TRƯỜNG ĐẠI HỌC ĐẠI NAM
KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP LỚN

TÊN MÔN HỌC: HỆ THỐNG MÁY TÍNH

TÊN ĐỀ TÀI: XÂY DỰNG BẢO MẬT CHO HỆ THỐNG MÁY TÍNH, MÁY VĂN PHÒNG CHO CÔNG TY VÂN NAM

Giảng viên hướng dẫn: ThS. Lê Văn Phong

Nhóm thực hiện: Nhóm 2:

Lưu Văn Nguyên

Nguyễn Nhật Anh

Hà Nội, 2024

TRƯỜNG ĐẠI HỌC ĐẠI NAM
KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP LỚN

TÊN MÔN HỌC: HỆ THỐNG MÁY TÍNH

TÊN ĐỀ TÀI: XÂY DỰNG BẢO MẬT CHO HỆ THỐNG MÁY TÍNH, MÁY VĂN PHÒNG CHO CÔNG TY VÂN NAM

STT	Mã Sinh Viên	Họ và Tên	Ngày Sinh	Điểm	
				Bằng Số	Bằng Chữ
1	1871020431	Lưu Văn Nguyên	04/10/2005		
2	1871020013	Nguyễn Nhật Anh	20/08/2006		

CÁN BỘ CHẤM THI 1 *CÁN BỘ CHẤM THI 2*

Hà Nội, 2024

LỜI NÓI ĐẦU

Trong kỷ nguyên số hóa hiện nay, công nghệ thông tin đóng vai trò quan trọng trong mọi hoạt động của doanh nghiệp, từ quản lý dữ liệu, truyền thông nội bộ đến các giao dịch với khách hàng và đối tác. Tuy nhiên, sự phát triển không ngừng của công nghệ cũng đi kèm với nhiều rủi ro về an ninh mạng, khi mà các mối đe dọa tấn công mạng ngày càng trở nên tinh vi và phức tạp hơn. Việc xây dựng một hệ thống bảo mật hiệu quả là yêu cầu cấp thiết để bảo vệ dữ liệu và tài sản của doanh nghiệp trước các nguy cơ tiềm ẩn.

Đề tài này được thực hiện nhằm cung cấp những kiến thức cơ bản và tổng quan về bảo mật hệ thống máy tính và thiết bị văn phòng trong doanh nghiệp. Nghiên cứu này tập trung vào việc phân tích các nguy cơ an ninh mạng hiện nay, những biện pháp bảo mật cần thiết, và phương pháp quản lý dữ liệu một cách hiệu quả. Thông qua đó, các doanh nghiệp có thể áp dụng những chiến lược phù hợp nhằm đảm bảo an toàn thông tin, nâng cao tính bảo mật và hiệu suất làm việc trong môi trường số.

Bố cục của nghiên cứu gồm nhiều phần, trong đó mỗi chương sẽ đi sâu vào các khía cạnh khác nhau của an toàn thông tin. Chương đầu tiên giới thiệu tổng quan về lý thuyết an toàn và bảo mật thông tin, cung cấp nền tảng kiến thức cho các phần tiếp theo. Tiếp theo, nghiên cứu sẽ đi sâu vào việc xây dựng các biện pháp bảo mật hệ thống mạng, quản lý phân quyền truy cập, và bảo vệ các thiết bị văn phòng khỏi các mối đe dọa phổ biến.

Với mong muốn cung cấp một tài liệu có giá trị thực tiễn, tài liệu này không chỉ là lý thuyết mà còn mang tính ứng dụng cao, hướng đến các doanh nghiệp vừa và nhỏ đang có nhu cầu nâng cao khả năng bảo mật hệ thống của mình. Hy vọng rằng nghiên cứu này sẽ là tài liệu

tham khảo hữu ích cho những ai quan tâm đến lĩnh vực bảo mật thông tin trong môi trường doanh nghiệp.

MỤC LỤC

MỤC LỤC BẢNG

MỤC LỤC HÌNH ẢNH

BẢNG CÁC TỪ VIẾT TẮT

STT	TỪ VIẾT TẮT	VIẾT ĐẦY ĐỦ
1	NAT	Network Address Translation
2	VLAN	Vitrual LAN
3	NAS	Network Attached Storage
4	SMB	Sever Message Block
5	FTP	File Transfer Protocol
6	DDoS	Distributed Denial of Service
7	URL	Uniform Resource Locator

CHƯƠNG I: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN

1.1. Giới thiệu về an toàn và bảo mật thông tin

An toàn và bảo mật thông tin là một trong những yếu tố quan trọng đối với bất kỳ hệ thống công nghệ thông tin nào, đặc biệt là trong môi trường doanh nghiệp. Với sự phát triển mạnh mẽ của công nghệ kéo theo đó là các mối đe dọa an ninh cũng ngày càng phức tạp và đa dạng. Việc đảm bảo an toàn thông tin giúp bảo vệ dữ liệu khỏi bị truy cập trái phép, mất mát hoặc thay đổi không mong muốn, từ đó góp phần bảo vệ quyền riêng tư và tài sản trí tuệ của doanh nghiệp.

Hình 1-1 An toàn và bảo mật thông tin

1.2. Khái niệm về an toàn và bảo mật thông tin

An toàn thông tin: Là việc bảo vệ thông tin tránh các nguy cơ mất mát, rò rỉ hoặc bị xâm nhập trái phép.

Bảo mật thông tin: Là việc giới hạn quyền truy cập vào thông tin, đảm bảo rằng chỉ những người có quyền mới được sử dụng dữ liệu.

Tuy hai khái niệm này liên quan chặt chẽ với nhau nhưng lại có 1 số sự khác biệt

Bảng 1 So sánh sự khác nhau

Tiêu chí	An toàn thông tin	Bảo mật thông tin
Phạm vi	Rộng hơn, bao gồm cả bảo mật, toàn vẹn và sẵn sàng.	Hẹp hơn, chỉ tập trung vào tính bí mật.
Mục tiêu chính	Đảm bảo thông tin không bị mất, thay đổi, hoặc bị gián đoạn.	Ngăn chặn truy cập trái phép vào thông tin.
Ứng dụng	Bảo vệ toàn bộ hệ thống thông tin (dữ liệu, thiết bị, mạng).	Bảo vệ quyền riêng tư và truy cập của dữ liệu.
Yếu tố liên quan	Toàn bộ vòng đời thông tin: lưu trữ, truyền tải, sử dụng.	Quyền truy cập và sử dụng dữ liệu cụ thể.

1.3. Nguyên tắc cơ bản.

An toàn và bảo mật thông tin có các nguyên tắc cơ bản như sau:

Confidentiality (Tính bảo mật): Đảm bảo rằng chỉ những người có quyền mới có thể truy cập thông tin.

Integrity (Tính toàn vẹn): Đảm bảo thông tin không bị thay đổi, sửa đổi hoặc giả mạo một cách trái phép.

Availability (Tính sẵn sàng): Đảm bảo rằng các hệ thống và thông tin luôn sẵn sàng cho người dùng hợp pháp khi cần.

Ba yếu tố này thường được gọi là "tam giác CIA" và là nền tảng của các chiến lược bảo mật thông tin.

Hình 1-2 Tam giác CIA

1.4. Các phương pháp bảo mật hệ thống.

Hình 1-3 Biện pháp bảo mật hệ thống

Có nhiều phương pháp để bảo vệ hệ thống trước các mối đe dọa bảo mật:

- Mã hóa dữ liệu: Mã hóa giúp bảo vệ thông tin bằng cách biến đổi dữ liệu thành một dạng không thể đọc được, trừ khi có khóa giải mã.

- Firewall (Tường lửa): Ngăn chặn các truy cập trái phép từ bên ngoài vào mạng nội bộ.

- Xác thực đa yếu tố (Multi-Factor Authentication): Yêu cầu người dùng xác thực qua nhiều yếu tố (mật khẩu, OTP, v.v.) để tăng cường bảo mật.

- Phân quyền người dùng: Phân quyền hợp lý giúp kiểm soát ai được phép truy cập vào tài nguyên nào, giảm nguy cơ truy cập trái phép.

- Sao lưu và phục hồi dữ liệu: Đảm bảo dữ liệu được lưu trữ an toàn và có thể phục hồi khi gặp sự cố.

1.5. Bảo mật trong môi trường doanh nghiệp

Hình 1-4 Bảo mật môi trường doanh nghiệp

Trong môi trường doanh nghiệp, việc bảo mật không chỉ giới hạn ở bảo vệ dữ liệu, mà còn bao gồm cả bảo vệ các thiết bị vật lý và tài nguyên của công ty. Để đảm bảo an ninh toàn diện, cần kết hợp các biện pháp kỹ thuật, quản lý, và nâng cao nhận thức của nhân viên:

- Biện pháp kỹ thuật: Áp dụng các công cụ và phần mềm bảo mật như firewall, phần mềm diệt virus, hệ thống phát hiện xâm nhập (IDS/IPS), và mạng riêng ảo (VPN).

- Biện pháp quản lý: Đặt ra chính sách bảo mật rõ ràng, đào tạo nhân viên về an ninh thông tin, và thường xuyên đánh giá các quy trình bảo mật.

- Nâng cao nhận thức: Đào tạo nhân viên về các mối đe dọa an ninh mạng và hướng dẫn họ cách phòng tránh, chẳng hạn như không nhấp vào các liên kết hoặc tệp đính kèm không xác định.

1.6. Sự quan trọng của bảo vệ an toàn thông tin

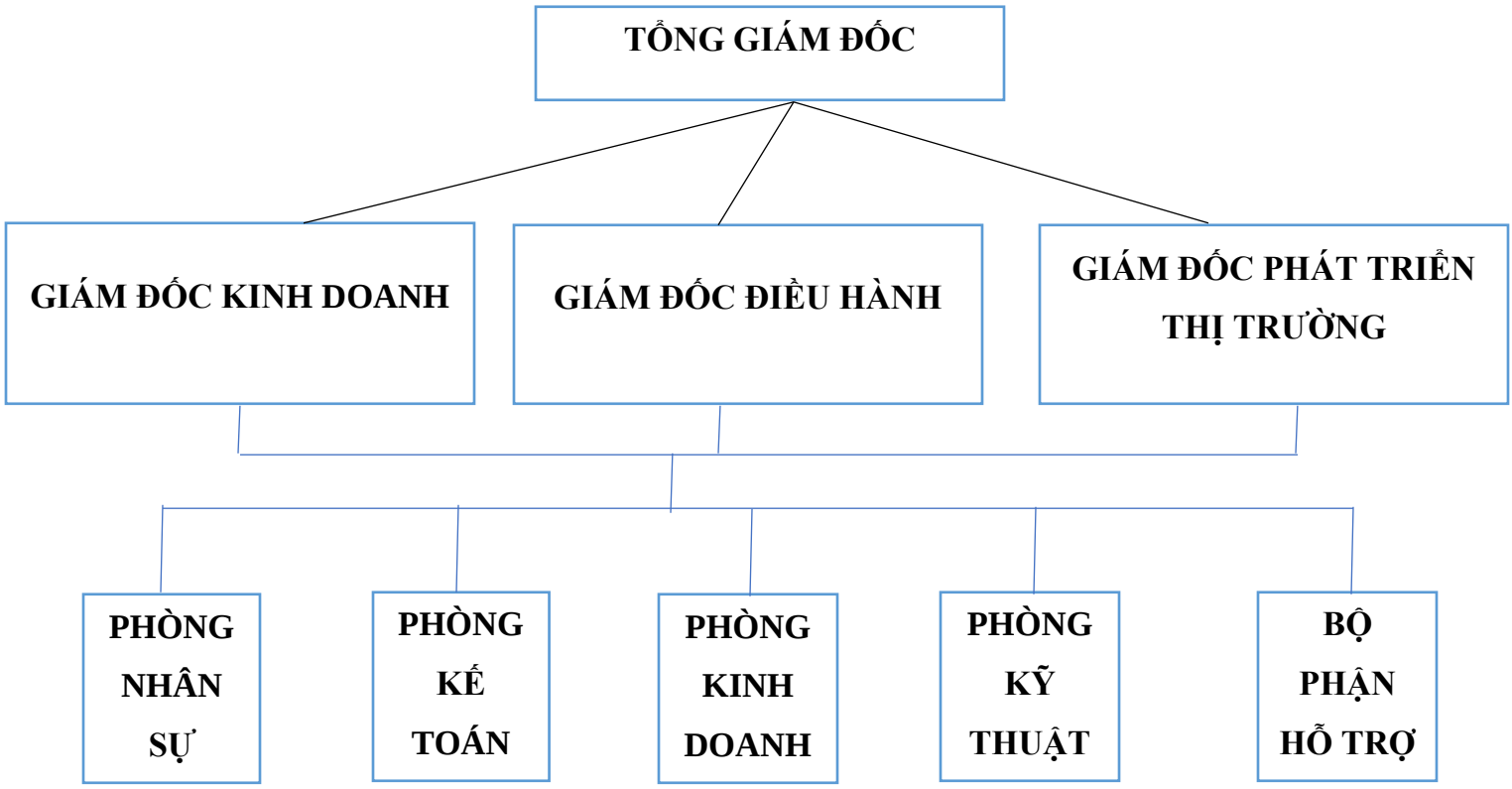
An toàn thông tin là một phần không thể thiếu trong quản lý hệ thống thông tin của các doanh nghiệp hiện đại. Bằng cách áp dụng các phương pháp bảo mật, như mã hóa, firewall, và phân quyền người dùng, kết hợp với các biện pháp quản lý và nâng cao nhận thức cho nhân viên, doanh nghiệp có thể bảo vệ hệ thống của mình khỏi các mối đe dọa, đảm bảo tính bảo mật, toàn vẹn, và sẵn sàng của thông tin.

Hình 1-5 Tầm quan trọng của bảo vệ thông tin

CHƯƠNG II:GIỚI THIỆU VỀ CÔNG TY VÂN NAM

2.1. Cơ cấu tổ chức

Sơ đồ cơ cấu tổ chức của công ty



2.2. Hệ thống máy văn phòng tại công ty

Phòng Tổng Giám đốc:

- Máy tính: 01 (được ưu tiên bảo mật cao nhất Tổng Giám đốc là người nắm các dữ liệu quan trọng và nhạy cảm của công ty, có mức độ truy cập rộng rãi)

Phòng Giám đốc Kinh Doanh:

- Máy tính: 01

- Quản lý dữ liệu chiến lược kinh doanh

Phòng Giám đốc Điều Hành:

-Quản lý các phòng ban

-Máy tính: 01

Phòng Giám đốc Phát Triển Thị Trường:

- Máy tính: 01

-Quản lý thông tin đối tác và nghiên cứu thị trường

Phòng Nhân Sự:

-Máy tính: 05

-Lưu trữ hợp đồng và các dữ liệu nhân sự

Phòng Kế toán:

-Máy tính: 05

-Máy in: 01

-Quản lý dữ liệu tài chính

Phòng Kinh Doanh:

-Máy tính: 10

-Máy in: 01

-Trao đổi dữ liệu khách hàng và hợp đồng

Phòng Kỹ thuật:

-Máy tính: 08

-Xử lý vấn đề kỹ thuật trong công ty

Bộ phận hỗ trợ:

-Máy tính: 04

-Hỗ trợ khách hàng

Hạ tầng mạng:

Switch: 02, chia cho tầng 1 và tầng 2

Hình 2-1 Switch mạng

Modem: 02, chia cho tầng 1 và tầng 2

Hình 2-2 Modem wifi

CHƯƠNG III: XÂY DỰNG BẢO MẬT CHO HỆ THỐNG MÁY VĂN PHÒNG

3.1. Mục tiêu xây dựng hệ thống bảo mật

Bảo vệ các thiết bị trong văn phòng khỏi các các thiết bị bên ngoài và nội bộ đồng thời đảm bảo tính an toàn cho dữ liệu hiện đang sử dụng

Xây dựng một hệ thống bảo mật toàn diện , đảm bảo tính bí mật và toàn vẹn của thông tin trong các thiết bị văn phòng. Nâng cao nhận thức của nhân viên về bảo mật thông tin để giảm thiểu rủi ro từ yếu tố con người

3.2. Cấu hình và triển khai bảo mật hệ thống máy tính

3.2.1. Bảo mật hệ thống mạng

1.Modem:

- Thay đổi mật khẩu và bật tường lửa tích hợp

Hướng dẫn thay đổi mật khẩu:

Bước 1: Đăng nhập vào giao diện quản lý modem.

- Kết nối máy tính hoặc điện thoại với modem qua cáp hoặc wifi..

- Mở trình duyệt web, nhập địa chỉ IP của modem.

- Đăng nhập bằng tài khoản quản trị.

Bước 2:Thay đổi mật khẩu:

- Sau khi đăng nhập vào phần Administration.

- Tìm Change Password hoặc Account Setting.

- Nhập mật khẩu cũ và mật khẩu mới.

-Lưu thay đổi.

Hướng dẫn bật tường lủa tích hợp:

Bước 1: Truy cập cài đặt Firewall

-Trong giao diện quản lý tìm mục Firewall

Bước 2: Kích hoạt tường lửa

- Đảm bảo tường lửa được Enable.

- Chọn các mức bảo vệ.

Bước 3:Lưu thay đổi

- Cấu hình NAT (Network Address Translation)

+NAT động(Dynamic NAT): Tự động gán IP công cộng từ một pool(tập hợp IP)

+NAT tĩnh(Static NAT): Ánh xạ một địa chỉ IP riêng cố định với một địa chỉ IP công cộng

Cách cấu hình NAT

Cấu hình NAT động:

-Truy cập giao diện NAT: Vào giao diện NAT settings hoặc Port Forwarding trong giao diện quản lý.

-Thiết lập pool IP: Đặt dải IP công cộng được ISP cung cấp.

- Lưu và áp dụng : Nhấn Save để kích hoạt NAT động.

Cấu hình NAT tĩnh:

- Truy cập giao diện NAT/Port Forwarding:Vào Port Mapping

- Tạo ánh xạ tĩnh: nhập địa chỉ IP riêng và địa chỉ IP công cộng tương ứng, thiết lập cổng giao tiếp nếu cần.

- Lưu cấu hình

-Ngăn chặn truy cập trái phép từ bên ngoài

Kích hoạt tường lửa.

Tắt dịch vụ không cần thiết

Cấu hình ACL (Access Control List): Thiết lập danh sách Ip được phép truy cập

Cập nhật firmware

Đặt mật khẩu mạnh, sử dụng WPA3 hoặc ít nhất là WPA2

- Thường xuyên kiểm tra nhật ký truy cập của modem.

- Thay đổi mật khẩu quan trị định kì

2. Switch :

-Chia VLAN (Virtual LAN): Phân đoạn mạng cho từng phòng ban để tăng cường bảo mật.

+VLAN 10: Phòng Hành chính.

+VLAN 20: Phòng Kế toán.

+VLAN 30: Phòng Kinh doanh

-Bật Port Security:

+Giới hạn số lượng thiết bị có thể kết nối với mỗi cổng của Switch.

+Chỉ cho phép các thiết bị đã được đăng ký (MAC address).

3.Wifi và Access Point:

Cách cài đặt mật khẩu WPA3 cho Wi-Fi

Bước 1: Truy cập giao diện quản lý Wi-Fi

- Kết nối thiết bị (máy tính, điện thoại) với Wi-Fi hoặc qua cáp LAN.

- Mở trình duyệt web và nhập địa chỉ IP của router/access point (thường là 192.168.1.1 hoặc 192.168.0.1).

- Đăng nhập bằng tài khoản quản trị (thường mặc định là admin/admin hoặc thông tin ghi trên router).

Bước 2: Cài đặt WPA3

- Tìm mục cài đặt Wi-Fi:

+ Vào tab Wireless, Wi-Fi Settings, hoặc tương tự.

+ Chọn Advanced Wireless Settings nếu cần.

- Chọn chế độ mã hóa:

+ Tìm mục Security Mode hoặc Encryption.

+ Chọn WPA3-Personal (hoặc WPA3-Enterprise nếu dùng trong môi trường doanh nghiệp).

- Đặt mật khẩu:

+ Trong mục Passphrase/Password, nhập mật khẩu Wi-Fi mạnh (ít nhất 12 ký tự, bao gồm chữ cái, số, và ký tự đặc biệt).

Ví dụ: V@nph0ng2024!

- Lưu thay đổi:

+ Nhấn Save hoặc Apply để áp dụng cài đặt.

Bước 3: Kiểm tra kết nối

- Kết nối lại Wi-Fi trên các thiết bị.

- Đảm bảo thiết bị hỗ trợ WPA3. Nếu không, thiết lập chế độ WPA2/WPA3 Mixed để tương thích.

3.2.2. Bảo mật máy tính và thiết bị văn phòng

1.Bảo vệ máy tính

Hướng dẫn cài đặt phần mềm chống virus và thiết lập tường lửa cá nhân:

Phần mềm chống virus**:**

- Tìm phần mềm phù hợp:

+ Lựa chọn các phần mềm đáng tin cậy như Kaspersky, Norton, hoặc Windows Defender (miễn phí tích hợp trong Windows).

- Cài đặt:

+Tải xuống từ trang chính thức , làm theo hướng dẫn cài đặt từng bước, đảm bảo bật chế độ quét tự động và cập nhật thường xuyên.

- Thiết lập nâng cao**:**

+ Bật bảo vệ thời gian thực (Real-time Protection).

+ Đặt lịch quét định kỳ hàng tuần.

Thiết lập tường lửa cá nhân:

- Windows Firewall:

+ Vào Control Panel > System and Security > Windows Defender Firewall.

+ Bật tường lửa cho cả mạng công cộng và riêng tư.

+ Thêm quy tắc (Inbound/Outbound Rules) để chặn hoặc cho phép ứng dụng cụ thể.

-Tường lửa bên thứ ba: Nếu cần, sử dụng phần mềm như ZoneAlarm để có các tính năng nâng cao.

Mã hóa ổ đĩa:

- Sử dụng BitLocker (Windows)**:**

Bước 1: Mở Control Panel > System and Security > BitLocker Drive Encryption.

Bước 2: Chọn ổ đĩa cần mã hóa, nhấn Turn on BitLocker.

Bước 3: Thiết lập mật khẩu hoặc khóa khôi phục.

Bước 4: Chọn chế độ mã hóa phù hợp (New hoặc Compatible mode).

Bước 5: Hoàn tất và kiểm tra lại bằng cách khởi động lại máy.

- Sử dụng VeraCrypt (Windows/Linux)**:**

Bước 1: Tải VeraCrypt từ trang chủ và cài đặt.

Bước 2: Mở VeraCrypt, chọn *Create Volume*.

Bước 3: Lựa chọn *Encrypt a non-system partition/drive*.

Bước 4: Thiết lập mật khẩu và thuật toán mã hóa.

Bước 5: Hoàn tất bằng cách mount ổ đĩa và kiểm tra truy cập.

Ví dụ về phân quyền tài khoản:

- Windows**:**

+ Mở Control Panel > User Accounts > Manage Accounts.

+ Tạo tài khoản Standard User cho người dùng thông thường.

+ Tài khoản Administrator chỉ dành cho quản trị viên để tránh lạm dụng quyền.

- Linux**:**

+ Dùng lệnh adduser [username] để thêm tài khoản thông thường.

+ Chỉ sử dụng sudo khi cần quyền root.

+ Chỉnh quyền thư mục: chmod và chown. Ví dụ:

Lệnh chmod 700 sensitive_file giới hạn chỉ chủ sở hữu được truy cập.

2. Bảo vệ máy in và máy photocopy

Giới hạn truy cập:

- Cách cấu hình máy in để giới hạn quyền truy cập qua IP nội bộ

+ Truy cập giao diện quản trị máy in qua trình duyệt (thường qua địa chỉ IP, ví dụ: 192.168.1.x)

+ Vào mục Network Settings hoặc Access Control.

+ Thiết lập danh sách IP được phép truy cập (Whitelist) hoặc chặn các IP lạ (Blacklist).

+ Áp dụng và kiểm tra lại bằng cách thử kết nối từ một thiết bị không được phép.

Đặt mật khẩu in ấn

-Quy trình đặt mật khẩu khi in tài liệu:

+ Truy cập giao diện cài đặt máy in hoặc máy photocopy.

+ Vào phần Job Accounting hoặc Secure Print.

+ Thiết lập chế độ yêu cầu mật khẩu trước khi in:

+ Nhập mật khẩu trên máy in khi in tài liệu nhạy cảm.

+ Lưu lại thiết lập và thông báo cho người dùng về quy trình.

3.3. Quản lý và chia sẻ dữ liệu an toàn

1.Thiết lập thư mục chia sẻ:

- Phân quyền truy cập:

+ Phòng Hành chính: Chỉ được quyền đọc tài liệu chung.

+ Phòng Kế toán: Được chỉnh sửa dữ liệu tài chính nhưng không truy cập các thư mục khác.

+ Phòng Kinh doanh**:** Được chỉnh sửa dữ liệu khách hàng, không truy cập tài liệu nội bộ.

2. Sử dụng công cụ lưu trữ tập trung:

- Giải pháp NAS (Network Attached Storage):

+ Lưu trữ và chia sẻ dữ liệu an toàn nội bộ.

+ Đặt quyền truy cập và kiểm soát nhật ký hoạt động (log).

- Cloud nội bộ:

+ Cung cấp giải pháp sao lưu tự động và chia sẻ tài liệu nhanh chóng.

- Hướng dẫn thiết lập NAS với phân quyền

+ Chuẩn bị thiết bị NAS**:**

Lựa chọn thiết bị phổ biến như Synology, QNAP hoặc DIY NAS bằng máy tính cũ.

+ Cấu hình cơ bản**:**

Kết nối NAS với mạng nội bộ qua cổng Ethernet.

Truy cập giao diện quản trị qua trình duyệt (thường qua địa chỉ IP).

+ Tạo người dùng và phân quyền**:**

Tạo tài khoản cho từng người dùng hoặc nhóm trong mục User Management.

Gán quyền truy cập thư mục (Read-only, Read/Write hoặc No Access).

Ví dụ: Nhân viên kế toán chỉ được truy cập thư mục tài chính, trong khi bộ phận IT có toàn quyền.

+ Cài đặt dịch vụ**:**

Kích hoạt dịch vụ SMB, FTP hoặc WebDAV để truy cập từ xa.

- Hướng dẫn cấu hình lịch sao lưu tự động

+ Lựa chọn công cụ sao lưu**:**

Sử dụng phần mềm tích hợp trên NAS hoặc công cụ như Acronis, Veeam.

+ Thiết lập lịch sao lưu**:**

Chọn chu kỳ sao lưu: hàng ngày, hàng tuần.

Lựa chọn phương thức: Full Backup (sao lưu toàn bộ) hoặc Incremental *Backup* (chỉ sao lưu phần thay đổi).

+ Lưu trữ đa lớp**:**

Sao lưu lên ổ cứng thứ hai hoặc dịch vụ Cloud như AWS, Google Drive.

+ Kiểm tra định kỳ**:**

Xác minh các bản sao lưu để đảm bảo tính toàn vẹn.

3. Kế hoạch phục hồi dữ liệu khi xảy ra sự cố (Disaster Recovery Plan)

- Phân tích rủi ro**:**

+ Xác định các tình huống có thể gây mất dữ liệu (mất điện, lỗi phần cứng, mã độc).

- Chuẩn bị phương án**:**

+ Duy trì ít nhất 3 bản sao của dữ liệu (quy tắc 3-2-1):

3 bản sao dữ liệu.

2 bản lưu trữ trên các thiết bị khác nhau.

1 bản sao lưu ở địa điểm khác.

- Thực hiện khôi phục dữ liệu**:**

+ Xác định phiên bản sao lưu cần khôi phục.

+ Dùng công cụ quản lý sao lưu trên NAS hoặc phần mềm bên ngoài để phục hồi.

- Kiểm tra sau phục hồi**:**

+ Xác minh dữ liệu đã khôi phục đầy đủ và không bị lỗi.

- Đánh giá và cập nhật kế hoạch**:**

+ Sau mỗi lần khôi phục, đánh giá quy trình và cập nhật kế hoạch để cải thiện hiệu quả.

3.4. Kiểm tra định kỳ và nâng cao nhận thức bảo mật

3.4.1.Kiểm tra hệ thống

1.Quy trình kiểm tra định kỳ các thiết bị mạng

- Modem và Router:

+ Kiểm tra firmware:

Đăng nhập vào giao diện quản trị của modem/router (thường qua địa chỉ IP như 192.168.1.1).

Đảm bảo firmware được cập nhật để vá các lỗ hổng bảo mật.

+ Xem nhật ký (log):

Kiểm tra nhật ký kết nối để phát hiện các truy cập bất thường hoặc tấn công brute force.

+ Thay đổi mật khẩu định kỳ:

Thay đổi mật khẩu quản trị mạnh, gồm chữ, số và ký tự đặc biệt.

- Switch:

+ Kiểm tra cấu hình VLAN:

Đảm bảo các VLAN được phân tách rõ ràng giữa các bộ phận, giảm nguy cơ xâm nhập trái phép.

+ Giám sát lưu lượng mạng:

Sử dụng công cụ như Wireshark để phát hiện các luồng dữ liệu không hợp lệ hoặc tấn công DDoS.

- NAS (Network-Attached Storage):

+ Kiểm tra quyền truy cập:

Định kỳ xem lại danh sách người dùng và quyền hạn, xóa tài khoản không còn sử dụng.

+ Cập nhật phần mềm NAS:

Đảm bảo hệ điều hành của NAS và các ứng dụng được cập nhật đầy đủ.

2. Cách phát hiện và khắc phục lỗ hổng bảo mật

- Cách phát hiện:

+ Kiểm tra hệ thống thường xuyên:

Dùng công cụ quét bảo mật như Nessus, OpenVAS để tìm các lỗ hổng.

- Giám sát bất thường:

+ Theo dõi sự gia tăng đột biến trong lưu lượng mạng hoặc kết nối từ các IP đáng ngờ.

- Kiểm tra tấn công phishing:

+ Xem xét email hoặc URL có chứa yếu tố đáng ngờ như sai chính tả, địa chỉ lạ.

- Khắc phục lỗ hổng:

+ Vá lỗi phần mềm:

Luôn cập nhật hệ điều hành, phần mềm ứng dụng và firmware.

+ Tăng cường bảo mật:

Sử dụng tường lửa (Firewall), thiết lập VPN cho kết nối từ xa.

+ Xây dựng chính sách bảo mật:

Quy định cụ thể việc truy cập tài liệu, hạn chế quyền admin.

3.4.2. Đào tạo nhân viên

1.Bài học nhận diện email phishing và đường link độc hại

- Nhận diện email phishing:

+ Đặc điểm thường gặp:

Tiêu đề giật gân, khẩn cấp như “Tài khoản của bạn bị khóa”.

Địa chỉ email người gửi bất thường hoặc chứa lỗi chính tả.

Yêu cầu cung cấp thông tin cá nhân hoặc tài khoản ngân hàng.

+ Ví dụ:

Một email từ "Banque_1234@xyz.com" yêu cầu xác minh tài khoản ngân hàng.

- Nhận diện đường link độc hại:

+ Kiểm tra URL trước khi nhấp:

Dùng chuột di chuột qua liên kết để xem địa chỉ thật.

Cảnh giác với link ngắn (shortened URL) hoặc chứa ký tự lạ.

+ Công cụ hỗ trợ:

Sử dụng VirusTotal để kiểm tra an toàn của đường link.

2. Quy trình xử lý khi gặp sự cố bảo mật

- Báo cáo sự cố:

+ Lập tức thông báo:

Nhân viên phát hiện sự cố phải báo cáo ngay cho bộ phận IT hoặc quản lý an ninh mạng.

+ Ghi nhận chi tiết:

Mô tả đầy đủ sự cố (thời gian, thiết bị, dấu hiệu bất thường).

- Cách ly thiết bị:

Ngắt kết nối thiết bị bị ảnh hưởng khỏi mạng để ngăn chặn lây lan.

Kiểm tra thiết bị bằng công cụ quét virus/mã độc như Malwarebytes.

- Khôi phục và đánh giá:

- Phục hồi dữ liệu:

Sử dụng bản sao lưu gần nhất để khôi phục hệ thống.

- Điều tra nguồn gốc:

Tìm nguyên nhân gốc rễ để vá lỗ hổng và ngăn ngừa sự cố lặp lại.

- Cập nhật quy trình bảo mật:

Rút kinh nghiệm từ sự cố và cải tiến các biện pháp an ninh.

KẾT LUẬN

Ưu điểm

- Bảo vệ dữ liệu quan trọng

  + Ngăn chặn mất mát dữ liệu**:** Các biện pháp bảo mật như mã hóa ổ đĩa, sao lưu định kỳ giúp bảo vệ dữ liệu quan trọng khỏi các sự cố mất mát do lỗi hệ thống, thiên tai hoặc tấn công mạng.

  + Bảo vệ thông tin nhạy cảm**:** Phân quyền truy cập và kiểm soát quyền sử dụng đảm bảo rằng chỉ những người được phép mới có thể truy cập vào các thông tin quan trọng của công ty.

  + Giảm thiểu rủi ro từ các mối đe dọa bên ngoài và bên trong

  + Phòng chống virus và mã độc**:** Cài đặt phần mềm chống virus và thiết lập tường lửa giúp ngăn chặn các phần mềm độc hại xâm nhập vào hệ thống.

  + Ngăn chặn truy cập trái phép**:** Thiết lập các biện pháp như tường lửa, VPN và phân quyền tài khoản giúp hạn chế khả năng truy cập trái phép từ bên ngoài và nội bộ.

- Tăng cường hiệu suất làm việc

  + Quản lý tài nguyên hiệu quả**:** Lưu trữ tập trung qua NAS hoặc các giải pháp đám mây nội bộ giúp quản lý dữ liệu và tài nguyên mạng một cách hiệu quả, dễ dàng truy cập và chia sẻ.

  + Giảm thời gian gián đoạn: Kế hoạch phục hồi dữ liệu và kiểm tra định kỳ hệ thống giúp giảm thiểu thời gian gián đoạn trong trường hợp sự cố xảy ra, đảm bảo hoạt động kinh doanh liên tục.

- Tuân thủ các quy định pháp luật và tiêu chuẩn ngành

+ Đáp ứng yêu cầu bảo mật: Các biện pháp bảo mật giúp doanh nghiệp tuân thủ các quy định về bảo vệ dữ liệu như GDPR, HIPAA, đảm bảo tránh các hình phạt pháp lý và duy trì uy tín doanh nghiệp.

+ Tăng cường niềm tin khách hàng**:** Bảo mật tốt giúp xây dựng niềm tin với khách hàng, đối tác, nâng cao hình ảnh và uy tín của công ty trên thị trường.

Nhược điểm

- Chi phí triển khai và duy trì cao

+ Đầu tư ban đầu lớn**:** Việc mua sắm phần cứng, phần mềm bảo mật, cũng như thiết lập hạ tầng mạng an toàn đòi hỏi một khoản đầu tư ban đầu đáng kể.

+ Chi phí vận hành và nâng cấp**:** Các giải pháp bảo mật cần được cập nhật thường xuyên để đối phó với các mối đe dọa mới, dẫn đến chi phí vận hành và bảo trì liên tục.

- Độ phức tạp trong quản lý

+ Yêu cầu kỹ năng chuyên môn**:** Việc thiết lập và quản lý các hệ thống bảo mật đòi hỏi nhân viên có kiến thức chuyên sâu về công nghệ thông tin và bảo mật.

+ Phức tạp trong cấu hình**:** Các biện pháp bảo mật phức tạp có thể gây khó khăn trong việc cấu hình và quản lý, đặc biệt đối với các doanh nghiệp nhỏ không có đủ nguồn lực.

- Ảnh hưởng đến trải nghiệm người dùng

+ Hạn chế quyền truy cập**:** Phân quyền chặt chẽ có thể làm giảm tính linh hoạt và tiện lợi cho người dùng trong việc truy cập và sử dụng tài nguyên.

+ Gián đoạn công việc**:** Các biện pháp bảo mật như quét virus thường xuyên hoặc yêu cầu xác thực đa yếu tố có thể gây gián đoạn nhỏ trong quá trình làm việc hàng ngày.

- Rủi ro từ yếu tố con người

+ Lỗi của người dùng**:** Nhân viên có thể vô tình vi phạm các quy định bảo mật do thiếu kiến thức hoặc do sơ suất, dẫn đến rủi ro bảo mật.

+ Mối đe dọa nội bộ**:** Các nhân viên không trung thực hoặc có ý định xấu có thể khai thác lỗ hổng trong hệ thống bảo mật để truy cập và lạm dụng dữ liệu.

Hướng phát triển

- Tích hợp công nghệ mới

+ Trí tuệ nhân tạo (AI) và máy học (Machine Learning)**:** Sử dụng AI và máy học để phát hiện các mối đe dọa bảo mật mới, phân tích hành vi bất thường và tự động hóa quá trình phản hồi sự cố.

+ Blockchain**:** Áp dụng công nghệ blockchain để tăng cường tính minh bạch và bảo mật trong việc lưu trữ và quản lý dữ liệu.

- Tăng cường đào tạo và nâng cao nhận thức bảo mật

+ Đào tạo liên tục cho nhân viên**:** Tổ chức các khóa đào tạo định kỳ về nhận diện mối đe dọa, quy trình xử lý sự cố và các biện pháp bảo mật mới nhất.

+ Chương trình nâng cao nhận thức**:** Xây dựng các chương trình truyền thông nội bộ để nâng cao nhận thức bảo mật, khuyến khích nhân viên tham gia vào việc bảo vệ dữ liệu và hệ thống.

- Phát triển các giải pháp bảo mật linh hoạt và dễ quản lý hơn

+ Giải pháp bảo mật dựa trên đám mây**:** Tận dụng các dịch vụ bảo mật dựa trên đám mây để giảm bớt gánh nặng quản lý hạ tầng bảo mật nội bộ và dễ dàng mở rộng khi cần thiết.

+ Quản lý bảo mật tích hợp (Integrated Security Management)**:** Phát triển các hệ thống quản lý bảo mật tích hợp để dễ dàng theo dõi, phân tích và phản hồi các sự cố bảo mật từ một giao diện duy nhất.

- Tăng cường hợp tác và chia sẻ thông tin về bảo mật

+ Hợp tác giữa các doanh nghiệp**:** Tham gia vào các liên minh bảo mật để chia sẻ thông tin về các mối đe dọa và biện pháp phòng chống hiệu quả.

+ Chia sẻ thông tin với các cơ quan chức năng: Thiết lập mối quan hệ với các cơ quan chức năng để nhận được hỗ trợ kịp thời và cập nhật các thông tin về các mối đe dọa mới.

- Phát triển các chính sách bảo mật toàn diện và linh hoạt

+ Chính sách bảo mật động: Xây dựng các chính sách bảo mật có khả năng thích ứng với các thay đổi nhanh chóng của môi trường công nghệ và các mối đe dọa mới.

+ Đánh giá và cải tiến liên tục: Thường xuyên đánh giá hiệu quả của các biện pháp bảo mật hiện tại và cải tiến chúng dựa trên các đánh giá này để đảm bảo luôn đáp ứng được các yêu cầu bảo mật mới.

TÀI LIỆU THAM KHẢO

[1]. Bộ Thông tin và Truyền thông (2024), *Hướng dẫn bảo mật cơ bản cho hệ thống văn phòng*, Nhà xuất bản Thông tin và Truyền thông, Hà Nội.

[2]. Phạm Thanh Bình (2019), *An toàn thông tin và bảo mật mạng*, Nhà xuất bản Giáo dục Việt Nam, Thành phố Hồ Chí Minh.

[3]. Trần Văn Luận (2021), *An toàn mạng máy tính*, Nhà xuất bản Đại học Quốc gia Hà Nội, Hà Nội.

[4]. Nguyễn Văn Nam; Nguyễn Thị Hoa (2020), "Phòng chống tấn công mạng: Thực trạng và giải pháp", *Tạp chí An toàn Thông tin*, Tập 10(2), 25-35.