AI phù hợp lý tưởng để thu thập lượng dữ liệu khổng lồ, phân tích và phản hồi dựa trên những hiểu biết được trích xuất. Những khả năng này có thể tăng cường khả năng phát hiện và phản ứng mối đe dọa của tổ chức bằng cách tăng tốc và mở rộng quy mô phát hiện và ứng phó với các cuộc tấn công mạng, giảm thiệt hại mà kẻ tấn công có thể gây ra cho tổ chức.

- *Nâng cao nhận thức tình huống và ra quyết định:* Thông thường, nhân viên bảo mật bị quá tải dữ liệu với nhiều thông tin hơn mức họ có thể xử lý và sử dụng hiệu quả. AI vượt trội trong việc thu thập và xử lý dữ liệu, và những hiểu biết mà nó cung cấp có thể cải

thiện nhận thức tình huống của nhân viên bảo mật và khả năng đưa ra quyết định dựa trên dữ liệu.

AI có nhiều ứng dụng tiềm năng trong bảo mật. Một số trường hợp sử dụng ví dụ bao gồm:

- Bảo mật điểm cuối: Các giải pháp AI có thể phân tích hành vi của người dùng và ứng dụng để tìm các chỉ số về tài khoản bị xâm phạm hoặc phần mềm độc hại trên hệ thống được bảo vệ.

- An ninh mạng: Các hệ thống AI có thể phân tích lưu lượng mạng cho các gói hoặc xu hướng có thể chỉ ra các loại tấn công khác nhau.

- Bảo mật đám mây: Các giải pháp AI có thể giúp giải quyết các thách thức phổ biến trong bảo mật đám mây, chẳng hạn như đảm bảo rằng các quyền trên đám mây, kiểm soát truy cập và cài đặt bảo mật được định cấu hình đúng.

- Phát hiện gian lận: Các hệ thống AI có thể phân tích hành vi của người dùng để tìm sự bất thường hoặc các hành động độc hại có thể chỉ ra gian lận tiềm ẩn.

Có thể thấy rằng, AI là một công cụ đầy hứa hẹn về bảo mật. Nó phù hợp lý tưởng để giải quyết nhiều thách thức chính mà các nhóm bảo mật phải đối mặt, bao gồm khối lượng dữ liệu lớn, tài nguyên hạn chế và nhu cầu phản ứng nhanh với các cuộc tấn công mạng.

Mặc dù AI có tiềm năng lớn trong lĩnh vực phòng thủ, nhưng sự trưởng thành ngày càng tăng của nó tạo ra một cuộc chạy đua giữa kẻ tấn công và người bảo vệ.

4.3. Tường lửa lưới lai (Hybrid Mesh Firewall)

Các hệ thống mạng ngày nay là những môi trường kết hợp phức tạp trải rộng trên nhiều biên, khiến hầu hết các tổ chức chuyển sang phương pháp tiếp cận mạng an toàn hội tụ bảo mật và kết nối. Một trong những thành tố mới, đáng lưu tâm của mạng an toàn là tường lửa thế hệ mới Hybrid Mesh Firewall.

Tường lửa dạng lưới lai (Hybrid Mesh Firewall) được thiết kế để thống nhất hệ thống bảo mật tường lửa của doanh nghiệp. Đồng thời, các tường lửa này được giám sát và quản lý tập trung thông qua một trình quản lý duy nhất được triển khai trên đám mây. Sự kết hợp này cho phép các tổ chức bảo mật toàn bộ cơ sở hạ tầng CNTT của mình trong khi vẫn duy trì khả năng hiển thị và kiểm soát toàn diện.

Với tường lửa lưới lai, doanh nghiệp có thể bảo vệ hệ thống mạng tổng, cơ sở hạ tầng đám mây công cộng và riêng tư, những nhân viên làm việc từ xa và các công ty chi nhánh.

Tường lửa dạng lưới kết hợp sử dụng một loạt tường lửa đa dạng và chúng được bảo trợ bởi hệ thống quản lý tập trung, dựa trên đám mây. Bằng cách đó, nó mang lại nhiều lợi ích khác nhau cho tổ chức, bao gồm:

- *Khả năng hiển thị toàn diện:* Tường lửa dạng lưới lai cho phép nhân viên an ninh vận hành một mạng lưới các tường lửa từ một bảng điều khiển duy nhất. Điều này cung cấp khả năng hiển thị toàn diện về lưu lượng CNTT của công ty mà không có lỗ hổng do các giải pháp bảo mật riêng lẻ tạo ra.

- *Bảo mật nhất quán:* Việc quản lý bảo mật tập trung của kiến trúc tường lửa cũng giúp doanh nghiệp dễ dàng thực thi các chính sách bảo mật nhất quán trên toàn bộ doanh nghiệp. Cấu hình tường lửa được quản lý tập trung, cho phép nhân viên an ninh dễ dàng giám giám sát và đưa ra các bản cập nhật cho toàn bộ hệ thống.

- *Giảm độ phức tạp:* Việc quản lý một loạt các tường lửa có thể phức tạp, dẫn đến bảo mật kém hơn. Tường lửa dạng lưới lai là một giải pháp duy nhất có phạm vi phân tán, giúp quản lý dễ dàng và hiệu quả hơn.

- *Bảo mật nâng cao:* Tường lửa dạng lưới lai cho phép các công ty triển khai khả năng bảo mật tường lửa cấp doanh nghiệp trên toàn bộ hệ thống của họ. Điều này làm giảm nguy cơ lỗ hổng bảo mật,…

- *Tự động hóa và AI:* Các giải pháp tường lửa lưới lai thường kết hợp tự động hóa cùng với AI và ML (machine learning) để xác định và ứng phó với các mối đe dọa tiềm ẩn. Điều này làm tăng khả năng mở rộng nỗ lực của nhóm bảo mật và cho phép họ phản ứng nhanh chóng và hiệu quả hơn trước các mối đe dọa bảo mật tiềm ẩn.

4.4. Nền tảng bảo vệ ứng dụng gốc đám mây (Cloud-native application protection platform - CNAPP)

CNAPP là thuật ngữ do Gartner đặt ra nhằm mô tả một nền tảng toàn diện giúp hợp nhất các chức năng bảo mật và tuân thủ để ngăn chặn, phát hiện và ứng phó với các mối đe dọa bảo mật đám mây. CNAPP tích hợp nhiều giải pháp bảo mật đám mây vốn nằm

riêng rẽ vào một giao diện người dùng duy nhất, giúp các tổ chức bảo vệ toàn bộ phạm vi hiện diện của ứng dụng đám mây dễ dàng hơn.

Một trong các mục tiêu chính của CNAPP là đưa bảo mật vào các giai đoạn sớm nhất của quy trình phát triển ứng dụng. Đám mây cho phép các tổ chức đổi mới và mở rộng quy mô ứng dụng, nhưng song hành với khả năng mở rộng ưu việt đó là những phương thức mới mà tội phạm mạng có thể sử dụng để tấn công. Do đó, các nhà phát triển và chuyên gia bảo mật cần phát hiện và khắc phục các lỗi bảo mật càng sớm càng tốt trong quá trình phát triển ứng dụng. Đây là xu hướng "kiểm thử sớm" để ngăn chặn các lỗ hổng bảo mật lớn hơn trong tương lai.

Dưới đây là các cấu phần giúp CNAPP hoạt động liền mạch:

- *Quản lý vị thế bảo mật trên đám mây (CSPM):* Các giải pháp CSPM được thiết kế để cung cấp cho nhóm bảo mật dạng xem có phân loại và kết nối về các lỗ hổng và cấu hình sai tiềm ẩn trên các môi trường đa đám mây và môi trường kết hợp. CSPM liên tục đánh giá vị thế bảo mật tổng thể của bạn và cung cấp cho nhóm bảo mật cảnh báo cũng như đề xuất tự động về các vấn đề quan trọng có thể khiến tổ chức của bạn gặp phải vi phạm về dữ liệu. Giải pháp này có các công cụ quản lý tuân thủ và khắc phục tự động để phát hiện lỗ hổng và xử lý các lỗ hổng đó.

- *Nền tảng bảo vệ khối lượng công việc trên đám mây (CWPP):* CWPP cung cấp tính năng phát hiện và ứng phó theo thời gian thực với các mối đe dọa, dựa trên thông tin mới nhất trên mọi khối lượng công việc đa đám mây của bạn, chẳng hạn như máy ảo, bộ chứa, Kubernetes, cơ sở dữ liệu, tài khoản lưu trữ, lớp mạng và dịch vụ ứng dụng. CWPP giúp các nhóm bảo mật điều tra nhanh chóng các mối đe dọa và giảm bề mặt tấn công cho tổ chức của họ.

- *Bảo mật mạng dịch vụ đám mây (CSNS):* Các giải pháp CSNS bổ sung sức mạnh cho CWPP bằng cách bảo vệ hạ tầng đám mây trong thời gian thực. Giải pháp CSNS có thể bao gồm nhiều công cụ bảo mật đa dạng như tường lửa ứng dụng web, khả năng chống từ chối dịch vụ phân tán, kiểm tra bảo mật tầng giao vận và cân bằng tải.

- *Bảo mật DevOps cho nhiều quy trình:* Quản lý bảo mật DevOps cung cấp cho các nhà phát triển và nhóm bảo mật một bảng điều khiển trung tâm để quản lý bảo mật DevOps trong mọi quy trình. Nhờ vậy, khả năng giảm thiểu cấu hình sai trên đám mây và quét mã

mới để ngăn chặn các lỗ hổng xuất hiện trong môi trường sản xuất cũng tăng lên. Các công cụ quét hạ tầng dưới dạng mã sẽ xem xét tệp cấu hình của bạn từ những giai đoạn phát triển sớm nhất để xác nhận rằng các tệp cấu hình mới tuân thủ các chính sách bảo mật của bạn.

- *Quản lý quyền sử dụng hạ tầng đám mây (CIEM):* CIEM tập trung quản lý quyền trên toàn bộ phạm vi hiện diện trên đám mây và kết hợp của bạn, giúp ngăn chặn việc sử dụng sai quyền do vô tình hoặc với dụng ý xấu. Giải pháp này giúp các nhóm bảo mật chống rò rỉ dữ liệu và thực thi nguyên tắc đặc quyền thấp nhất trên toàn bộ hệ thống.

Bằng cách kết hợp nhiều công cụ bảo mật ứng dụng đám mây vào một nền tảng chuyên dụng, CNAPP giúp việc đưa bảo mật vào vòng đời ứng dụng trở nên đơn giản hơn, trong khi vẫn cung cấp khả năng bảo vệ vượt trội cho khối lượng công việc và dữ liệu trên đám mây.

Cụ thể, sau đây là một số lợi ích của CNAPP trong việc bảo mật an toàn thông tin:

- *Bảo vệ toàn diện cho khối lượng công việc trên đám mây:* Cải thiện khả năng quan sát tất cả khối lượng công việc của bạn để phát hiện các lỗ hổng và cấu hình sai dễ dàng hơn.

- *Hỗ trợ đa đám mây:* Hợp nhất bảo mật và tuân thủ một cách liền mạch trên nhiều môi trường hạ tầng đám mây công cộng và riêng tư, mang đến cho bạn khả năng quan sát toàn diện tài sản dữ liệu đa đám mây của mình.

- *Cải thiện khả năng hiển thị:* Có nhiều công cụ quét, giám sát và quan sát bảo mật dành cho khối lượng công việc trên nền tảng đám mây. Tuy nhiên, điều khiến CNAPP trở nên khác biệt là khả năng ngữ cảnh hóa thông tin và có khả năng hiển thị từ đầu đến cuối trên cơ sở hạ tầng ứng dụng của doanh nghiệp. Ví dụ: với khả năng hiển thị toàn diện và chi tiết chi tiết về cấu hình, ngăn xếp công nghệ và danh tính, giải pháp CNAPP có thể ưu tiên cảnh báo những nguy cơ rủi ro cao nhất cho doanh nghiệp.

- *Tích hợp thông tin về mối đe dọa:* Tập trung trước tiên vào các lỗ hổng nghiêm trọng nhất nhờ dạng xem tích hợp, có phân loại ưu tiên về các mối đe dọa và giảm rủi ro bằng các công cụ đề xuất và khắc phục tự động.

- *Kiểm soát chặt chẽ hơn:* CNAPP cho phép doanh nghiệp chủ động quét, phát hiện và nhanh chóng khắc phục các rủi ro về bảo mật và tuân thủ do cấu hình sai.

- *Quản lý bảo mật DevOps được "kiểm thử sớm":* Cho phép các nhóm bảo mật cộng tác với nhà phát triển trên một nền tảng có quy trình làm việc, dữ liệu và thông tin chuyên sâu chung để họ có thể đưa bảo mật vào mã ứng dụng ngay khi mã đó được tạo.

4.5. Quản lý tiếp xúc với mối đe dọa (Threat Exposure Management)

Khối lượng, mức độ phức tạp và tốc độ ngày càng tăng của các cuộc tấn công mạng đặt ra thách thức lớn đối với việc đảm bảo an ninh mạng. Để bảo vệ hệ thống mạng khỏi các mối đe dọa mạng đang ngày càng tăng, các tổ chức cần chủ động đánh giá và quản lý mức độ rủi ro của mình.

Quản lý tiếp xúc với mối đe dọa (TEM) là một cách tiếp cận tập trung vào việc đánh giá rủi ro để lập kế hoạch bảo mật. Các nhóm bảo mật xác định các mối đe dọa tiềm ẩn đối với tổ chức và đánh giá rủi ro mà mỗi mối đe dọa gây ra cho công ty. Dựa trên thông tin này, công ty đưa ra các chiến lược giảm thiểu rủi ro cụ thể cho từng trường hợp.

Với bối cảnh ngày càng phức tạp của tình hình đe dọa mạng và các quy định, việc chấp nhận TEM ngày càng trở nên quan trọng. Bằng cách thực hiện quá trình xác định và đánh giá mối đe dọa này thường xuyên, tổ chức có thể duy trì khả năng phán đoán và ứng phó với các hình thức tấn công mới.

4.6. Bảo vệ toàn diện (Comprehensive Protection)

Môi trường CNTT của doanh nghiệp đã phát triển nhanh chóng và trở nên đa dạng hơn trong những năm gần đây. Sự bùng nổ của các dịch vụ đám mây đã có tác động đáng kể đến môi trường CNTT của công ty và góp phần thúc đẩy sự phát triển của ứng dụng. Hình thức làm việc kết hợp và làm việc từ xa đã mở rộng vai trò của thiết bị di động. Các thiết bị Internet of Things (IoT) đã phát triển tinh vi và phổ biến hơn. Điều này cũng mở đường cho sự trưởng thành và mở rộng của mạng di động 5G.

Kết quả của sự mở rộng này là các công ty phải đối mặt với một loạt các mối đe dọa và vectơ tấn công tiềm năng hơn bao giờ hết. Các tác nhân đe dọa mạng có thể tạo ra các lỗ hổng trong các hệ thống và thiết bị truyền thống, thiết bị di động, hệ thống IoT và cơ sở hạ tầng làm việc từ xa. Với nhiều hệ thống hơn cần giám sát và bảo mật, các nhóm an toàn thông tin có thể dễ bỏ qua một số lỗ hổng, kẻ tấn công có thể lợi dụng điều này để tiếp cận hệ thống của họ.

Kết quả cuối cùng của tất cả sự tăng trưởng và đổi mới công nghệ này là sự mở rộng quy mô bề mặt tấn công mạng của các tổ chức. Do đó, các tổ chức cần xác định các mối đe dọa tấn công tiềm ẩn và đảm bảo rằng họ có các giải pháp sẵn sàng để ứng phó với tất cả các rủi ro này.

4.7. Hợp nhất bảo mật (Security Consolidation)

Việc mở rộng quy mô tấn công mạng và sự xuất hiện ngày càng nhiều của những mối đe dọa mạng đã dẫn đến sự bùng nổ về số lượng các công cụ bảo mật mà các công ty vận hành. Với một loạt các mối đe dọa tiềm ẩn, các công ty cần phải khắc phục các lỗ hổng bảo mật và trong quá khứ, họ thường chọn làm như vậy bằng cách triển khai các sản phẩm bảo mật được thiết kế để giải quyết một vectơ tấn công cụ thể hoặc nâng cao bảo mật trên một nền tảng cụ thể.

Tuy nhiên, thách thức của việc tập trung vào triển khai các sản phẩm bảo mật đặc trưng là tính phức tạp và không linh hoạt. Mỗi công cụ tạo ra các cảnh báo và thông báo, làm tăng thêm sự mệt mỏi khi cảnh báo và khiến nhân viên an ninh khó xác định và khắc phục các mối đe dọa thực sự. Ngoài ra, việc vận hành nhiều giải pháp bảo mật khác nhau làm tăng yêu cầu đào tạo, tạo ra tình hình phải liên tục chuyển dịch giữa các giao diện điều khiển và quản lý, dẫn đến nguy cơ về lỗ hổng bảo mật và làm cho chính sách bảo mật không nhất quán.

Trước những thách thức này, nhiều tổ chức đang thay đổi hướng đi và tập trung vào việc cải thiện bảo mật thông qua hợp nhất bảo mật. Thay vì các giải pháp cục bộ, họ đang tìm kiếm các nền tảng tích hợp cung cấp khả năng bảo mật mà họ cần trong một giải pháp thống nhất. Các nền tảng này cung cấp khả năng tăng cường hiển thị và tăng hiệu quả và hiệu suất phát hiện và ứng phó với mối đe dọa bằng cách giảm các quy trình thủ công cho nhân viên an ninh.

V. CÁC GIẢI PHÁP VÀ XU HƯỚNG CÔNG NGHỆ CHUNG

5.1. Giải pháp chung

- *Nâng cao nhận thức và đào tạo an ninh mạng cho nhân viên:* Cung cấp đào tạo định kỳ về an ninh mạng cho nhân viên, bao gồm cách nhận biết và phản ứng với các mối đe dọa mạng, cũng như quy trình an toàn khi sử dụng email, lướt web và xử lý dữ liệu.

- *Áp dụng các giải pháp bảo mật hiện đại:* Sử dụng các giải pháp bảo mật mạng tiên tiến như Firewall, IDS/IPS, Antivirus, Endpoint Protection, các công nghệ phát hiện và ngăn chặn tấn công APT (Advanced Persistent Threats), và các xu hướng công nghệ 2024 như: Hybrid Data Center, Hybrid Mesh Firewall, Cloud-native application protection platform - CNAPP,…

- *Tăng cường kiểm soát truy cập và xác thực người dùng:* Thực hiện các biện pháp kiểm soát truy cập như MFA (Multi-Factor Authentication), VPN (Virtual Private Network), và quản lý danh sách trắng/danh sách đen để giảm thiểu nguy cơ từ các người dùng không đáng tin cậy.

- *Thực hiện cập nhật phần mềm và vá lỗ hổng định kỳ:* Đảm bảo rằng tất cả các hệ thống và phần mềm đều được cập nhật đầy đủ và kịp thời để giảm thiểu nguy cơ từ các lỗ hổng bảo mật đã biết.

- *Quản lý rủi ro và tuân thủ chuẩn bảo mật:* Thực hiện các đánh giá rủi ro thường xuyên để xác định và ưu tiên các mối đe dọa tiềm ẩn, và đảm bảo tuân thủ các chuẩn bảo mật như ISO 27001 hoặc NIST.

- *Sử dụng giải pháp phòng chống tấn công phishing:* Triển khai các giải pháp như email filtering, web filtering, và giáo dục nhân viên về cách nhận diện và tránh các cuộc tấn công phishing.

- *Giám sát và phản ứng mạnh mẽ:* Xây dựng các hệ thống giám sát mạng để phát hiện sớm các hoạt động đáng ngờ và có kế hoạch phản ứng kịp thời khi có mối đe dọa xuất hiện.

- *Bảo vệ dữ liệu cả trong và ngoài mạng:* Sử dụng mã hóa dữ liệu, sao lưu dữ liệu định kỳ, và triển khai các biện pháp bảo mật vật lý như cửa an toàn và hệ thống giám sát vùng.

- *Tích hợp trí tuệ nhân tạo và máy học:* Sử dụng các công nghệ như AI và machine learning để phát hiện và phản ứng tự động với các mối đe dọa mạng phức tạp một cách nhanh chóng.

- *Hợp tác và chia sẻ thông tin về mối đe dọa:* Tham gia vào các cộng đồng an ninh mạng, chia sẻ thông tin và kinh nghiệm để học hỏi và cùng nhau phòng tránh các mối đe dọa mạng.

5.2. Xu hướng công nghệ chung

- *Sử dụng Blockchain trong bảo mật:* Khai thác công nghệ Blockchain để tăng cường tính toàn vẹn và bảo mật cho dữ liệu quan trọng và giao dịch trong mạng doanh nghiệp.

- *Sử dụng trí tuệ nhân tạo và máy học:* Áp dụng AI và machine learning để phát hiện và phản ứng tự động với các mối đe dọa mạng một cách nhanh chóng và chính xác.

- *Phát triển giải pháp bảo mật đám mây (Cloud Security):* Bảo vệ dữ liệu trong môi trường đám mây và triển khai các giải pháp bảo mật đám mây để ngăn chặn các cuộc tấn công từ bên ngoài doanh nghiệp.

- *Bảo mật IoT (Internet of Things):* Bảo vệ các thiết bị kết nối internet và dữ liệu từ các thiết bị IoT bằng cách triển khai các giải pháp bảo mật IoT.

- *Tích hợp Automation và Orchestration:* Sử dụng các công nghệ tự động hóa để tăng cường khả năng phản ứng và giảm thiểu thời gian phản ứng đối với các mối đe dọa mạng.

KẾT LUẬN

Với bối cảnh hiện nay, an toàn thông tin không chỉ là một vấn đề cơ bản mà còn là trọng tâm quan trọng của mọi doanh nghiệp và tổ chức. Thảo luận về nguy cơ và giải pháp đảm bảo an toàn đối với hệ thống người dùng trong các mạng doanh nghiệp đã đưa ra những nhận thức sâu sắc về tầm quan trọng của việc bảo vệ thông tin và dữ liệu trong môi trường kinh doanh.

Trong bài thảo luận, chúng ta đã thấy rằng nguy cơ đối với an toàn thông tin không ngừng gia tăng do sự phát triển của công nghệ và các mối đe dọa mạng ngày càng phức tạp hơn. Tuy nhiên, thông qua việc áp dụng các biện pháp phòng ngừa và bảo mật phù hợp, chúng ta có thể giảm thiểu rủi ro và đảm bảo rằng hệ thống người dùng trong các mạng doanh nghiệp được bảo vệ một cách hiệu quả.

Tầm quan trọng của an toàn thông tin không thể phủ nhận, vì nó không chỉ ảnh hưởng đến sự tin cậy của doanh nghiệp mà còn đe dọa sự riêng tư và quyền lợi của khách hàng và đối tác kinh doanh. Do đó, việc đầu tư vào an toàn thông tin không chỉ là một nhu cầu mà còn là một trách nhiệm đạo đức. Một hệ thống an toàn thông tin sẽ giúp

doanh nghiệp tránh được những tổn thất lớn, bảo vệ danh tiếng và thúc đẩy sự phát triển bền vững.

Trong tương lai, việc đầu tư vào an toàn thông tin không chỉ là một nhiệm vụ mà còn là một cơ hội để doanh nghiệp nâng cao sức cạnh tranh và duy trì sự bền vững trong thị trường ngày càng cạnh tranh. Cần khuyến khích các doanh nghiệp và cá nhân liên quan nắm vững các nguy cơ và giải pháp an toàn thông tin, thúc đẩy sự nhận thức và đầu tư vào hệ thống bảo mật mạng, và thực hiện các biện pháp phòng ngừa để đảm bảo rằng dữ liệu và thông tin quan trọng luôn được bảo vệ tốt nhất. Chỉ khi có sự hợp tác và nỗ lực chung từ tất cả các bên liên quan, chúng ta mới có thể đảm bảo an toàn cho hệ thống người dùng trong các mạng doanh nghiệp và duy trì sự tin cậy của môi trường kinh doanh trực tuyến. Ngoài ra, cần có sự hợp tác chặt chẽ giữa các bộ phận trong tổ chức, các nhà cung cấp dịch vụ an ninh mạng, và cơ quan chức năng để tạo ra một môi trường an toàn thông tin toàn diện.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Thực trạng an toàn thông tin mạng hiện nay ở Việt Nam và giải pháp phòng chống vi phạm pháp luật trên không gian mạng - Tạp chí Tài chính (tapchitaichinh.vn)

[2] An ninh thương mại điện tử: Các vấn đề, thực trạng và giải pháp (magenest.com)

[3] Mỗi tháng các hệ thống thông tin Việt Nam chịu gần 1.000 cuộc tấn công mạng gây sự cố - Tuổi Trẻ Online (tuoitre.vn)

[4] 88% doanh nghiệp vừa và nhỏ Việt Nam bị tấn công mạng mất thông tin khách hàng | VTV.VN

[5] Internet Việt Nam 2023: Số liệu mới nhất và xu hướng... (vnetwork.vn)

[6] Hybrid Data Center lên ngôi, doanh nghiệp thay đổi cách thức quản lý dữ liệu số - CMC Telecom | Cloud - Data – Internet – Data Center - Voice – VAS

[7] Trung tâm dữ liệu lai: Tương lai của cơ sở hạ tầng thế hệ tiếp theo (infolensa.com)

[8] Top 7 Cyber Security Trends in 2024 - Check Point Software

[9] (Sự khác nhau giữa hai ứng dụng Cloud-Native vs. Cloud-Based | Học trực tuyến CNTT, học lập trình từ cơ bản đến nâng cao (funix.edu.vn)

[10] Xây dựng một hệ sinh thái bảo mật tự phòng vệ (mic.gov.vn)