BÁO CÁO THỰC HÀNH

Môn học: Quản lý rủi ro và an toàn thông tin trong doanh nghiệp

Lab 2: Risk Analysis, Evaluation, and Assessment

GVHD: Đỗ Thị Phương Uyên

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT207.P11.ANTT

Nhóm 16

STT	Họ và tên	MSSV	Email
1	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn
3	Nguyễn Thị Hồng Lam	20521518	20521518@gm.uit.edu.vn
4	Nguyễn Thị Thanh Mai	21521112	21521112@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Câu 1	100%
2	Câu 2	100%
3	Câu 3	100%
4	Câu 4	100%
5	Câu 5	100%
6	Câu 6	100%

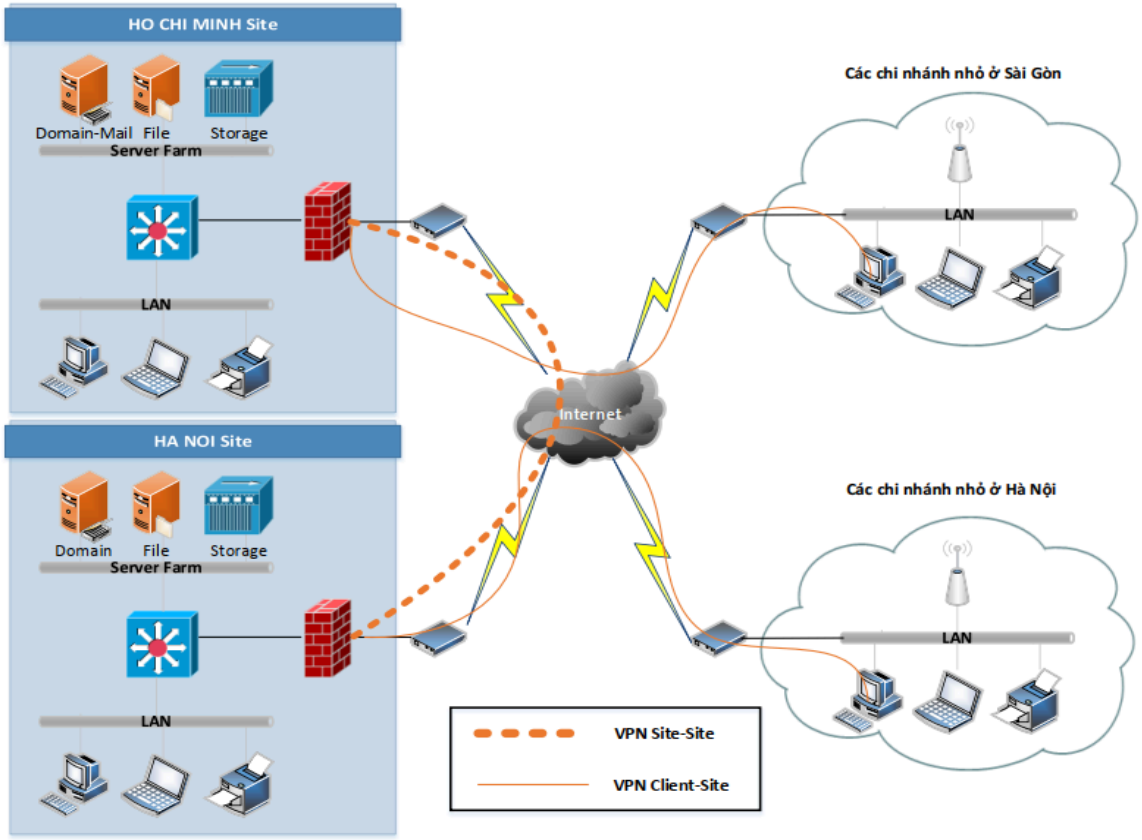
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Mô hình mạng hiện tại

Cho sơ đồ mạng hiện tại của doanh nghiệp như hình vẽ bên dưới:



Hình 1: Mô hình mạng doanh nghiệp

1. Phân tích Tính sẵn sàng của các dịch vụ trong hệ thống (Domain, File và Email)

1.1 Domain Server

Lỗ hổng	Rủi ro
Chưa có biện pháp bảo vệ server khỏi các cuộc tấn công nhắm vào khả năng sẵn sàng của hệ thống như DoS/DDoS attack, Ransomware attack, Swatting attack	Dễ bị tấn công từ bên trong một khi attacker thâm nhập được vào mạng LAN
Không có Caching DNS server để hỗ trợ Primary Server phản hồi cho các truy vấn mà Primary server đã từng trả lời	Nếu số lượng người dùng tăng lên thì Domain server dễ bị quá tải, giảm hiệu suất làm việc

Chỉ dùng một SDC để hỗ trợ PDC	Việc có SDC giúp tăng tính sẵn sàng so với chỉ có một PDC nhưng hệ thống này chỉ dùng 1 SDC và 1 PDC nên sẽ tiềm ẩn các rủi ro như: + Phụ thuộc vào đường truyền mạng WLAN: Khi cần xác thực người dùng, máy tính sẽ ưu tiên liên lạc với SDC trước nếu SDC không có thông tin cần thiết thì nó sẽ liên lạc với PDC. Do đó một khi kết nối mạng bị gián đoạn hoặc mất kết nối thì SDC dễ bị thiếu thông tin (do chưa kịp sao chép từ PDC) hoặc SDC không liên lạc được với PDC dẫn tới quá trình xác thực thất bại và người dùng không thể đăng nhập + Khả năng chịu lỗi bị hạn chế: Vì chỉ có 1 PDC và 1 SDC nên nếu cả 2 Domain Controller này đều gặp sự cố (ví dụ: bị phá huỷ do thiên tai, hư hỏng phần cứng hay phần mềm) thì toàn bộ dịch vụ Domain sẽ bị gián đoạn do không có DC dự phòng dẫn tới ảnh hưởng nghiêm trọng đến hoạt động của công ty.

1.2 File Server

Lỗ hổng	Rủi ro
Chưa có biện pháp bảo vệ server khỏi các cuộc tấn công nhắm vào khả năng sẵn sàng của hệ thống như DoS/DDoS attack, Ransomware attack, Swatting attack	Dễ bị tấn công từ bên trong một khi attacker thâm nhập được vào mạng LAN
Có 2 File server nhưng chúng chạy độc lập với nhau và không có cơ chế backup lẫn nhau	Nếu một máy chủ File Server gặp sự cố, người dùng ở khu vực tương ứng sẽ không thể truy cập vào dữ liệu. Mỗi miền lại lưu trữ data ở 1 File server khiến data bị phân tán, gây khó khăn trong việc chia sẻ và cộng tác giữa các nhân viên ở các chi nhánh khác nhau. Vì không có cơ chế backup lẫn nhau nên một khi 1 File Server bị hư hỏng hay gặp sự cố thì các người dùng (được phân quyền truy cập vào File Server này) không thể truy xuất data được, ảnh hưởng tới công việc họ đang làm

	Ngoài ra, do không thực hiện backup nên việc sao lưu và khôi phục dữ liệu trên một File Server rất phức tạp và tốn thời gian

1.3 Email Server

Lỗ hổng	Rủi ro
Không có một server chuyên biệt, độc lập mà tích hợp với Domain server	Vì Email Server tích hợp với Primary Server nên khi một trong hai có lỗ hổng và bị khai thác thì sẽ gây ra thiệt hại lớn cho công ty
Chỉ có duy nhất 1 Email Server	Nếu server gặp sự cố, toàn bộ dịch vụ email của công ty sẽ bị gián đoạn, ảnh hưởng nghiêm trọng đến hoạt động giao tiếp và kinh doanh. Ngoài ra, khi thực hiện nâng cấp hoặc bảo trì server thì sẽ làm gián đoạn các dịch vụ đang chạy trên server vì công việc này yêu cầu server ngừng hoạt động
Không có các biện pháp bảo vệ server khỏi các cuộc tấn công	Dễ bị tấn công bằng các cuộc tấn công DoS/DDOs, Spam mail,…
Tồn tại CVE (CVE-2019-1266) trên Exchange Email 2019	Attacker thực hiện khai thác CVE trên Email Server

2. Phân tích tính sẵn sàng của hạ tầng mạng

Lỗ hổng	Rủi ro
Chỉ có một core switch tại mỗi khu vực mạng (trụ sở và các chi nhánh)	Nếu switch này gặp sự cố thì sẽ làm gián đoạn toàn bộ mạng LAN tại khu vực triển khai switch này.

Chỉ sử dụng VPN để tạo kết nối mạng WAN, thiếu cơ chế dự phòng cho kết nối WAN	VPN là kết nối được thiết lập qua Internet công cộng nên chất lượng và tính sẵn sàng của kết nối này phụ thuộc vào khả năng kết nối Internet của các bên tham giao tiếp bằng VPN. Do đó nếu đường truyền Internet tại một trong hai điểm kết nối (trụ sở chính và các chi nhánh lớn, nhỏ) gặp sự cố thì kết nối VPN sẽ bị gián đoạn dẫn tới mất kết nối giữa các bên liên quan, gián đoạn hoặc ngừng các hoạt động, dịch vụ đang diễn ra giữa trụ sở và chi nhánh. Vì dụ các hậu quả có thể xảy ra: SDC không thể lấy thông tin từ PDC để xác thực user; các nhân viên trong công ty không thể trao đổi email với nhau.
Sử dụng modem Vigor với vai trò firewall và router	Modem này thường không được thiết kế cho mạng doanh nghiệp lớn với yêu cầu về tính sẵn sàng cao. Nếu modem gặp sự cố, toàn bộ kết nối Internet và mạng nội bộ của địa điểm đó sẽ bị gián đoạn.
Mỗi dịch vụ (File, Application) đều chạy trên một máy server. Riêng dịch vụ Domain và Email lại dùng chung 1 server	Nếu một máy chủ bị hỏng, dịch vụ tương ứng sẽ bị gián đoạn hoàn toàn vì không có server phụ thay thế server chính xử lý công việc.
Chỉ sử dụng dòng HP DL 380G5 làm server triển khai các dịch vụ trong công ty	HP DL 380G5 là dòng máy cũ, có khả năng hỏng hóc cao hơn so với các dòng máy mới nên tỉ lệ xảy ra sự cố gây tương đối cao.
Mỗi một vùng mạng LAN chỉ có 1 thiết bị lưu trữ NAS	Nếu NAS bị hỏng, dữ liệu sao lưu sẽ bị mất gây ảnh hưởng đến khả năng khôi phục hệ thống, mất mát dữ liệu và khó khôi phục lại.
Mỗi địa điểm (trụ sở và các chi nhánh) đều chỉ có duy nhất một kết nối ra Internet	Nếu đường truyền Internet gặp sự cố, toàn bộ địa điểm đó sẽ mất kết nối Internet và không thể truy cập các dịch vụ bên ngoài.

Sử dụng Wireless N Access Point (TL-WA801ND)	Nếu một access point bị hỏng thì chỉ một phần nhỏ người dùng bị ảnh hưởng nhưng TL-WA801ND là thiết bị có công nghệ khá cũ, dễ gây nghẽn mạng nếu số lượng người dùng lớn.
Mỗi địa điểm chỉ có một modem/firewall duy nhất. + DC HCM chỉ dùng 1 Modem ADSL Draytek 3200 và không có thêm firewall nào + DC HN dùng 1 Modem ADSL Draytek 2900 – Firewall + Các chi nhánh nhỏ dùng duy nhất 1 VIGOR 2830 để làm Firewall và Router	Tại mỗi địa điểm (trụ sở và chi nhánh), nếu modem/firewall bị hỏng, toàn bộ kết nối Internet và bảo mật của địa điểm đó sẽ bị gián đoạn.
Mạng LAN phẳng (không chia thành VLAN)	Nhân viên có thể vô tình gây ra sự cố (ví dụ như: broadcast storm, vòng lặp mạng) dẫn tới làm nghẽn toàn bộ mạng LAN, gây gián đoạn dịch vụ. Nếu một máy tính trong mạng LAN của công ty bị nhiễm malware hay virus, sự lây lan có thể dễ dàng diễn ra và tiêm nhiễm vào các máy tính khác trong cùng mạng LAN do đây là mạng phẳng. Các malware/virus này thường phá hoại dữ liệu, làm treo thiết bị mà chúng nhiễm vào hoặc làm gián đoạn hoạt động diễn ra trên máy tính,… Ngoài ra, do không có sự phân đoạn mạng nào nên sniffing dễ dàng được thực hiện vì tất cả các gói tin đều được phát tán trong cùng một mạng con dẫn tới dự liệu nội bộ bị rò rỉ. Nhân viên hay kẻ xâm nhập có thể lợi dụng mạng phẳng để thực hiện leo thang đặc quyền.

3. Phân tích những rủi ro dẫn đến mất mát thông tin do người dùng gây ra

Rủi ro	Hành động của user
Mật khẩu yếu và quản lý mật khẩu kém	+ Sử dụng mật khẩu dễ đoán: Mật khẩu quá ngắn, sử dụng thông tin cá nhân (ngày sinh, tên), hoặc các từ phổ biến rất dễ bị đoán. + Tái sử dụng mật khẩu: Sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau. Nếu một tài khoản bị lộ, tất cả các tài khoản khác cũng có nguy cơ bị xâm phạm. + Lưu trữ mật khẩu không an toàn: Ghi mật khẩu ra giấy, lưu trong tệp văn bản không được mã hóa, hoặc chia sẻ mật khẩu với người khác.
Phishing và các tấn công lừa đảo	+ Nhấp vào liên kết độc hại: Nhân viên nhấp vào liên kết/file đính kèm trong email, tin nhắn, hoặc quảng cáo trực tuyến chuyển tiếp đến các trang web giả mạo hoặc chứa mã độc hoặc tự động tải malware về máy nạn nhân . + Cung cấp thông tin cá nhân cho kẻ lừa đảo: Bị lừa cung cấp thông tin đăng nhập, thông tin thẻ tín dụng, hoặc các thông tin nhạy cảm khác cho kẻ lừa đảo giả danh là ngân hàng, cơ quan chính phủ, hoặc các tổ chức uy tín.
Sử dụng thiết bị cá nhân không an toàn	+ Thiếu cập nhật phần mềm: Không cập nhật hệ điều hành, trình duyệt, và các ứng dụng, khiến thiết bị dễ bị tấn công bởi các lỗ hổng bảo mật đã được biết đến. + Không sử dụng phần mềm diệt virus: Không cài đặt hoặc không cập nhật phần mềm diệt virus, khiến thiết bị dễ bị nhiễm malware hoặc bị attacker xâm nhập. + Mất hoặc bị đánh cắp thiết bị: Mất điện thoại, máy tính xách tay, hoặc máy tính bảng chứa dữ liệu nhạy cảm liên quan tới công ty

Người dùng có hành vi bất cẩn và thiếu hiểu biết	+ Dùng tuỳ tiện các phần mềm và thư viện do các bên không uy tín cung cấp: Nhân viên tải và sử dụng các phần mềm có backdoor, CVE, hay các lỗ hổng chưa được khắc phục. Cài đặt các thư viện mã nguồn mở độc hại hoặc các thư viện lỗi thời, chứa lỗ hổng dễ bị tấn công. + Truy cập các trang web giả mạo hoặc không an toàn: Nhân viên mở lung tung các trang web mà không quan tâm tới yếu tố an toàn. + Không tuân thủ các quy định bảo mật của công ty: Nhân viên chia sẻ thông tin hoặc gửi tài liệu bằng các ứng dụng truyền gửi không được mã hoá, mạng xã hội. + Thực hiện các thao tác làm mất dữ liệu: Nhân viên vô tình xóa nhầm các tài liệu, ghi đè dữ liệu lên file gốc, chỉnh sửa nhầm file,…
Người dùng có hành vi gây hại bằng tác động vật lý	+ Phá hoại các thiết bị phần cứng: Vô tình hoặc cố ý làm hỏng thiết bị, máy móc trong công ty hay phá huỷ các phần cứng.

Bảng Risk Score đánh giá những rủi ro dẫn đến mất mát thông tin do người dùng gây ra

Threat		Vulneribitily	Impact				Likelihood				Risk
Agent	Action		C	I	A	Impact Score	Exposure	Frequency	Control	Likelihood Score	Risk Score

Employee	Click vào các link lạ, truy cập tới các trang web độc hại, giả mạo do attacker tạo ra	Đối với endpoint: Không cài phần mềm anti-virus, không triển khai tường lửa trên thiết bị Đối với network: Không có hệ thống giám sát lưu lượng mạng như IDS, NSM, các hệ thống phân tích và phát hiện sự cố như SIEM, NDR, Đối với user: chưa tập huấn nâng cao ý thức nhân viên về vấn đề rủi ro và an toàn thông tin	**5**	**0**	**0**	**5**	**3**	**5**	**1**	**4**	**20**
Employee	Tải phần mềm hoặc các file từ nguồn không đáng tin cậy	Đối với endpoint: Không cài phần mềm anti-virus Đối với network: Không có các hệ thống phân tích và phát hiện sự cố như SIEM, NDR. Không có firewall tích hợp anti-virus Đối với user: chưa tập huấn nâng cao ý thức nhân viên về vấn đề rủi ro và an toàn thông tin	**3**	**5**	**0**	**5**	**3**	**5**	**2 (Reverse= 0.8)**	**3.2**	**15**

Employee	Chụp ảnh, nhắn tin và đính kèm tài liệu của công ty rồi gửi nó ra bên ngoài thông qua các ứng dụng nhắn tin như zalo, messenger, gmail,…	Đối với endpoint: Không cài phần mềm chặn các ứng dụng mạng xã hội, Không cài phần mềm theo dõi hoạt động người dùng Đối với network: Không có các hệ thống phân tích và phát hiện sự cố như SIEM, NDR. Không có cấu hình firewall chặn các kết nối ra bên ngoài mạng nội bộ	**5**	**0**	**0**	**5**	**3**	**5**	**1**	**4**	**20**

4. Phân tích những rủi ro hệ thống bị tấn công

Lỗ hổng	Rủi ro
Chưa có firewall chuyên dụng để bảo vệ thiết bị đầu cuối	Nếu một cuộc tấn công có chủ đích đến Domain-mail thì có thể attacker thực hiện tấn công thành công do thiếu firewall chuyên dụng bảo vệ Domain-mail
Hệ thống không phân vùng DMZ	Nếu các server bị nhiễm malware thì nó có thể lan ra vùng mạng nội
Hệ thống không sử dụng phần mềm antivirus	Khi có Virus xâm nhập vào hệ thống, nó có thể không bị phát hiện và được ngăn chặn kịp thời, dẫn đến hệ thống có thể bị tấn công và kiểm soát bởi attacker.
Hệ thống chưa có IDS/IPS	Nếu Attacker tấn công vào hệ thống, thì lúc này hệ thống không có nhận được cảnh báo, và ngăn chặn các hành vi độc hại.

Hệ thống chưa có sự phân chia các bộ phận quản lý trong công ty	khó khăn trong việc quản lý, nhân viên có thể truy cập vào bất kỳ dữ liệu nào của công ty mà không có sự kiểm soát truy cập rõ ràng nào.
Mạng wifi truy cập vào máy chủ	Nguy cơ xâm nhập trái phép Client kết nối vào mạng wifi có thể truy cập trực tiếp vào vùng máy chủ, tạo điều kiện cho tấn công nội bộ hoặc kẻ xấu có thể xâm nhập khi wifi bị bẻ khóa.

5. Phân tích những rủi ro trong quy trình sao lưu và phục hồi dữ liệu

- Hệ thống có 2 File Server chạy độc lập ở hai chi nhánh Hồ Chí Minh và Hà Nội mà không có cơ chế chạy song song để backup lẫn nhau dẫn đến việc khi một hoặc cả hai File Server bị hư hỏng thì không có dữ liệu để phục hồi và sử dụng.
- Khi dữ liệu được kết nối trực tiếp với máy Printer mà không có quá trình sao lưu thích hợp thì dữ liệu có thể bị mất do các vấn đề về kỹ thuật, lỗi phần mềm hoặc hư hỏng phần cứng.
- Cơ chế sao lưu dữ liệu của Windows Server 2003 không linh hoạt dẫn đến ảnh hưởng khả năng sao lưu dữ liệu và không đáp ứng được tính linh hoạt, nhanh chóng trong doanh nghiệp.
- Quy trình sao lưu được đặt trong cùng máy có các chức năng khác làm cho hiệu suất sao lưu không được ổn định, khi máy chủ bị hư hỏng do thiên nhiên hay bị tấn công thì sẽ không thể sao lưu được nữa.
- Dữ liệu được lưu trữ tại Storage nằm cùng một khu vực với các Server khác dễ dẫn đến việc bị mất mát, đánh cắp dữ liệu khi một trong các Server lân cận bị xâm nhập.
- Không có cấu hình chạy song song giữa 2 Storage dẫn đến việc mất mát dữ liệu không thể phục hồi nếu một trong hai máy bị hư hỏng.
- Sử dụng thiết bị NAS Thecus N8810U-G để lưu trữ dữ liệu backup: nếu nguồn điện bị ngắt đột ngột sẽ gây rối dữ liệu hoặc ảnh hưởng đến hoạt động của NAS Thecus N8810U-G.
- Nếu nơi đặt thiết bị NAS Thecus N8810U-G không được an toàn do điều kiện môi trường như độ ẩm, nhiệt độ, bụi bẩn dễ dẫn đến thiết bị NAS bị hư hỏng, ảnh hưởng đến hiệu suất hoạt động.
- Không có quy trình sao lưu định kỳ dẫn đến việc mất mát dữ liệu do lỗi phần cứng, do người dùng, hay các sự cố khác như hỏng ổ đĩa hoặc lỗi RAID.
- Không có quy định về vận hành hệ thống trong việc cấu hình firewall bảo vệ NAS Thecus N8810U-G dẫn đến việc bị tấn công từ các mối đe dọa như tấn công từ xa, quét cổng, dữ liệu độc hại được truyền vào NAS gây ra thất thoát dữ liệu, hư hỏng thiết bị, chiếm quyền kiểm soát.

6. Đề xuất các giải pháp hạn chế những rủi ro này

6.1. Rủi ro do người dùng

- Tổ chức đào tạo định kỳ cho nhân viên về an toàn thông tin, bao gồm cả nhận biết tấn công Social Engineering và Phishing.
- Nhân viên IT phải có kiến thức về bảo mật thông tin, kỹ thuật an ninh mạng, triển khai và duy trì được các biện pháp bảo mật.
- Triển khai phần mềm antivirus và anti-malware trên tất cả các máy tính và cập nhật đều đặn. Thiết lập chính sách cấm tải và cài đặt phần mềm không được phép từ nguồn không an toàn.

- Hạn chế việc sử dụng email và internet cho mục đích cá nhân và giới hạn việc tải về các file từ nguồn không an toàn hoặc mở các file từ các email lạ. Cảnh báo nhân viên về các mối đe dọa qua email (phishing) và cách nhận diện chúng.
- Đảm bảo rằng tất cả các hệ thống và phần mềm đều được cập nhật đều đặn với các bản vá mới nhất để ngăn chặn lỗ hổng bảo mật.
- Yêu cầu nhân viên giữ bí mật thông tin và dữ liệu của công ty. Ban hành các quy định và hình phạt cụ thể cho việc tiết lộ dữ liệu của công ty.
- Thiết lập một chính sách mật khẩu rõ ràng mà mọi nhân viên đều phải tuân thủ. Yêu cầu mật khẩu có độ dài tối thiểu, yêu cầu sử dụng chữ hoa, chữ thường, số và ký tự đặc biệt. Nhắc nhở nhân viên về tầm quan trọng của việc thay đổi mật khẩu định kỳ và cung cấp hướng dẫn về cách thực hiện điều này để giảm nguy cơ bị tấn công do sử dụng mật khẩu cũ quá lâu.
- Mọi nhân viên phải thực hiện thiết lập xác thực đa yếu tố cho các tài khoản trong hệ thống để tăng cường bảo mật khi đăng nhập tài khoản người dùng.
- Áp dụng chính sách quản lý thiết bị để giảm thiểu rủi ro mất mát hoặc đánh cắp thiết bị. Sử dụng mã hóa dữ liệu cho các thiết bị lưu trữ dữ liệu nhạy cảm. Thực hiện sao lưu dữ liệu định kỳ để ngăn chặn mất mát dữ liệu do xóa vô ý hoặc hỏng hóc.
- Xây dựng và thực hiện chính sách phân quyền rõ ràng để hạn chế quyền truy cập của nhân viên, nhân viên chỉ nên vào những gì cần thiết cho công việc của họ. Theo dõi và kiểm soát quyền truy cập định kỳ. Thiết lập hệ thống giám sát và theo dõi liên tục để phát hiện sớm các hoạt động bất thường.

6.2. Rủi ro do hệ thống bị tấn công

- Cần sử dụng các Firewall chuyên dụng như Fortigate hoặc Palo Alto cho các thiết bị để có thể ngăn chặn tấn công đến các thiết bị đó mà không bỏ qua bất kỳ dấu hiệu, hay trường hợp nào.
- Phân chia vùng DMZ để có thể bảo vệ được các vùng khác trong mạng nội bộ khỏi bị tấn công trực tiếp từ attacker
- Sử dụng thiết bị tìm kiếm, phát hiện và ngăn ngừa xâm nhập để nhận được cảnh báo và ngăn chặn tấn công từ attacker.
- Sử dụng thiết bị Antivirus trên tất cả máy chủ và client để có thể phát hiện và ngăn chặn Virus, Malware tồn tại trong hệ thống.
- Cần có chính sách kiểm soát, phân chia, quản lý việc truy cập dữ liệu cho nhân viên, họ nên có quyền truy cập vào những dữ liệu gì của công ty, chứ không phải là có thể truy cập được vào hết dữ liệu của công ty.
- Cấu hình VLAN riêng biệt cho wifi khách và wifi nội
- Triển khai IDP/IPS để giám sát và phát hiện sớm các cuộc tấn

6.3. Rủi ro trong quá trình sao lưu và phục hồi dữ liệu

- Cấu hình chạy song song cho hai máy File Server ở hai chi nhánh để dữ liệu hai bên đồng bộ với nhau nếu một trong hai máy bị hư thì vẫn còn dữ liệu để phục hồi.
- Xây dựng thêm một nơi để backup tất cả các dữ liệu từ các Server trong hai chi nhánh để có thể phục hồi dữ liệu nhanh chóng khi các máy Server bị hư hỏng.
- Thiết lập quy trình sao lưu hợp lý: thiết lập chính sách sao lưu thích hợp và sao lưu ở một nơi khác với máy in để đảm bảo an toàn dữ liệu.
- Storage nên được đặt ở một khu vực riêng với các Server trong môi trường an toàn và kết nối với các Server thông qua đường truyền VPN để giảm thiểu khả năng mất mát toàn bộ dữ liệu khi các Server khác bị tấn công.
- Cấu hình chạy song song cho hai máy Storage để dữ liệu được đồng bộ và có thể phục hồi khi một trong hai máy hỏng.

- Sử dụng nguồn điện dự phòng (UPS) dùng để cung cấp nguồn điện cho các thiết bị bị ngắt điện đột ngột hoặc bị giảm chất lượng nguồn điện.
- Thực hiện sao lưu định kỳ và giữ nhiều phiên bản sao lưu để có khả năng khôi phục dữ liệu từ nhiều thời điểm.
- Cấu hình Firewall quản lý quyền truy cập vào NAS Thecus N8810U-G chỉ cho phép kết nối từ các địa chỉ IP cụ thể hoặc giới hạn quyền truy cập theo các giao thức nhất định, cấu hình kiểm soát lưu lượng dữ liệu ra vào từ NAS để đảm bảo chỉ những dữ liệu cần thiết và an toàn được truyền qua mạng.