

BÁO CÁO ĐỒ ÁN
MÔN KIẾN TRÚC AN TOÀN THÔNG TIN

XÂY DỰNG KIẾN TRÚC AN TOÀN CHO HỆ THỐNG MẠNG
DOANH NGHIỆP

Ngành: **AN TOÀN THÔNG TIN**

GVHD: ThS. Nguyễn Minh Thắng

SVTH: Nguyễn Thị Hoài Hiếu

MSSV: 2187700785

Trần Nhật Vũ

MSSV: 2187701120

Nguyễn Phạm Tuyên

MSSV: 2187701116

Lớp: 21DATA1

TP.Hồ Chí Minh, 2024

LỜI CẢM ƠN

Chúng em xin chân thành gửi lời cảm ơn đến Trường Đại Học Công Nghệ TP. Hồ Chí Minh – Hutech, với sự hỗ trợ và cung cấp học phần Kiến trúc an toàn thông tin cho chúng em. Đặc biệt, chúng em muốn bày tỏ lòng biết ơn sâu sắc đến Thầy Nguyễn Minh Thắng - giảng viên bộ môn Kiến trúc an toàn thông tin. Suốt quá trình học tập, thầy đã dành thời gian và công sức để chỉ bảo, truyền đạt những kiến thức quý báu từ giáo trình đến kinh nghiệm cá nhân của mình. Những kiến thức mà thầy chia sẻ không chỉ là bổ ích mà còn là nền tảng quan trọng giúp chúng em vững bước trên con đường tương lai. Chúng em rất biết ơn và trân trọng sự đóng góp của thầy trong việc phát triển kiến thức và kỹ năng của chúng em.

MỤC LỤC

LỜI CẢM ƠN.....	1
CHƯƠNG 1: TỔNG QUAN	4
1.1 TỔNG QUAN VỀ ĐỒ ÁN.....	4
1.2 NHIỆM VỤ ĐỒ ÁN	4
1.3 CẤU TRÚC ĐỒ ÁN.....	4
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	6
2.1 AN TOÀN THÔNG TIN.....	6
<i>2.1.1 Khái niệm</i>	<i>6</i>
<i>2.1.2 Các yếu tố ảnh hưởng đến an toàn thông tin</i>	<i>9</i>
2.2 THỰC TRẠNG AN TOÀN THÔNG TIN TẠI VIỆT NAM.....	13
<i>2.2.1 Thực trạng an toàn thông tin tại các tổ chức doanh nghiệp.....</i>	<i>13</i>
<i>2.2.2 Hoạt động tấn công vào các tổ chức doanh nghiệp.....</i>	<i>16</i>
2.3 CÁC TIÊU CHUẨN CẦN ĐẢM BẢO ĐỂ HỆ THỐNG DOANH NGHIỆP ĐẠT AN TOÀN THÔNG TIN.....	18
<i>2.3.1 Tổng quan tiêu chuẩn.....</i>	<i>18</i>
<i>2.3.2 Cấu trúc của tiêu chuẩn</i>	<i>21</i>
2.4 PHÂN TÍCH ĐỀ NGHỊ VÀ GIẢI PHÁP	23
<i>2.4.1 Phân tích yêu cầu mạng cho doanh nghiệp</i>	<i>23</i>
<i>2.4.2 Giải pháp cho doanh nghiệp</i>	<i>23</i>
CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM.....	25
3.1 CÔNG NGHỆ SỬ DỤNG CHO HỆ THỐNG MẠNG CỦA CÔNG TY	25
3.1 SƠ ĐỒ THIẾT KẾ MẠNG TRONG DOANH NGHIỆP	31
3.2 ĐỊA CHỈ IP CỦA CÁC THIẾT BỊ	31
3.3 CẤU HÌNH CÁC THIẾT BỊ	32
3.4 THỰC HIỆN CHẠY CÁC DỊCH VỤ	48
CHƯƠNG 4: KẾT LUẬN	51

4.1 KẾT LUẬN	51
4.2 GIẢI PHÁP	51
TÀI LIỆU THAM KHẢO	53
VIDEO DEMO	53

CHƯƠNG 1: TỔNG QUAN

1.1 Tổng quan về đồ án

Đồ án sẽ giới thiệu về việc xây dựng một kiến trúc an toàn cho hệ thống mạng doanh nghiệp, đồng thời giải pháp bảo vệ thông tin quan trọng và dữ liệu của doanh nghiệp trước các mối đe dọa mạng. Qua đó, không chỉ đảm bảo an ninh dữ liệu mà còn giúp duy trì sự uy tín, niềm tin của khách hàng và đối tác đối với doanh nghiệp.

Một hệ thống mạng an toàn không chỉ giúp bảo vệ dữ liệu mà còn giúp tổ chức tuân thủ các quy định pháp lý về bảo mật thông tin. Điều này giúp tránh các hậu quả pháp lý tiềm ẩn có thể xảy ra do việc xâm nhập hoặc mất dữ liệu. Đồng thời, hệ thống mạng an toàn cũng giúp doanh nghiệp nắm rõ các tiêu chuẩn cần đảm bảo để hệ thống đạt an toàn thông tin.

1.2 Nhiệm vụ đồ án

Giúp người dùng sử dụng trong những mục đích sau:

- Phân tích rủi ro và giải pháp.
- Các thiết kế mạng an toàn.
- Triển khai công nghệ bảo mật.
- Nâng cấp và duy trì.
- Hiểu về các tiêu chuẩn để đảm bảo cho an toàn thông tin.

1.3 Cấu trúc đồ án

Đồ án gồm có 4 chương:

Chương 1: Tổng quan

Phần này giới thiệu tổng quan, nhiệm vụ của đồ án, giúp chúng ta hiểu nội dung căn bản của đồ án

Chương 2: Cơ sở lý thuyết

Phần này sẽ giới thiệu cụ thể về phân tích đề nghị và giải pháp cho doanh nghiệp, những công nghệ và thiết bị được áp dụng trong doanh nghiệp, những tiêu chuẩn đảm bảo cho an toàn thông tin.

Chương 3: Kết quả thực nghiệm

Phần này sẽ cho chúng ta biết các thiết bị và sơ đồ thiết kế cấu hình mạng trong doanh nghiệp sao cho an toàn.

Chương 4: Kết luận

Phần này tóm tắt nội dung chính của bài báo cáo đồ án này, ngoài ra còn đề xuất các giải pháp và hướng nghiên cứu tiếp theo để nâng cao hiệu quả của kiến trúc an ninh mạng dành cho doanh nghiệp.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1 An toàn thông tin

2.1.1 Khái niệm

a) Khái niệm về thông tin

Thông tin được hiểu là kết quả của hoạt động trí óc mang tính chất vô hình. Thông tin tồn tại dưới nhiều hình thức khác nhau như: được in ra, được viết ra, được lưu trữ trong các thiết bị điện tử, được truyền tải thông qua các phương tiện thông tin, truyền thông hay được chuyển qua các thiết bị đa phương tiện.

Trong mọi tình huống thì thông tin đều có tính chất là tài sản có giá trị hữu hình hoặc vô hình. Theo định nghĩa của ISO 27000, thông tin là một loại tài sản, cũng như các loại tài sản quan trọng khác của một doanh nghiệp, có giá trị cho một tổ chức và do đó, cần có nhu cầu để bảo vệ thích hợp.



Hình 2.1: hình ảnh về thông tin

Nhưng cho dù thông tin tồn tại dưới dạng nào đi chăng nữa, thông tin được đưa ra với 2 mục đích chính là chia sẻ và lưu trữ, nó luôn luôn cần sự bảo vệ nhằm đảm bảo sự an toàn thích hợp.

b) Khái niệm về an toàn thông tin

Information Security hay còn được gọi với cái tên An toàn thông tin là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.



Hình 2.2: Hình ảnh về an toàn thông tin

An toàn thông tin là một khái niệm bao hàm nhiều vấn đề, trong đó có:

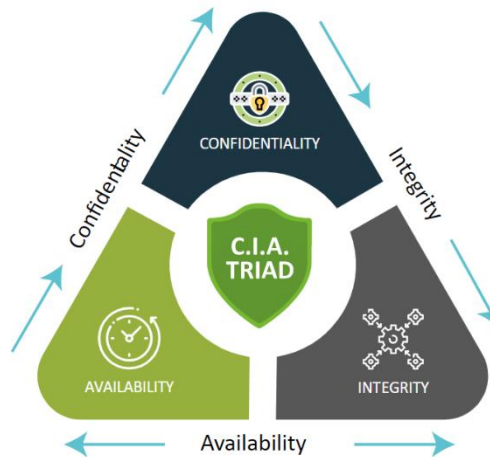
- + An toàn thông tin cho các tài sản vật lý như: máy chủ, thiết bị an ninh mạng, đường truyền internet,...
- + An toàn thông tin cho các tài sản phần mềm như: cơ sở dữ liệu, hệ điều hành, các phần mềm nghiệp vụ,...
- + An toàn thông tin cho tài sản thông tin như: bí mật kinh doanh, chính sách của một tổ chức hay chiến lược phát triển của đơn vị,...
- + An toàn thông tin cho tài sản dịch vụ như: các dịch vụ tổ chức cung cấp ra bên ngoài cũng như các dịch vụ mà bên ngoài cung cấp cho tổ chức của mình,...
- + An toàn thông tin cho tài sản con người như: lãnh đạo và nhân viên trong tổ chức,...

Có nhiều cách tiếp cận về an toàn thông tin, trong đó mô hình tam giác bảo mật CIA là cách tiếp cận dựa trên các thuộc tính của an toàn thông tin, bao gồm 3 thuộc tính:

- Confidentiality (tính bí mật hay tính bảo mật).
- Integrity (tính toàn vẹn hay tính nguyên vẹn).
- Availability (tính sẵn sàng hay tính khả dụng).

c) Mô hình CIA

Hình dưới đây thể hiện về các thuộc tính và mối quan hệ của các thuộc tính trong an toàn thông tin.



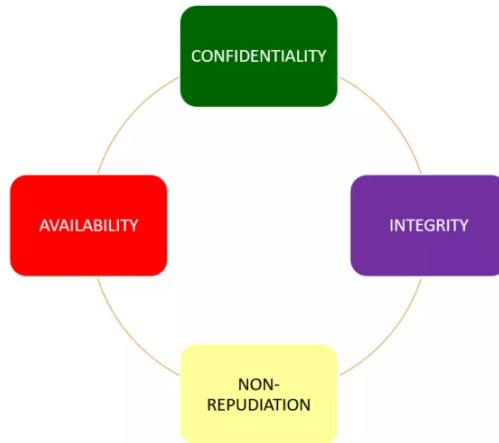
Hình 2.3: Mô hình tam giác an toàn thông tin CIA.

Tính bảo mật hay tính bí mật (Confidentiality) của thông tin thể hiện việc thông tin được bảo vệ khỏi việc bị tiết lộ, sử dụng bởi các cá nhân hoặc hệ thống trái phép. Tính bảo mật của thông tin bảo đảm rằng chỉ có những người dùng đã được phân quyền thì mới có thể truy cập, sử dụng thông tin. Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng.

Tính toàn vẹn hay tính nguyên vẹn (Integrity) của thông tin là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi. Tính toàn vẹn thông tin được coi là nền tảng của hệ thống thông tin, bởi thông tin sẽ không còn giá trị sử dụng nếu người dùng không thể xác minh tính toàn vẹn của nó. Nhiều mã độc hại (virus, worm...) máy tính được thiết kế với mục đích làm hỏng dữ liệu.

Tính sẵn sàng (Availability) tính sẵn sàng cho phép người dùng hợp pháp hay hệ thống máy tính có thể truy cập thông tin mà không bị can thiệp hay cản trở. Một số ví dụ về tính sẵn sàng của thông tin đó chính là việc một Website phải hoạt động một cách liên tục để đảm bảo bất cứ người dùng hợp pháp nào có thể truy nhập và tìm kiếm thông tin trên website đó.

Ngày nay, mô hình tam giác bảo mật CIA còn được bổ sung thêm các yếu tố khác là Non-Repudiation (Tính không chối bỏ).



Hình 2.4 Các thuộc tính của an toàn thông tin

Tính không chối bỏ (Non-repudiation) phải có biện pháp giám sát, đảm bảo một đối tượng khi tham gia trao đổi thông tin thì không thể từ chối, phủ nhận việc mình đã phát hành hay sửa đổi thông tin.

2.1.2 Các yếu tố ảnh hưởng đến an toàn thông tin

Các yếu tố ảnh hưởng đến an toàn thông tin gồm các yếu tố sau:

- Con người (People).
- Quy trình (Procedure).
- Công nghệ (Technology).

Giải thích từng các yếu tố:

a) Con người (People)

Con người (People) mặc dù luôn bị bỏ qua nhưng con người lại là mối đe dọa lớn đối với an toàn thông tin. Nguy cơ mất an toàn thông tin do phía con người có thể xuất phát từ các hành vi vô ý hay cố tình thực hiện các hành vi tấn công mạng, sử dụng công cụ tấn công là các phần mềm có hại, truy cập trái phép thông tin mật.



Hình 2.5: Hình ảnh về con người

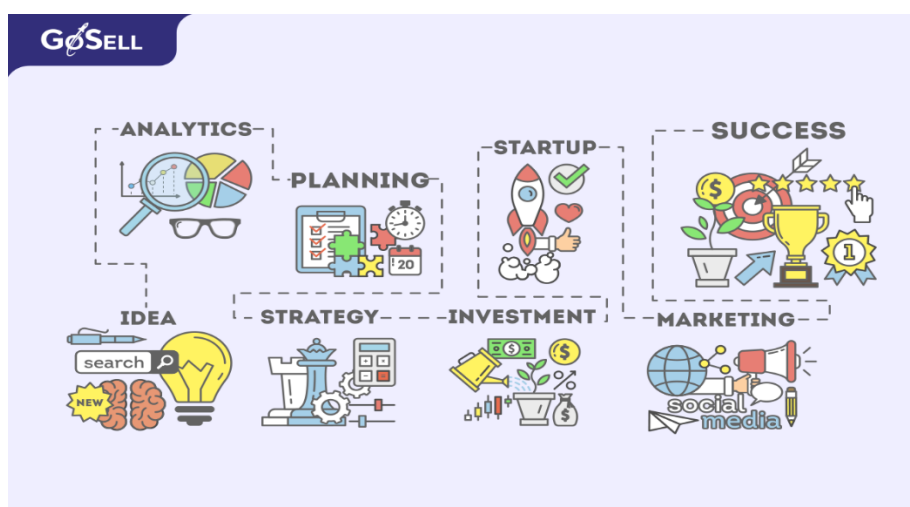
Các hành vi đó bao gồm:

- + Kẻ tấn công thực hiện các hành vi xâm nhập hệ thống, truy cập hệ thống trái phép, sử dụng phương thức tấn công lừa đảo bằng các kỹ nghệ xã hội (Social Engineering).
- + Tội phạm máy tính sử dụng các hình thức giả mạo thông tin, mua chuộc để lấy cắp thông tin nhằm mục đích phá hủy, sửa đổi dữ liệu trái phép, phổ biến các thông tin trái phép.
- + Các tổ chức khủng bố thâm nhập, tấn công hệ thống thông tin nhằm phá hoại, gây ra các cuộc chiến tranh thông tin.
- + Các tổ chức tình báo sử dụng các biện pháp ăn cắp thông tin, thâm nhập hệ thống nhằm ăn cắp các thông tin giá trị của đối thủ cạnh tranh, của quốc gia khác phục vụ mục đích kinh doanh, chính trị.
- + Các hành vi do chính các nhân viên bên trong tổ chức thực hiện như lạm dụng quyền truy cập, ăn trộm các thông tin kinh doanh, bán thông tin bí mật, sửa đổi các thông tin.

Qua những hành vi đã nêu ở phía trên thì rủi ro lớn nhất là từ phía con người, nên tổ chức phải có những chính sách chế tài, chương trình đào tạo và nâng cao nhận thức công nghệ hợp lý để tránh việc con người vô tình làm tổn hại hoặc thất thoát thông tin.

b) Quy trình (Procedure)

Là một yếu tố có thể gây ảnh hưởng đến an toàn hệ thống mà thường hay bị tổ chức chưa được quan tâm đúng mức. Quy trình ở đây được hiểu là các văn bản có tính định hướng của tổ chức và các văn bản cụ thể hướng dẫn thực thi một tập các nhiệm vụ được thiết kế để xác định, giới hạn, quản lý và kiểm soát các nguy cơ đối với dữ liệu, hệ thống để đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng của hoạt động hệ thống.



Hình 2.6: Hình ảnh về quy trình

Khi kẻ tấn công hiểu được quy trình của một tổ chức thì hắn có thể lợi dụng để tìm ra các kẽ hở gây ảnh hưởng tính toàn vẹn của thông tin.

Ví dụ: Nếu một nhà tư vấn ngân hàng biết được quy trình chuyển tiền qua hệ thống máy tính của ngân hàng, người này lợi dụng nó để ra lệnh chuyển hàng triệu đô la vào tài khoản của mình qua các điểm yếu an ninh (thiếu xác thực) trong quy trình này. Hầu hết các tổ chức đều phổ biến các quy trình để nhân viên có thể truy cập hợp pháp vào hệ thống thông tin nhằm thực hiện các nhiệm vụ của mình.



Hình 2.7: Lợi dụng sự yếu điểm trong hệ thống để rút tiền

Việc xây dựng các chính sách, quy định, quy trình và tuân thủ đúng văn bản an toàn thông tin đóng vai trò quan trọng trong việc bảo vệ thông tin, do vậy những kiến thức, hiểu biết về văn bản cần phải được phổ biến rộng rãi cho tất cả các thành viên trong tổ chức.

c) Công nghệ (Technology)

Công nghệ đóng vai trò quan trọng trong việc bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa an ninh mạng. Tuy nhiên, các hệ thống và phần mềm không hoàn hảo và có thể bị khai thác bởi những kẻ tấn công. Một số ví dụ về các lỗ hổng công nghệ có thể dẫn đến vi phạm an ninh mạng bao gồm:

- Lỗ hổng phần mềm: là lỗi trong phần mềm có thể bị khai thác bởi những kẻ tấn công để truy cập trái phép vào hệ thống hoặc dữ liệu.
- Phần mềm độc hại: Virus, worm và Trojan horse có thể lây nhiễm hệ thống và gây ra thiệt hại cho dữ liệu.
- Các cuộc tấn công mạng: Kẻ tấn công có thể sử dụng nhiều kỹ thuật khác nhau để tấn công hệ thống mạng, chẳng hạn như tấn công từ chối dịch vụ (DoS) hoặc tấn công xâm nhập mạng.



Hình 2.8: Hình ảnh về công nghệ

Việc sử dụng các giải pháp, biện pháp kỹ thuật theo sự phát triển của khoa học công nghệ nói chung và công nghệ thông tin nói riêng nhằm đảm bảo an toàn thông tin. Ngày nay, các giải pháp kỹ thuật đảm bảo an toàn thông tin thường bao gồm: hệ thống tường lửa (Firewall), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), phần mềm phòng chống virus, giải pháp mã hóa (Encryption), chữ ký số (CA)...

Kết luận ba yếu tố đã nêu ở trên: là con người, quy trình và công nghệ đều có mối quan hệ mật thiết, chặt chẽ với nhau, hỗ trợ và bổ sung cho nhau. Một hệ thống muốn đảm bảo an toàn thông tin thì phải chú ý cả ba yếu tố này.

2.2 Thực trạng an toàn thông tin tại Việt Nam

2.2.1 Thực trạng an toàn thông tin tại các tổ chức doanh nghiệp

Theo Cục An toàn thông tin – Bộ Thông tin và Truyền thông, qua khảo sát, đánh giá an toàn thông tin mạng một số cơ quan, doanh nghiệp trong thời gian qua ghi nhận một số đơn vị đã có sự quan tâm, đầu tư cho công tác đảm bảo an toàn thông tin mạng. Bước đầu áp dụng các tiêu chuẩn kỹ thuật về an toàn thông tin, triển khai các thiết bị bảo vệ, phát hiện, cảnh báo xâm nhập. Thành lập đơn vị quản trị hệ thống kiêm đảm bảo an toàn thông tin mạng.

Tuy nhiên, tại hầu hết các đơn vị được kiểm tra đều phát hiện hệ thống mạng có lỗ hổng bảo mật, bị tấn công xâm nhập, chiếm đoạt thông tin, tài liệu, nhiều máy chủ và hệ thống thông tin quan trọng bị kiểm soát, gây nguy cơ tấn công mạng rất nghiêm trọng như kiểm soát toàn bộ các liên lạc nội bộ qua thư điện tử, chiếm đoạt dữ liệu quan trọng trên máy tính và hệ thống mạng nội bộ. Biến các máy tính, điện thoại thông minh bị kiểm soát trở thành thiết bị gián điệp, bí mật ghi âm, ghi hình.



Hình 2.9: Trung tâm giám sát an ninh mạng quốc gia (NCSC)

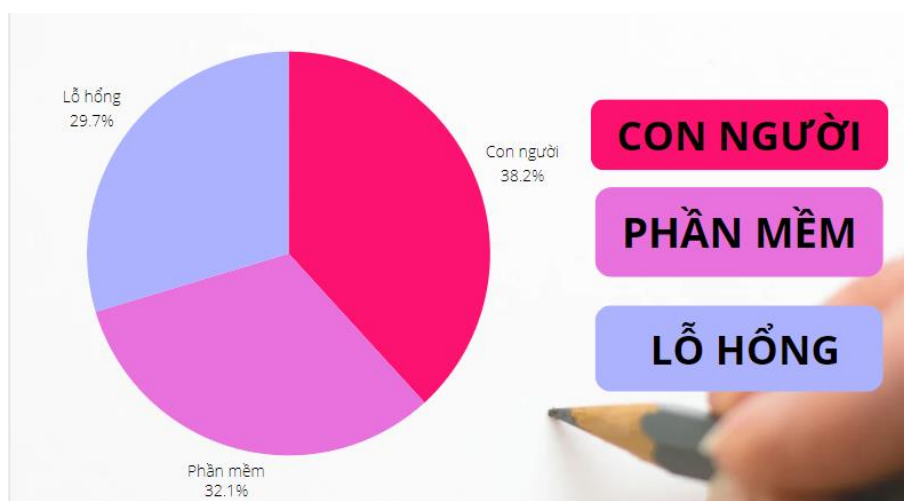
Trong năm 2023, các cuộc tấn công mạng có quy mô và mức độ lớn gia tăng dẫn đến gây mất dữ liệu và thiệt hại về kinh tế. Theo tổng hợp của National Cyber Security Centre (Trung tâm An ninh mạng Quốc gia) ghi nhận: so với năm 2022, số vụ tấn công mạng trong năm 2023 đã tăng 9,5%. Đặc biệt, trong 3 tháng cuối năm 2023, số vụ tấn công mạng gia tăng mạnh mẽ, lên đến 1.614 vụ mỗi tháng. Nguyên nhân được cho là do đây là thời điểm nhiều dự án công nghệ thông tin cần hoàn thành, dẫn đến nhân viên làm việc quá tải và dễ mắc sai sót, tạo cơ hội cho hacker tấn công.



Hình 2.10: Số lượng tấn công mạng trong những năm vừa rồi

Theo các chuyên gia Cyber Security Centre, hacker tập trung tấn công vào 3 điểm yếu chính:

- Điểm yếu con người (32,6%): Hacker sử dụng email giả mạo (phishing) có chứa tệp đính kèm mã độc hoặc đường link giả mạo để đánh lừa người dùng, chiếm quyền truy cập tài khoản và kiểm soát máy tính từ xa.
- Lỗ hổng phần mềm (27,4%): Các phần mềm thường bị khai thác bao gồm Mail Server, nền tảng quản lý nội dung và nền tảng chia sẻ dữ liệu.
- Lỗ hổng website do tổ chức tự phát triển (25,3%): Các lỗ hổng thường gặp là SQL Injection, mật khẩu quản trị yếu hoặc sử dụng thư viện tồn tại lỗ hổng.



Hình 2.11: Thống kê phần trăm các cuộc tấn công vào các yếu điểm

Theo đánh giá của các hãng bảo mật quốc tế, Việt Nam nằm trong nhóm 3 quốc gia bị tấn công mạng nhiều nhất tại khu vực châu Á - Thái Bình Dương... Đây là những con số được các chuyên gia đưa ra tại Hội nghị tập huấn công tác bảo vệ bí mật nhà nước (BMNN), an ninh mạng năm 2023 do Bộ Khoa học và Công nghệ (KH&CN) tổ chức.

2.2.2 Hoạt động tấn công vào các tổ chức doanh nghiệp

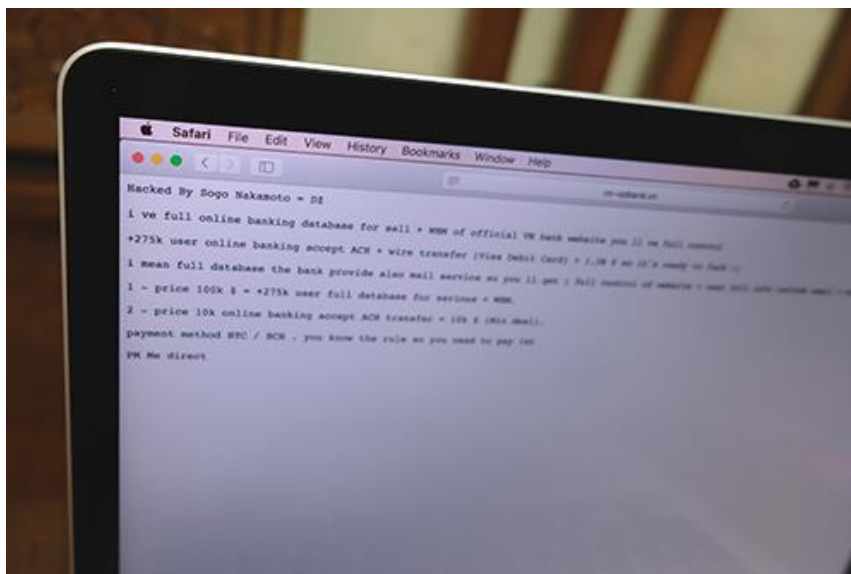
Trong thời gian qua, hoạt động tấn công mạng vào các tổ chức, doanh nghiệp Việt Nam có sự gia tăng mạnh cả về số lượng và mức độ nguy hiểm, xuất hiện ngày càng nhiều các cuộc tấn công có quy mô lớn nhằm vào mục tiêu quan trọng, kể cả những đơn vị được đầu tư mạnh để đảm bảo an toàn thông tin. Dưới đây là các vụ tấn công mạng nổi tiếng ở Việt Nam:

Sân bay Nội Bài, Tân Sơn Nhất bị tin tặc tấn công: Khoảng 16 giờ ngày 29/7/2016, tại sân bay Nội Bài, Tân Sơn Nhất thì màn hình ở các sân bay hiển thị các thông tin kích động, xúc phạm Việt Nam, Philippines và xuyên tạc các nội dung về Biển Đông. Cùng thời điểm, website của hãng hàng không Việt Nam cũng bị thay đổi thành hiển thị ngôn ngữ với lời lẽ kích động. Phía cuối website có dẫn đường link đến Pastebin.com để tải về tệp tin danh sách trên 400 nghìn tài khoản khách hàng thành viên của Việt Nam Airlines, trong đó bao gồm họ tên, ngày sinh, địa chỉ. Một số thành viên còn bị lộ chức vụ, cơ quan công tác, số điện thoại...



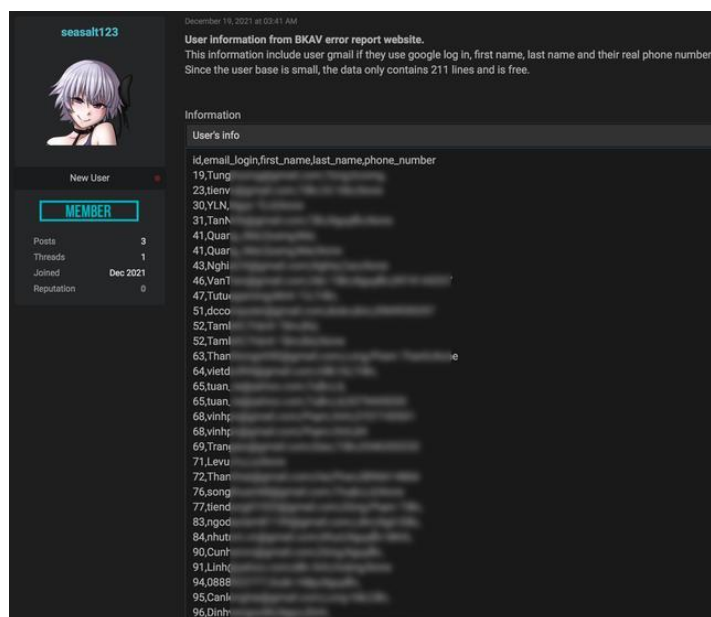
Hình 2.12: Tin tặc tấn công vào sân bay nội bài

Website Ngân hàng Hợp tác xã Việt Nam bị tấn công đòi tiền chuộc: Tối 13/10/2018, một địa chỉ thuộc website của ngân hàng Hợp tác xã Việt Nam (Co-op Bank) hiển thị thông tin bằng tiếng Anh với nội dung "Đã bị hack bởi Sogo Nakamoto". Tin tặc còn tuyên bố nắm trong tay toàn bộ cơ sở dữ liệu người dùng ngân hàng trực tuyến cũng như trình quản lý máy chủ web (WHM - Web Host Manager). Cụ thể, hacker yêu cầu 100.000 USD (khoảng 2,3 tỷ đồng) để đổi lấy toàn bộ database của hơn 275.000 người dùng kèm WHM, hoặc 10.000 USD (khoảng 233 triệu đồng) cho 10.000 tài khoản ngân hàng trực tuyến sử dụng ACH transfer (ngân hàng hối đoái tự động). Việc thanh toán được thực hiện thông qua Bitcoin hoặc Bitcoin Cash.



Hình 2.13: Website Ngân hàng Hợp tác xã Việt Nam bị tấn công đòi tiền chuộc

BKAV bị hacker phát tán thông tin người dùng: Ngày 22/12/2021, trên diễn đàn của hacker Raidforums, một tài khoản có tên seasalt123 đã chia sẻ về tập dữ liệu chứa thông tin người dùng được cho là của websiteBreport.vn, website mới được BKAV thành lập hồi tháng 9 nhằm cho phép người dùng báo cáo lỗi về Bphone. Trong đó, tập dữ liệu này bao gồm địa chỉ email, tên và số điện thoại của hơn 200 người dùng.



Hình 2.14: Tin tặc leak thông tin người dùng từ BKAV

Các hoạt động tấn công vào các tổ chức và doanh nghiệp ở Việt Nam cũng không phải là một vấn đề xa lạ. Một số hoạt động phổ biến mà các tổ chức và doanh nghiệp luôn phải đối mặt như tấn công mạng, sử dụng phần mềm độc, sử dụng kỹ thuật xã hội, tấn công từ chối dịch vụ (DDoS)... Những hoạt động tấn công này đe dọa sự an toàn và ổn định của các tổ chức doanh nghiệp ở Việt Nam và cần được đối phó bằng các biện pháp bảo mật hiệu quả, cũng như việc tăng cường nhận thức và đào tạo cho nhân viên về an ninh mạng.

2.3 Các tiêu chuẩn cần đảm bảo để hệ thống doanh nghiệp đạt an toàn thông tin

2.3.1 Tổng quan tiêu chuẩn

Hiện nay có rất là nhiều tiêu chuẩn quốc tế và quốc gia về an toàn thông tin mà doanh nghiệp có thể áp dụng để đảm bảo hệ thống của mình được bảo vệ an toàn. Dưới đây là một số tiêu chuẩn phổ biến hiện nay đang được sử dụng:

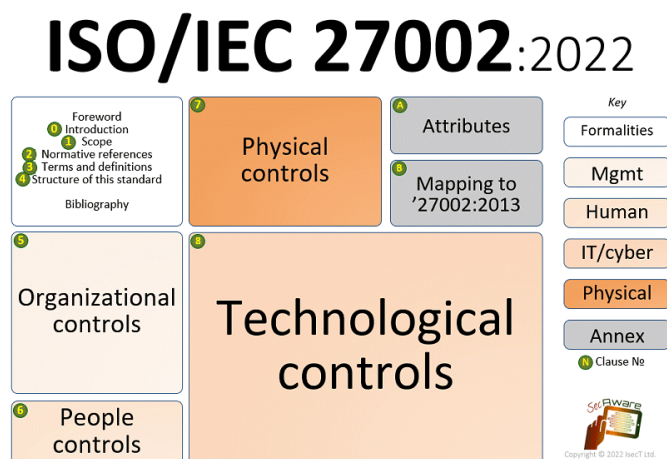
a) Tiêu chuẩn quốc tế

ISO/IEC 27001: Đây là một tiêu chuẩn quốc tế về quản lý an toàn thông tin, cung cấp một bộ khung để thiết lập, triển khai, vận hành, giám sát, xem xét, duy trì và cải tiến hệ thống quản lý an toàn thông tin (ISMS) trong tổ chức.



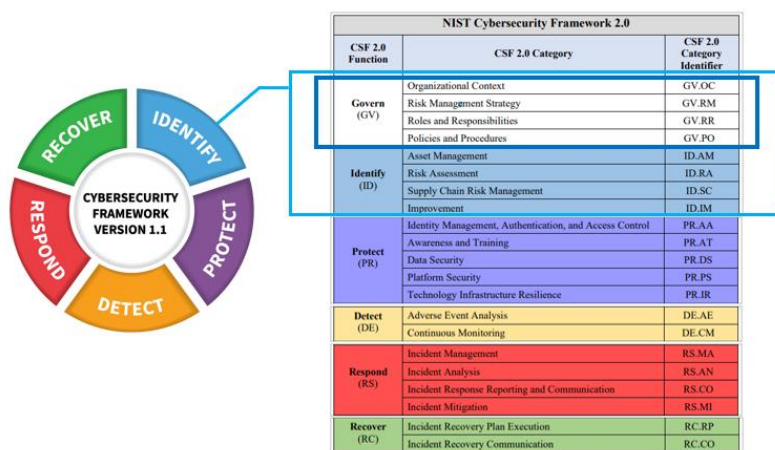
Hình 2.15: Tiêu chuẩn ISO/IEC 27001

ISO/IEC 27002: Hướng dẫn thực hành tốt nhất cho ISO/IEC 27001 hoặc ISO/IEC 17799 trước đây, cung cấp các chi tiết về các biện pháp kiểm soát an toàn thông tin cho các lĩnh vực như quản lý tài sản, kiểm soát truy cập, bảo mật hoạt động, bảo mật truyền thông, vv.....



Hình 2.16: Tiêu chuẩn ISO/IEC 27002

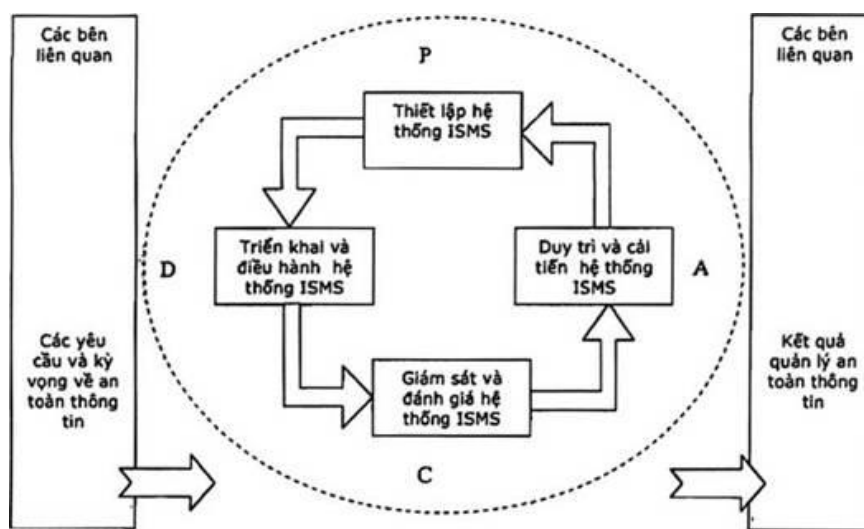
NIST Cybersecurity Framework (CSF): là một khung làm việc được phát triển bởi National Institute of Standards (Viện tiêu chuẩn) and Technology (Công nghệ quốc gia) viết tắt là(NIST) của Hoa Kỳ. Được công bố lần đầu vào năm 2014, cung cấp một phương pháp toàn diện để quản lý rủi ro an ninh mạng và cải thiện an ninh thông tin trong tổ chức.



Hình 2.17: Sơ đồ tiêu chuẩn của NIST CSF

b) Tiêu chuẩn quốc gia

Tiêu chuẩn quốc gia TCVN ISO/IEC 27001 là phiên bản tiếng Việt của tiêu chuẩn quốc tế ISO/IEC 27001 về hệ thống quản lý an ninh thông tin. Được phát triển bởi Tổng cục Tiêu chuẩn Đo lường Chất lượng Việt Nam (TCVN), tiêu chuẩn này là một bộ nguyên tắc và yêu cầu để tổ chức xây dựng, triển khai, duy trì và cải thiện một hệ thống quản lý an ninh thông tin hiệu quả.



Hình 1 - Áp dụng mô hình PDCA cho các quy trình hệ thống ISMS

Hình 2.18: Tiêu chuẩn quốc gia TCVN ISO/IEC 27001

QCVN 12:2018/BTTTT là quy chuẩn kỹ thuật quốc gia Việt Nam do Bộ Thông tin và Truyền thông ban hành. Quy chuẩn này áp dụng cho thiết bị điện và thiết bị viễn thông, cụ thể là về "An toàn điện và an toàn cơ bản đối với thiết bị và công trình viễn thông".

2.3.2 Cấu trúc của tiêu chuẩn

Cấu trúc của tiêu chuẩn là một phần quan trọng trong việc hiểu biết và triển khai tiêu chuẩn an toàn thông tin trong hệ thống doanh nghiệp. Cấu trúc này cung cấp một khung chung để tổ chức và trình bày các yêu cầu, nguyên tắc và hướng dẫn một cách logic và dễ hiểu. Dưới đây là một số điểm chính cần lưu ý:



Hình 2.19: Cấu trúc tiêu chuẩn ISO/IEC 27001:2013

a) Giới thiệu (Introduction)

- Giới thiệu ngắn gọn về tiêu chuẩn, bao gồm mục đích, lý do tồn tại, và cách sử dụng của tiêu chuẩn trong môi trường doanh nghiệp.
- Nêu rõ đối tượng mục tiêu của tiêu chuẩn.
- Giải thích bối cảnh và tầm quan trọng của việc áp dụng tiêu chuẩn.

b) Phạm vi (Scope)

- Xác định rõ ràng phạm vi của tiêu chuẩn, nêu rõ những gì được bao gồm và những gì không được bao gồm.
- Giúp làm rõ ranh giới và định hình kỳ vọng cho việc áp dụng tiêu chuẩn.
- Nêu rõ các loại hệ thống hoặc tổ chức mà tiêu chuẩn áp dụng.

c) Thuật ngữ và Định nghĩa (Terms and Definitions)

- Định nghĩa các thuật ngữ và khái niệm sử dụng trong tiêu chuẩn.
- Đảm bảo sự hiểu biết đồng nhất và tránh nhầm lẫn khi áp dụng tiêu chuẩn.
- Cung cấp định nghĩa rõ ràng cho các thuật ngữ chuyên ngành.

d) Yêu cầu (Requirements)

- Chứa các yêu cầu cụ thể mà hệ thống doanh nghiệp cần tuân thủ để đạt được tuân thủ tiêu chuẩn an toàn thông tin.
- Các yêu cầu này có thể bao gồm về quản lý rủi ro, bảo mật vật lý, bảo mật mạng, quản lý nhân sự, và nhiều lĩnh vực khác.
- Xác định các biện pháp kiểm soát cần thiết để bảo vệ thông tin.

e) Phương pháp thử nghiệm hoặc đánh giá (Testing or Evaluation Methods)

- Mô tả các phương pháp cụ thể để kiểm tra hoặc đánh giá việc tuân thủ các yêu cầu trong tiêu chuẩn.
- Giúp đảm bảo rằng các yêu cầu được thực hiện một cách chính xác và hiệu quả.
- Cung cấp hướng dẫn về cách thức đánh giá hiệu quả của các biện pháp kiểm soát.

f) Hướng dẫn về việc sử dụng (Guidelines for Use)

- Cung cấp hướng dẫn hoặc gợi ý về cách sử dụng tiêu chuẩn một cách hiệu quả trong môi trường doanh nghiệp.
- Bao gồm các bước cần thiết để thực hiện và duy trì tuân thủ tiêu chuẩn.
- Đề xuất các phương pháp hay nhất để áp dụng tiêu chuẩn.

g) Tham chiếu (References)

- Liệt kê các tài liệu hoặc tiêu chuẩn khác mà tiêu chuẩn hiện tại đề cập hoặc dựa vào.
- Giúp người đọc có thể tra cứu và tìm hiểu thêm về các nguồn tham khảo liên quan.
- Cung cấp thông tin về các tiêu chuẩn và quy định khác có liên quan.

h) Phụ lục (Appendices)

- Chứa các thông tin bổ sung, ví dụ hoặc dữ liệu hỗ trợ mà không thích hợp để đặt trong phần chính của tiêu chuẩn.
- Cung cấp thông tin chi tiết bổ sung cho các yêu cầu trong tiêu chuẩn.
- Bao gồm các ví dụ thực tế về cách áp dụng tiêu chuẩn.

2.4 Phân tích đề nghị và giải pháp

2.4.1 Phân tích yêu cầu mạng cho doanh nghiệp

- Yêu cầu đặt ra là dùng công nghệ mới về hạ tầng mạng 100/1000Mbps, Wire.
- Xây dựng vùng bên ngoài, mô phỏng internet của nhà mạng bằng các con router, firewall, server, PC, switch, printer.
- Tạo vùng DMZ, vùng này gồm các máy chủ DHCP, DNS, file.
- Tạo vùng Internet, vùng này gồm Server-PT (google.com) và PC-PT (khách hàng).
- Dựng tường lửa bảo mật.
- Xây dựng switch 3056 – 24PS và nối với các switch 2960 - 24TT.
- Tổ chức hệ thống mạng theo Vlan: Tức là chia nhỏ mạng của trung tâm thành các mạng con cho các phòng ban. Xác định nhu cầu kinh doanh: Hiểu rõ mục tiêu kinh doanh và yêu cầu cơ bản của doanh nghiệp để đảm bảo rằng hệ thống mạng đáp ứng được các yêu cầu này.

Phân tích định dạng mạng: Đánh giá cấu trúc tổ chức của doanh nghiệp để xác định cách mạng được triển khai và kết nối với nhau.

Xác định ứng dụng và dịch vụ mạng: Xác định các ứng dụng và dịch vụ mạng cần thiết như email, truy cập internet, cơ sở dữ liệu, truyền dữ liệu, video họp, và các ứng dụng kinh doanh khác.

Đánh giá nhu cầu về băng thông và hiệu suất: Phân tích nhu cầu băng thông và hiệu suất để đảm bảo rằng mạng có thể xử lý lượng dữ liệu lớn và đáp ứng các yêu cầu về thời gian thực.

Xác định yêu cầu bảo mật: Xác định các yêu cầu bảo mật như phân quyền truy cập, mã hóa dữ liệu, giám sát mạng, và kiểm soát người dùng.

2.4.2 Giải pháp cho doanh nghiệp

Xây dựng kiến trúc mạng:

Thiết kế kiến trúc mạng phù hợp với yêu cầu của doanh nghiệp bao gồm mạng LAN, WAN, WLAN, và VPN.

Triển khai thiết bị mạng:

Triển khai các thiết bị mạng như router, switch, firewall, và hệ thống phần mềm bảo mật để xây dựng một hệ thống mạng an toàn và tin cậy.

Quản lý băng thông và hiệu suất mạng:

Áp dụng các chiến lược quản lý băng thông và hiệu suất mạng để đảm bảo rằng mạng hoạt động một cách hiệu quả và ổn định.

Tăng cường bảo mật mạng:

Cấu hình các thiết bị mạng và triển khai các giải pháp bảo mật như tường lửa, IDS/IPS, và phần mềm diệt virus để bảo vệ mạng khỏi các mối đe dọa mạng.

Giám sát và duy trì:

Thực hiện giám sát và duy trì định kỳ để phát hiện sớm các vấn đề và thực hiện các biện pháp phòng ngừa và khắc phục.

Đào tạo và nâng cao nhận thức về an ninh mạng:

Cung cấp đào tạo cho nhân viên và tăng cường nhận thức về an ninh mạng để đảm bảo rằng họ hiểu và tuân thủ các quy tắc và biện pháp bảo mật mạng.

CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM

3.1 Công nghệ sử dụng cho hệ thống mạng của công ty

a) Vlan (virtual local area network)

Khái niệm:

VLAN (Virtual Local Area Network) là một mạng LAN ảo được tạo ra trên cùng một hạ tầng vật lý bằng cách sử dụng các switch có hỗ trợ VLAN. VLAN giúp chia nhỏ mạng LAN thành các nhóm logic riêng biệt, giúp tăng cường bảo mật, quản lý lưu lượng dễ dàng hơn và tiết kiệm băng thông.

Ứng dụng của Vlan:

- Giới hạn lưu lượng quảng bá chỉ trong Vlan cụ thể, giúp giảm lưu lượng truy cập không cần thiết trên mạng.
- Gia tăng tính bảo mật của hệ thống khi phân chia mạng thành các nhóm riêng biệt, hạn chế truy cập trái phép giữa các Vlan với nhau.
- Tạo ra vùng Broadcast Domain để sử dụng chung một ứng dụng nào đó. Ví dụ: điện thoại (VoIP).

Phân loại:

- Dựa vào trên cổng, loại này khá là phổ biến nhất. Mỗi máy tính kết nối tới một cổng trên switch đều thuộc một Vlan nào đó.
- Vlan dựa trên địa chỉ vật lý MAC của thiết bị kết nối.
- Vlan dựa trên giao thức mạng được sử dụng. Ví dụ: IP, IPX.

Ưu điểm của Vlan

- Tiết kiệm băng thông của mạng vì có thể chia nhỏ Lan thành các vùng. Khi một gói tin quảng bá, nó sẽ lan truyền trong một mạng Vlan duy nhất, không truyền sang các Vlan khác nên tiết kiệm được băng thông đường truyền.
- Tăng khả năng bảo mật vì các Vlan khác không truy cập vào nhau được trừ việc khai báo định tuyến.

- Dễ dàng thêm hay bớt các máy tính vào Vlan nên mạng có tính linh động cao.
- Giảm thiểu va chạm dữ liệu và cải thiện hiệu suất mạng cho các ứng dụng quan trọng.

Nhược điểm của Vlan:

- Cần sử dụng Switch có hỗ trợ tính năng Vlan để triển khai.
- Việc cấu hình và quản lý Vlan có thể phức tạp hơn so với mạng Lan truyền thống.
- Cần cẩn thận khi cấu hình Vlan để xảy ra sự cố kết nối hoặc lỗi mạng.

b) VTP (Vlan Trunking Protocol)

Khái niệm:

VTP (VLAN Trunking Protocol) là một giao thức độc quyền của Cisco hoạt động ở lớp 2 của mô hình OSI. VTP giúp quản lý cấu hình VLAN đồng nhất trên toàn mạng, bao gồm việc thêm, xóa, sửa đổi và đổi tên VLAN. Nó sử dụng các khung Trunk để truyền thông tin VLAN giữa các switch trong cùng một domain VTP.

Hoạt động:

- VTP sử dụng các phiên bản thông báo VTP để trao đổi thông tin VLAN giữa các switch.
- Phiên bản thông báo VTP bao gồm thông tin về tên VLAN, ID VLAN, chế độ VTP và phiên bản VTP.
- Switch VTP có thể hoạt động ở một trong ba chế độ:
 - Server: Là switch chính trong domain VTP, lưu trữ và quản lý cấu hình VLAN cho toàn mạng.
 - Client: Nhận cấu hình VLAN từ switch Server và sao chép vào bộ nhớ cục bộ.

- Transparent: Không tham gia vào việc quản lý cấu hình VLAN, chỉ chuyển tiếp thông tin VTP qua các liên kết Trunk.

Ưu điểm:

- VTP giúp đảm bảo cấu hình VLAN đồng nhất trên toàn mạng, giảm thiểu nguy cơ lỗi do cấu hình thủ công.
- Cho phép quản lý cấu hình VLAN tập trung từ một switch Server, giúp tiết kiệm thời gian và công sức.
- Đơn giản hóa việc triển khai VLAN mới trên toàn mạng, chỉ cần thực hiện thay đổi trên switch Server.

Nhược điểm:

- Do VTP sử dụng giao thức độc quyền của Cisco, nó có thể bị khai thác bởi kẻ tấn công để truy cập trái phép vào mạng.
- Hoạt động với các switch Cisco hỗ trợ VTP.
- Việc gỡ lỗi sự cố liên quan đến VTP có thể phức tạp do cấu hình VLAN được phân tán trên nhiều switch..

c) RIP (Routing Information Protocol)

Khái niệm:

RIP (Routing Information Protocol) là một giao thức định tuyến vector-distance nội miền, được sử dụng để trao đổi thông tin về các mạng con (subnet) giữa các router trong một mạng. RIP hoạt động trên Layer 3 (Network Layer) của mô hình OSI.

Hoạt động:

- Các router RIP định kỳ gửi bảng định tuyến của chúng bao gồm cả thông tin về các mạng con có thể đến được và số hop để đến các router lân cận.
- Mỗi router nhận được bảng định tuyến sẽ cập nhật bảng định tuyến của riêng mình bằng cách sử dụng thông tin nhận được.

- Router chỉ cập nhật các mục đích đến trong bảng định tuyến nếu số hop được quảng cáo ít hơn so với số hop hiện có trong bảng.
- Quá trình này được lặp lại định kỳ, cho phép các router xây dựng và duy trì một bức tranh toàn cảnh về mạng.

Ưu điểm:

- RIP là một giao thức đơn giản, dễ hiểu và dễ dàng cấu hình.
- Đây là một trong những giao thức định tuyến được sử dụng rộng rãi nhất trong các mạng quy mô nhỏ và trung bình.
- Nó có thể nhanh chóng hội tụ sau khi có sự thay đổi về topology mạng.

Nhược điểm:

- RIP chỉ tính đến số hop (hop count) để xác định đường đi tốt nhất, không tính đến các yếu tố khác như băng thông hay độ trễ. Điều này có thể dẫn đến việc chọn đường đi không tối ưu.
- Nó không phù hợp cho các mạng có quy mô lớn do vấn đề loop và cập nhật bảng định tuyến chậm.
- RIP không có tính năng bảo mật mặc định, khiến nó dễ bị tấn công giả mạo để can thiệp vào việc định tuyến.

d) VPN (Virtual private network)

Khái niệm:

VPN (Virtual Private Network) hay còn gọi là mạng riêng ảo, là một đường hầm được mã hóa thiết lập qua mạng internet công cộng, cho phép bạn tạo kết nối mạng an toàn và riêng tư giữa thiết bị của bạn (máy tính, điện thoại,...) và một mạng khác, thường là mạng của công ty hoặc dịch vụ VPN.

Phân loại:

- Site to site: Bằng việc sử dụng một thiết bị chuyên dụng và cơ chế bảo mật diện rộng, mỗi công ty có thể tạo ra kết nối với rất nhiều các site qua mạng công cộng như Internet.

- Remote Access: Đây là dạng kết nối user-to-lan áp dụng cho các công ty mà các nhân viên có nhu cầu kết nối mạng riêng từ các địa điểm từ xa và bằng các thiết bị khác nhau.

Hoạt động:

- Người dùng cung cấp thông tin xác thực như tên đăng nhập và mật khẩu để xác minh quyền truy cập VPN.
- Dữ liệu gửi, nhận giữa thiết bị của bạn và máy chủ VPN được mã hóa, giúp bảo vệ thông tin khỏi những kẻ theo dõi.
- Máy chủ VPN định tuyến lưu lượng truy cập internet của bạn, che giấu địa chỉ IP thực của bạn và tạo ra địa chỉ IP ảo.
- Khi dữ liệu đến đích, nó được giải mã để bạn có thể truy cập tài nguyên mong muốn trên internet.

Ưu điểm:

- Mã hóa dữ liệu của bạn giúp ngăn chặn những kẻ tấn công nghe lén trên mạng Internet công cộng.
- Giúp che giấu địa chỉ IP thực và tạo ra IP ảo để giúp người dùng che giấu thân phận.
- VPN có thể giúp bạn vượt qua các hạn chế về truy cập internet do nhà cung cấp dịch vụ internet (ISP) áp đặt.

Nhược điểm:

- Quá trình mã hóa và giải mã dữ liệu có thể làm chậm tốc độ Internet của bạn, tùy thuộc vào chất lượng kết nối và cấu hình của VPN.
- Một số dịch vụ VPN miễn phí có thể giới hạn băng thông của bạn, ảnh hưởng đến tốc độ truy cập Internet.
- Bạn cần lựa chọn nhà cung cấp VPN uy tín để đảm bảo họ không lưu trữ hoặc bán dữ liệu cá nhân của bạn.

e) DHCP, DNS Server

DHCP (Dynamic Host Configuration Protocol): Đây là giao thức được thiết kế để làm giảm thời gian chỉnh cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho các máy tính khi chúng vào mạng. Thiết bị sẽ sử dụng địa chỉ IP này để giao tiếp với các thiết bị khác trên mạng.

Ưu điểm của DHCP:

- Tự động hóa việc gán địa chỉ IP.
- Quản lý dễ dàng.
- Hiệu quả sử dụng địa chỉ IP.

Nhược điểm của DHCP:

- Phụ thuộc vào server DHCP.
- Rủi ro bảo mật.
- Xung đột địa chỉ IP.

DNS Server (Máy chủ hệ thống tên miền): Chủ yếu được dùng để dịch tên miền (domain name) thành địa chỉ IP. Giúp cho người dùng dễ nhớ tên miền hơn nhiều so với địa chỉ IP dạng số.

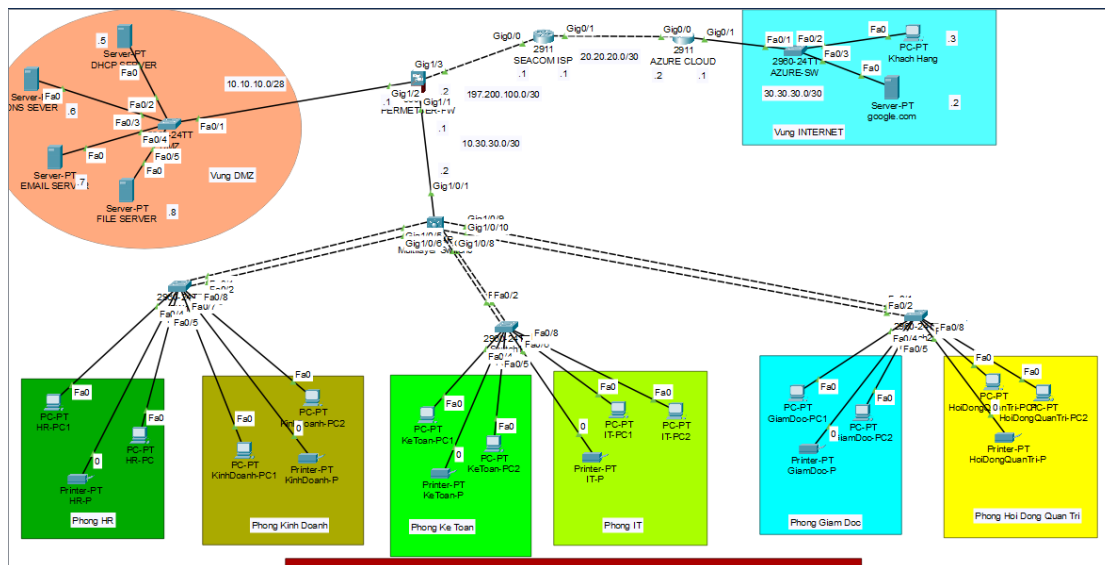
Ưu điểm của DNS Server:

- Dễ sử dụng.
- Tăng hiệu quả truy cập.
- Khả năng mở rộng.
- Tính linh hoạt.

Nhược điểm của DNS Server

- Phụ thuộc vào Server DNS.
- Rủi ro bảo mật.
- Độ trễ truy cập.
- Ảnh hưởng bởi sự cố ISP.

3.1 Sơ đồ thiết kế mạng trong doanh nghiệp



Hình 3.1: Sơ đồ thiết kế trong doanh nghiệp

Mô tả

Phân chia 3 vùng INSIDE, OUTSIDE, DMZ:

Vùng INSIDE các thiết bị:

- Firewall: 1, Switch layer 3 (3650): 1, Switch layer 2 (2960): 3
- Phòng ban: 6, PC: 12, Máy in: 6

Vùng DMZ các thiết bị:

- Switch layer 2 (2960): 1, Server: 4

Vùng OUTSIDE các thiết bị:

- Router 2911: 2, Switch 2960: 1, PC khách hàng: 1, Server ngoài: 1

3.2 Địa chỉ IP của các thiết bị

a) Vùng DMZ

Tên thiết bị	Địa chỉ IP	Subnet Mask	Default Gateway
DHCP Server	10.10.10.5	255.255.255.240	10.10.10.1
DNS Server	10.10.10.6		
Email Server	10.10.10.7		
File Server	10.10.10.8		

Bảng 3.1: Địa chỉ vùng DMZ

b) Vùng OUTSIDE

Tên thiết bị	Cổng kết nối	Địa chỉ IP	Subnet Mask	Default Gate way
Seacom ISP	Gig0/0	197.200.100.1	255.255.255.252	
	Gig0/1	20.20.20.1		
Azure cloud	Gig0/0	20.20.20.2	255.255.255.252	
	Gig0/1	30.30.30.1		
Khách Hang		30.30.30.3	255.255.255.252	30.30.30.1
Google.com		30.30.30.2	255.255.255.252	30.30.30.1

Bảng 3.2: Địa chỉ vùng OUTSIDE

c) Vùng INSIDE

Tên thiết bị	Cổng kết nối	Địa chỉ IP	Subnet mask	Default Gateway
PERMETTER-FW	Gig1/3	197.200.100.2	255.255.255.252	
	Gig1/2	10.10.10.1	255.255.255.252	
	Gig1/1	10.30.30.1	255.255.255.252	
Switch Multilayer Switch03	Gig1/0/1	10.30.30.2	255.255.255.252	

Bảng 3.3: Địa chỉ vùng INSIDE

3.3 Cấu hình các thiết bị

a) Vùng Dmz

*Switch L2:

```
hostname DMZ-SW
enable password cisco
no ip domain-lookup
ip domain-name cisco.net
```

b) Vùng Outside

*Router Seacom ISP

```
hostname Router
spanning-tree mode pvst
```

```
interface GigabitEthernet0/0

ip address 197.200.100.1 255.255.255.0

duplex auto

speed auto

ex

interface GigabitEthernet0/1

ip address 20.20.20.1 255.255.255.252

duplex auto

speed auto

ex

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

ex

interface Vlan1

no ip address

ex

router ospf 35

router-id 1.1.4.4

log-adjacency-changes

network 197.200.100.0 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

ip classless
```

```
ip route 10.30.30.0 255.255.255.252 197.200.100.2
```

```
ip route 10.20.0.0 255.255.255.252 197.200.100.2
```

```
ip route 192.168.10.0 255.255.255.0 197.200.100.2
```

```
ex
```

```
do wr
```

***Router AZURE CLOUD**

```
hostname Router
```

```
spanning-tree mode pvst
```

```
interface GigabitEthernet0/0
```

```
ip address 20.20.20.2 255.255.255.252
```

```
duplex auto
```

```
speed auto
```

```
ex
```

```
interface GigabitEthernet0/1
```

```
ip address 30.30.30.1 255.255.255.252
```

```
duplex auto
```

```
speed auto
```

```
ex
```

```
interface GigabitEthernet0/2
```

```
no ip address
```

```
duplex auto
```

```
speed auto
```

```
shutdown
```

```
ex
```

```
interface Vlan1

no ip address

shutdown

ex

router ospf 35

router-id 1.1.7.7

log-adjacency-changes

network 20.20.20.0 0.0.0.3 area 0

network 30.0.0.0 0.255.255.255 area 0

ex

ip classless

ip route 192.168.10.0 255.255.255.252 20.20.20.1

ip route 10.20.0.0 255.255.255.252 20.20.20.1

ip route 192.168.10.0 255.255.255.0 20.20.20.1

ip route 197.200.100.0 255.255.255.0 20.20.20.1

ip route 10.30.30.0 255.255.255.252 20.20.20.1

ip route 197.200.100.0 255.255.255.252 20.20.20.1

do wr
```

c) Vùng INSIDE

***Firewalld**

```
hostname FW

domain-name wr

enable password cisco

interface GigabitEthernet1/1
```

```
nameif INSIDE
security-level 100
ip address 10.30.30.1 255.255.255.252
ex
interface GigabitEthernet1/2
nameif DMZ
security-level 70
ip address 10.10.10.1 255.255.255.240
ex
interface GigabitEthernet1/3
nameif OUTSIDE
security-level 0
ip address 197.200.100.2 255.255.255.252
ex
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
ex
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
```

shutdown

ex

interface GigabitEthernet1/6

no nameif

no security-level

no ip address

shutdown

ex

interface GigabitEthernet1/7

no nameif

no security-level

no ip address

shutdown

ex

interface GigabitEthernet1/8

no nameif

no security-level

no ip address

shutdown

ex

interface Management1/1

management-only

no nameif

no security-level

no ip address

shutdown

ex

object network INSIDE-NET

subnet 10.30.30.0 255.255.255.252

nat (INSIDE,OUTSIDE) dynamic interface

object network INSIDE-OUT

subnet 192.168.10.0 255.255.255.0

nat (INSIDE,OUTSIDE) dynamic interface

object network INSIDE-OUT2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE,OUTSIDE) dynamic interface

object network INSIDE-OUT3

subnet 10.10.10.0 255.255.255.240

nat (DMZ,OUTSIDE) dynamic interface

ex

route OUTSIDE 0.0.0.0 0.0.0.0 197.200.100.1 1

route INSIDE 0.0.0.0 0.0.0.0 10.30.30.2 1

route OUTSIDE 0.0.0.0 0.0.0.0 20.20.20.2 1

route OUTSIDE 0.0.0.0 0.0.0.0 30.30.30.0 1

ex

access-list INSIDE-DMZ extended permit icmp any any

access-list INSIDE-DMZ extended permit udp any any

access-list INSIDE-DMZ extended permit udp any any eq bootps

```

access-list INSIDE-DMZ extended permit udp any any eq bootpc
access-list INSIDE-DMZ extended permit udp any any eq domain
access-list INSIDE-DMZ extended permit tcp any any eq domain
access-list INSIDE-DMZ extended permit tcp any any eq www
access-list INSIDE-DMZ extended permit tcp any any eq 8080
access-list INSIDE-DMZ extended permit tcp any any eq 443
access-list INSIDE-DMZ extended permit tcp any any eq 8443
access-list INSIDE-OUTSIDE extended permit icmp any any
access-list INSIDE-OUTSIDE extended permit tcp any any eq www
access-list INSIDE-OUTSIDE extended permit tcp any any eq 8080
access-list INSIDE-OUTSIDE extended permit tcp any any eq 443
access-list INSIDE-OUTSIDE extended permit tcp any any eq 8443
ex

access-group INSIDE-DMZ in interface DMZ
access-group INSIDE-OUTSIDE in interface OUTSIDE
ex

class-map inspection_default
  match default-inspection-traffic
ex

policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default

```


inspect dns preset_dns_map

inspect ftp

inspect http

inspect icmp

inspect tftp

ex

service-policy global_policy global

ex

telnet timeout 5

ssh timeout 5

router ospf 35

router-id 1.1.3.3

log-adjacency-changes

network 10.30.30.0 255.255.255.252 area 0

network 10.10.10.0 255.255.255.240 area 0

network 197.200.100.0 255.255.255.252 area 0

ex

do wr

*** Multilayer Switch0**

hostname CAIRO-CORE-SW

enable password cisco

ip routing

no ip domain-lookup

ip domain-name cisco.net

```
spanning-tree mode pvst

interface Port-channel1

    switchport mode trunk

interface Port-channel2

interface Port-channel3

    switchport mode trunk

interface Port-channel12

interface GigabitEthernet1/0/1

    no switchport

    ip address 10.30.30.2 255.255.255.252

    duplex auto

    speed auto

ex

interface GigabitEthernet1/0/2

    switchport mode trunk

ex

interface GigabitEthernet1/0/3

    switchport access vlan 60

    switchport mode access

ex

interface GigabitEthernet1/0/4

    switchport mode trunk

    channel-group 1 mode active

ex
```

```
interface GigabitEthernet1/0/5
```

```
switchport mode trunk
```

```
channel-group 1 mode active
```

```
ex
```

```
interface GigabitEthernet1/0/6
```

```
switchport mode trunk
```

```
channel-group 1 mode active
```

```
ex
```

```
interface GigabitEthernet1/0/7
```

```
channel-group 2 mode active
```

```
ex
```

```
interface GigabitEthernet1/0/8
```

```
channel-group 2 mode active
```

```
ex
```

```
interface GigabitEthernet1/0/9
```

```
switchport mode trunk
```

```
channel-group 3 mode active
```

```
ex
```

```
interface GigabitEthernet1/0/10
```

```
switchport mode trunk
```

```
channel-group 3 mode active
```

```
ex
```

```
interface Vlan1
```

```
no ip address
```

shutdown

ex

interface Vlan50

mac-address 000b.be9d.6701

ip address 192.168.10.1 255.255.255.0

ip helper-address 10.10.10.5

ex

interface Vlan60

mac-address 000b.be9d.6702

ip address 10.20.0.1 255.255.0.0

ip helper-address 10.10.10.5

ex

router ospf 35

router-id 1.1.2.2

log-adjacency-changes

network 192.168.10.0 0.0.0.255 area 0

network 10.20.0.0 0.0.0.255 area 0

network 10.30.30.0 0.0.0.3 area 0

ex

ip classless

ip route 20.20.20.0 255.255.255.252 10.30.30.1

ip route 30.30.30.0 255.255.255.252 10.30.30.1

ex

do wr


```

*Sw1:
  hostname CAIRO-ACCESS-SW1
  enable password cisco
  no ip domain-lookup
  ip domain-name cisco.net
  spanning-tree mode pvst
  spanning-tree extend system-id
  interface Port-channel1
    switchport mode trunk
  ex
  interface FastEthernet0/1
    switchport mode trunk
    channel-group 1 mode active
  ex
  interface FastEthernet0/2
    switchport mode trunk
    channel-group 1 mode active
  ex
  interface range FastEthernet0/3-23
    switchport access vlan 50
    switchport mode access
    switchport voice vlan 101
    spanning-tree portfast
    spanning-tree bpduguard enable
  ex
  interface FastEthernet0/24
    switchport access vlan 60
    switchport mode access
    spanning-tree portfast
    spanning-tree bpduguard enable
  ex

```

do wr

*SW 2

hostname CAIRO-ACCESS-SW2

enable password cisco

no ip domain-lookup

ip domain-name cisco.net

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel2

switchport mode trunk

ex

interface FastEthernet0/1

switchport mode trunk

channel-group 2 mode active

ex

interface FastEthernet0/2

switchport mode trunk

channel-group 2 mode active

ex

interface FastEthernet0/3

switchport access vlan 50

switchport mode access

switchport voice vlan 101

spanning-tree portfast

spanning-tree bpduguard enable

ex

Interface range FastEthernet0/4-23

switchport access vlan 50

switchport mode access

switchport voice vlan 101

```
spanning-tree portfast
spanning-tree bpduguard enable
```

ex

```
interface FastEthernet0/24
switchport access vlan 60
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

ex

```
interface Vlan1
no ip address
shutdown
```

ex

do wr

*SW 3

```
hostname CAIRO-ACCESS-SW3
enable password cisco
no ip domain-lookup
ip domain-name cisco.net
spanning-tree mode pvst
spanning-tree extend system-id
```

```
interface Port-channel2
switchport mode trunk
```

ex

```
interface Port-channel3
switchport mode trunk
```

ex





```
interface FastEthernet0/1
switchport mode trunk
channel-group 3 mode active
```



```
ex
interface FastEthernet0/2
  switchport mode trunk
  channel-group 3 mode active
ex
interface range FastEthernet0/3 - 23
  switchport access vlan 50
  switchport mode access
  switchport voice vlan 101
  spanning-tree portfast
  spanning-tree bpduguard enable
ex
interface FastEthernet0/24
  switchport access vlan 60
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
ex
interface Vlan1
  no ip address
  shutdown
ex
do wr
```



3.4 Thực hiện chạy các dịch vụ

Ping từ PC-HR đến vùng DMZ:

Fire	Last Status	Source	Destination	Type	Cc
	--	PER...	SEACOM...	ICMP	
	Successful	HR-P...	DHCP SE...	ICMP	

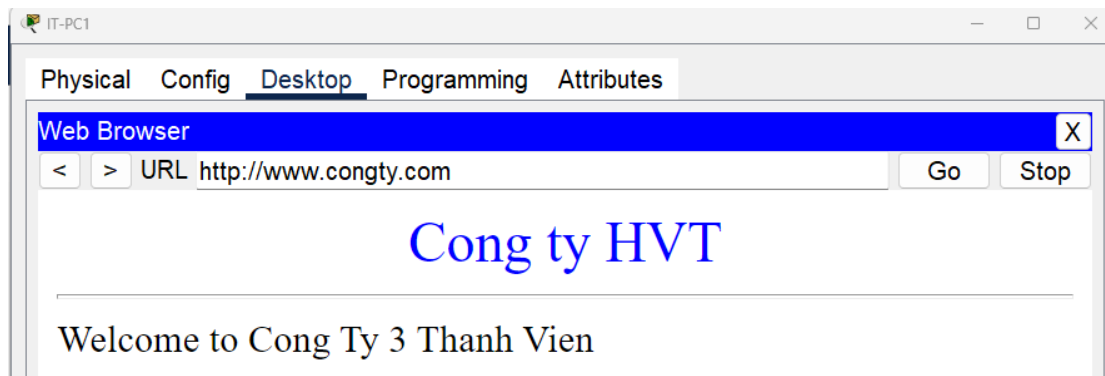
Hình 3.2: Ping từ PC-HR đến DHCP Server

Ping từ PC-KinhDoanh đến vùng Internet bên ngoài:

Fire	Last Status	Source	Destination	Type	Co
	Successful	Kinh...	google.com	ICMP	

Hình 3.3: Ping từ PC Kinh Doanh ra vùng Internet

Truy cập vào website của công ty từ máy PC-IT



Hình 3.4: Truy cập vào tên miền nội bộ công ty

Truy cập ra Internet bên ngoài bằng tên miền: google.com



Hình 3.5: Truy cập vào trang bên ngoài công ty

CHƯƠNG 4: KẾT LUẬN

4.1 Kết luận

Trong bài báo cáo này, chúng ta đã thảo luận về quan trọng của việc xây dựng kiến trúc an toàn cho hệ thống mạng của doanh nghiệp. An ninh mạng không chỉ là một yếu tố quan trọng mà còn là một yếu tố cần thiết để đảm bảo hoạt động ổn định và bền vững của doanh nghiệp. Tìm hiểu về các yếu tố ảnh hưởng đến an toàn thông tin, bao gồm con người, quy trình và công nghệ. Đặc biệt, chúng ta nhận thấy vai trò quan trọng của con người trong việc đảm bảo an toàn thông tin, từ việc đào tạo nhân viên đến việc tăng cường nhận thức về mối đe dọa từ mạng. Các giải pháp bảo mật mạng đã được đề xuất, bao gồm sử dụng firewall, phần mềm diệt virus, kiểm tra và giám sát liên tục, cùng với việc thực hiện các chính sách kiểm soát truy cập và đào tạo nhân viên.

Cuối cùng, chúng ta nhận thấy rằng việc xây dựng kiến trúc an toàn cho hệ thống mạng doanh nghiệp không chỉ là một cam kết ngắn hạn mà còn là một cam kết dài hạn để bảo vệ tài sản quan trọng của tổ chức và đảm bảo sự tin cậy của khách hàng và đối tác. Đầu tư vào an ninh mạng là một phần không thể thiếu của chiến lược kinh doanh của mọi doanh nghiệp trong thời đại số hóa ngày nay.

4.2 Giải pháp

- Triển khai Firewall và tường lửa ứng dụng (NGFW):

Sử dụng Firewall và NGFW để kiểm soát và giám sát lưu lượng mạng vào và ra khỏi hệ thống. Thiết lập các quy tắc cho phép hoặc từ chối truy cập dựa trên các nguyên tắc an toàn cụ thể.

- Sử dụng VPN (Virtual Private Network):

Triển khai VPN để bảo vệ dữ liệu khi truyền qua mạng công cộng, đặc biệt là khi nhân viên làm việc từ xa. VPN tạo ra một kênh kết nối an toàn giữa các thiết bị và mạng nội bộ của doanh nghiệp.

- Cập nhật hệ thống thường xuyên:

Đảm bảo rằng tất cả các hệ thống và phần mềm đều được cập nhật với các bản vá bảo mật mới nhất. Việc cập nhật định kỳ giúp loại bỏ các lỗ hổng bảo mật và giảm nguy cơ bị tấn công.

- Xác thực và quản lý tài khoản:

Triển khai các biện pháp xác thực đa yếu tố (MFA) để bảo vệ tài khoản người dùng khỏi việc truy cập trái phép. Quản lý tài khoản chặt chẽ bằng cách hạn chế quyền truy cập dựa trên nguyên tắc của người dùng.

- Giám sát và phát hiện tấn công:

Sử dụng giải pháp giám sát mạng để phát hiện và phản ứng nhanh chóng đối với các hoạt động đáng ngờ hoặc các mối đe dọa tiềm ẩn trên mạng.

- Nâng cao nhận thức an ninh:

Cung cấp đào tạo an ninh mạng định kỳ cho nhân viên và tăng cường nhận thức về an ninh thông tin trong toàn bộ tổ chức.

- Sao lưu và khôi phục dữ liệu định kỳ:

Thực hiện việc sao lưu dữ liệu định kỳ và triển khai kế hoạch khôi phục dữ liệu chi tiết để đảm bảo khả năng phục hồi sau sự cố mạng.

Tài liệu tham khảo

1. <https://vjst.vn/vn/tin-tuc/8126/an-toan--an-ninh-mang--thuc-trang-va-khuyen-cao.aspx>
2. <https://antoanthongtin.vn/an-toan-thong-tin/nam-2023-so-vu-tan-cong-mang-nham-vao-cac-he-thong-tai-viet-nam-tang-95-109609>
3. [What is Information Security? - GeeksforGeeks](#)
4. [What Is Information Security? | IBM](#)

Video Demo

[CLICK HERE](#)

<https://by.id.vn/8BEa>