Phòng thí nghiệm An toàn Thông tin InsecLab

Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: QUẢN LÝ RỦI RO VÀ AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

Tên chủ đề: Risk Analysis, Evaluation, and Assessment in Network system

GVHD: Đỗ Thị Phương Uyên

Nhóm: 6

1. THÔNG TIN CHUNG:

Lớp: NT207.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Trần Minh Duy	21522010	21522010@gm.uit.edu.vn
2	Phạm Ngọc Thiện	21522627	21522627@gm.uit.edu.vn
3	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn
4	Huỳnh Nguyễn Uyển Nhi	21522424	21522424@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng
1	Phân tích Tính sẵn sàng của các dịch vụ trong hệ thống (Domain, File và Email)	100%
2	Phân tích tính sẵn sàng của hạ tầng mạng	100%
3	Phân tích những rủi ro dẫn đến mất mát thông tin do người dùng gây ra	100%
4	Phân tích những rủi ro hệ thống bị tấn công	100%
5	Phân tích những rủi ro trong qui trình sao lưu và phục hồi dữ liệu	100%
6	Đề xuất các giải pháp hạn chế những rủi ro này	100%
Điểm tự đánh giá		

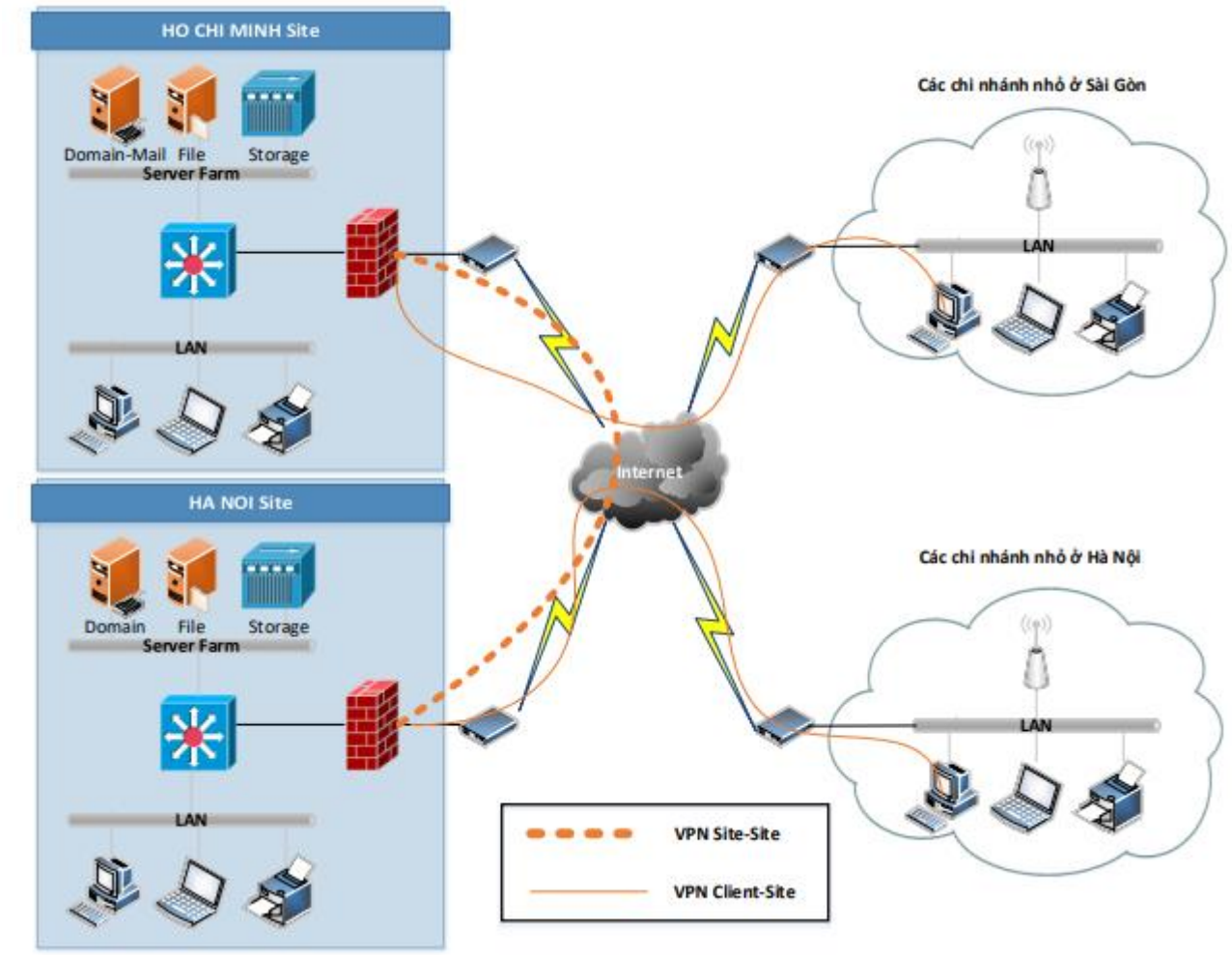
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

MỤC LỤC

BÁO CÁO CHI TIẾT

I. Mô hình mạng hiện tại



Hình 1 – Mô hình mạng doanh nghiệp hiện tại

- Công ty ABC có trụ sở chính đặt tại Hồ Chí Minh với 100 người dùng và chi nhánh lớn khác nằm ở Hà Nội khoảng 50 người dùng. Ngoài ra, tại Hồ Chí Minh và Hà Nội công ty còn có các chi nhánh nhỏ (HCM khoảng 15 chi nhánh nhỏ, HN khoảng 20 chi nhánh nhỏ). Mỗi chi nhánh dao động nhận viên từ 3 đến 10 người.

- Danh sách thiết bị:

STT	Thiết Bị	SL	Nơi Đặt	Serial Number
1	Server HP DL 380G5 (Domain - Email)	1	DC HCM	1
2	Server HP DL 380G5 (File)	1		2
3	Server HP DL 380G5 (Application)	1		3
4	NAS Thecus N8810U-G (Storage)	1		4
5	Core switch 3850G 24 port	1		5
6	Access switch 2960 PoE 48 port	4		6
7	HP Color LaserJet Pro MFP M476nw	2		7
8	HP LaserJet Enterprise Flow MFP M630z	1		8
9	Wireless N Access Point TL-WA801ND	5		9
10	Modem ADSL Draytek 3200	1		10
11	Server HP DL 380G5 (Domain)	1	DC HN	11
12	Server HP DL 380G5 (File)	1		12
13	Server HP DL 380G5 (Application)	1		13
14	NAS Thecus N8810U-G (Storage)	1		14
15	Core switch 3850G 24 port	1		15
16	Access switch 2960 PoE 48 port	4		16
17	HP Color LaserJet Pro MFP M476nw	2		17
18	HP LaserJet Enterprise Flow MFP M630z	1		18
19	Wireless N Access Point TL-WA801ND	5		19
20	Modem ADSL Draytek 2900 - Firewall	1		20
21	Access switch 2960 PoE 24 port	1	Mỗi chi nhánh	
22	HP LASERJET PRO 400 PRINTER M401N	1		
23	VIGOR 2830	1		

- Danh sách ứng dụng:

STT	Danh sách ứng dụng
1	Domain – Wink2k3
2	Exchange Email 2007 – Win2k3
3	File – Win2k3
4	Accounting Application
5	Client – Win7
6	MS Office
7	Những software thông dụng khác: skype, adobe, unikey, dropbox, yahoo, browser (IE, Firefox, Chrome),…

II. Quy trình vận hành hệ thống

- Tất cả các server chạy HDH: Windows Server 2003.
- Tất cả các client chạy HDH: Windown 7.
- Dịch vụ Domain: một máy chủ Primary Domain chạy tại trụ sở HCM và máy chủ Secondary Domain chạy tại HN.
- Dịch vụ Email: máy chủ exchange 2007, tất cả các client ở tất cả trụ sở và chi nhánh sẽ kết nối vào đây để gởi và nhận email.
- Dịch vụ File: trong hệ thống có 2 máy chủ file phân tán ở HCM và HN. Dữ liệu chạy độc lập không có cơ chế chạy song song để backup lẫn nhau.
- Dịch vụ in ấn: client kết nối trực tiếp vào máy Printer để in ấn.
- Firewall: sử dụng modem Vigor để làm firewall bảo vệ hệ thống.
- Ứng dụng đặc biệt: phần mềm kế toán.
- Qui trình kết nối internet của client: client truy cập internet trực tiếp tại trụ sở hay chi nhánh. Các client tại các chi nhánh phía Nam sẽ truy cập dữ liệu vào File tại HCM và các client tại các chi nhánh phía Bắc và Trung sẽ truy cập dữ liệu vào File tại HN.
- Qui trình sao lưu và phục hồi dữ liệu: sử dụng Windows Backup để backup dữ liệu, dữ liệu backup sẽ lưu tại Storage.
- Qui trình truy cập vào Data Center: sử dụng chìa khóa để vào. Trưởng phòng IT quản lý chìa khóa.
- Qui trình kết nối vào mạng nội bộ sử dụng dây mạng: client gắn dây mạng và truy cập bình thường, chưa có cơ chế kiểm soát.
- Qui trình kết nối vào mạng nội bộ sử dụng mạng không dây: client truy cập vào mạng wifi sử dụng Key. Khi truy cập client có thể truy cập vào vùng máy chủ. Vì hệ thống mạng là mạng phẳng, không chia VLAN.

III. Phân tích rủi ro ảnh hưởng đến tính sẵn sàng, bảo mật và toàn vẹn của dữ liệu

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

a, Tính sẵn sàng của Domain

- Có máy chủ Primary (ở Hồ Chí Minh) và Secondary Domain (ở Hà Nội) để dự phòng. Tuy nhiên, việc sử dụng Windows Server 2003 đã lỗi thời có thể gây ra các rủi ro về bảo mật và các vấn đề về khả năng tương thích.

- Không rõ cơ chế failover và sao lưu dữ liệu giữa Primary và Secondary Domain Controller, ảnh hưởng đến khả năng phục hồi khi xảy ra sự cố.
- Không có đề cập nào đến kế hoạch khắc phục thảm họa cho domain controllers, không có backup khác cho Domain, nếu cả hai máy chủ đều gặp sự cố, hệ thống có thể ngừng hoạt động hoàn toàn.

b, Tính sẵn sàng của File

- Hai file servers được đặt tại hai địa điểm khác nhau (Hồ Chí Minh và Hà Nội) nhưng hoạt động độc lập, không có cơ chế backup/mirror lẫn nhau, nguy cơ mất dữ liệu/không đồng bộ hoá dữ liệu. Từ đó dẫn đến khó khăn trong việc phục hồi dữ liệu khi cần thiết.
- Clients được kết nối đến file server gần nhất, không có cơ chế failover cho clients khi truy cập file và không có file server backup. Khi máy chủ File bị lỗi, các client tại vùng vị trí tương ứng sẽ không thể truy cập dữ liệu, dẫn đến downtime lớn.

c, Tính sẵn sàng của Email

- Dịch vụ Email cho phép kết nối từ tất cả các trụ sở và chi nhánh, tính sẵn sàng của dịch vụ phụ thuộc vào tính ổn định của máy chủ.
- Dịch vụ Email sử dụng máy chủ Exchange 2007, đã cũ, có thể gặp các vấn đề về bảo mật và tương thích.
- Không có thông tin về máy chủ Email dự phòng hoặc cơ chế backup/lưu trữ email, ảnh hưởng đến tính liên tục của dịch vụ khi máy chủ gặp sự cố.

→ Nhận xét chung:

- *Toàn bộ cơ sở hạ tầng dựa trên phần mềm lỗi thời (Windows Server 2003 và Exchange 2007 đã không còn được hỗ trợ), có thể gây ra các vấn đề nghiêm trọng về tính tương thích và tính bảo mật.*

- Sử dụng Windows Backup cho sao lưu là một giải pháp cơ bản, có thể không đủ để khôi phục nhanh chóng trong trường hợp xảy ra thảm họa. Dữ liệu backup cũng cần được bảo vệ và quản lý tốt hơn.

- Sử dụng chìa khóa để truy cập data center mà không có chính sách kiểm soát truy cập khác bổ sung → Dữ liệu có thể bị xóa, sửa đổi hoặc đánh cắp, tấn công vật lý dẫn đến mất mát thông tin, ảnh hưởng các máy chủ dịch vụ…

- Truy cập internet trực tiếp từ tất cả các địa điểm mà không có quy tắc và giám sát tường lửa toàn diện → Dịch vụ có thể bị ngừng hoạt động do tấn công (DDoS, malware, rò rỉ dữ liệu,…).

- Kết nối trực tiếp client tới máy in và server mà không có hệ thống kiểm soát truy cập mạng thích hợp → Khi một thiết bị client bị nhiễm malware, malware có thể tìm cách lây lan sang các thiết bị khác trong mạng, bao gồm cả máy chủ (kết nối mạng trực tiếp, chia sẻ tệp, …).

- Mạng thiếu phân đoạn Vlan → Tăng nguy cơ tấn công nội bộ, lây nhiễm malware, truy cập vào thông tin nhạy cảm và thực hiện hành động gây hại mà không bị phát hiện; Có thể dẫn đến tắc nghẽn lưu lượng khi nhiều thiết bị cùng truy cập ảnh hưởng khả năng cung cấp dịch vụ và trải nghiệm người dùng.

→ Đề xuất cải thiện:

- Nâng cấp tất cả các máy chủ lên phiên bản Windows Server được hỗ trợ.

- Cập nhật quy trình backup và recovery bằng các giải pháp hiện đại hơn mang lại khả năng khôi phục nhanh hơn.

- Triển khai cơ chế backup và chuyển đổi dự phòng thích hợp cho cả domain controllers và file servers.

- Với file servers, sử dụng giải pháp đồng bộ hóa dữ liệu thông minh và định kỳ, sao lưu thông tin phù hợp để đảm bảo tính nhất quán và an toàn của dữ liệu.

- Với email, chuyển sang phiên bản Exchange mới hơn hoặc xem xét các dịch vụ email dựa trên cloud được tích hợp high availability và disaster recovery; thiết lập chế độ sao lưu dữ liệu định kỳ và cải thiện cơ chế bảo mật để ngăn chặn sự cố và giảm thiểu nguy cơ mất dữ liệu.

- Triển khai hệ thống kiểm soát truy cập cho cả kết nối có dây và không dây để điều chỉnh và giám sát quyền truy cập vào tài nguyên mạng.

- Thiết lập chính sách truy cập data center nghiêm ngặt hơn để tăng cường bảo mật.

- Có cơ chế kiểm soát kết nối giữa client với printer và server, chia mạng thành các VLAN khác nhau để dễ quản lý lưu lượng truy cập, giới hạn quyền truy cập và tăng cường bảo mật, ngăn chặn nguy cơ tấn công từ bên trong.

2. Phân tích tính sẵn sàng của hạ tầng mạng

- Cơ sở hạ tầng Servers: Các máy chủ đang chạy Windows Server 2003, phiên bản này đã lỗi thời và không còn được hỗ trợ. Điều này gây ra rủi ro bảo mật đáng kể do thiếu bản cập nhật và bản vá lỗ hổng.

- Cơ sở hạ tầng Clients: Phía khách hàng chạy Windows 7 có thể gặp phải các lỗ hổng vì hệ điều hành này cũng đã hết hỗ trợ

- Cơ sở hạ tầng Services (Các dịch vụ): hệ thống các server cho service

  + Email: Máy chủ Exchange 2007 đã lỗi thời, gây ra các rủi ro về bảo mật và tương thích. Máy chủ Exchange duy nhất không có chuyển đổi dự phòng hoặc thiết lập tính sẵn sàng cao.

  + Domain: Không rõ cơ chế failover và sao lưu dữ liệu giữa Primary và Secondary Domain, không có kế hoạch backup - recovery và chuyển đổi dự phòng thích hợp.

  + File: Không có cơ chế backup/mirror lẫn nhau giữa các server, không có kế hoạch backup - recovery và chuyển đổi dự phòng thích hợp

  + Printer: Kết nối trực tiếp từ client đến máy in mà không có kiểm soát có thể dẫn đến sự cố bảo mật và làm gián đoạn dịch vụ in ấn.

- Thiết kế và phân đoạn mạng: Mạng dường như có kiến trúc phẳng(flat) và không có VLAN segmentation → kẻ tấn công có thể dễ dàng di chuyển trong mạng, có thể tiếp cận tất cả các dịch vụ và máy chủ trong hệ thống và thực hiện các cuộc tấn công.

- Kết nối mạng:

  + Kết nối bằng dây mạng: Gắn dây mạng và truy cập trực tiếp, thiếu cơ chế kiểm soát, dẫn đến việc truy cập không ủy quyền vào các tài nguyên mạng quan trọng.

  + Kết nối mạng không dây: Kết nối wifi sử dụng Key, có sự bảo mật hơn tuy nhiên client có khả năng truy cập trực tiếp vào vùng máy chủ vì mạng không dây được triển khai dựa trên mô hình mạng phẳng, không chia VLAN - môi trường không an toàn và không có cơ chế kiểm soát, có thể dẫn đến lỗ hổng bảo mật, tăng nguy cơ bị tấn công từ các đối tượng không ủy quyền.

  + Cơ chế thiết lập VPN không đủ, chỉ có VPN Client Hà Nội đến Site Hà Nội, VPN Client Hồ Chí Minh đến Site Hồ Chí Minh, và VPN giữa 2 Site, người dùng ở Hà Nội không thể truy cập tài nguyên của site Hồ Chí Minh một cách trực tiếp mà phải thông qua

VPN giữa hai site, điều này có thể làm giảm hiệu suất và khó khăn khi quản lý nhiều kết nối VPN (phức tạp và tốn thời gian, nhất là khi có sự cố xảy ra).

+ Không có đường truyền dự phòng, khi có sự cố có thể gây gián đoạn.

+ Tại mỗi Site chỉ có 1 CoreSW, nếu SW gặp sự cố sẽ gây gián đoạn.

- Firewall: sử dụng modem Vigor để làm firewall bảo vệ hệ thống, giải pháp này không đủ để đối phó với các mối đe dọa hiện đại, cần có giải pháp tường lửa phức tạp hơn.

- An ninh vật lý: Quy trình sử dụng truy cập vào Data Center là cơ bản, không có chính sách kiểm soát truy cập khác bổ sung như sử dụng access log điện tử hoặc xác thực đa yếu tố.

→ Đề xuất cải thiện:

- Nâng cấp hệ thống hạ tầng mạng: Nâng cấp hệ điều hành servers và clients lên phiên bản mới và được hỗ trợ để đảm bảo tính bảo mật cao hơn và nhận được các bản vá an ninh mới nhất.

- Với dịch vụ Email, chuyển sang phiên bản Exchange mới hơn hoặc dịch vụ dựa trên đám mây có tính dự phòng và tính sẵn sàng cao.

- Thiết lập cơ chế failover cho Primary và Secondary Domain và phát triển kế hoạch backup-recovery rõ ràng.

- Triển khai cơ chế sao lưu và mirror giữa các máy chủ file, cùng với kế hoạch phục hồi thích hợp.

- Chia mạng thành các VLAN khác nhau để giới hạn quyền truy cập và tăng cường bảo mật, ngăn chặn nguy cơ tấn công từ bên trong.

- Thiết lập thêm các đường truyền dự phòng cho các Site và chi nhánh, thêm CoreSW tại mỗi Site.

- Có thể đề xuất sử dụng cơ chế khác cho VPN, như VPN đa điểm hoặc Cloudflare,....

- Cải thiện kiểm soát truy cập vật lý bằng xác thực đa yếu tố và nhật ký điện tử, ...

- Cải thiện kiểm soát truy cập mạng (không dây và có dây) đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài nguyên nhạy cảm (phân quyền, xác thực 802.1X, MAC Address Filtering, sử dụng IDS/IPS, firewall, ghi log, ...) .

- Đầu tư vào giải pháp tường lửa cấp doanh nghiệp với các tính năng bảo vệ khỏi mối đe dọa hiện đại, nâng cao.

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

- Người dùng đặt mật khẩu quá yếu, dễ đoán thì thời gian brute force sẽ rất ngắn, hoặc với trường hợp đặt một loại mật khẩu cho rất nhiều tài khoản khác nhau, thì khi bị phishing và bị yêu cầu đăng nhập, attacker dễ dàng tấn công và đánh cắp thông tin, làm tăng nguy cơ mất dữ liệu.
- Người dùng không có đủ nhận thức về các mối đe dọa bảo mật, có thể là mục tiêu dễ bị lừa đảo qua các kỹ thuật như phishing hoặc social engineering, tiến hành cung cấp thông tin nhạy cảm cho attacker hoặc nhấn vào các đường dẫn độc hại đính kèm.
- Người dùng không có thói quen đăng xuất hoặc tắt máy tính sau khi sử dụng hay khi cần rời vị trí. Điều này tạo cơ hội cho người khác sử dụng tài khoản/máy tính mà không cần biết mật khẩu.
- Tải hay cài đặt các ứng dụng, tập tin không an toàn hoặc không được phép hay từ nguồn không đáng tin cậy.
- Người dùng tải hay cài đặt các ứng dụng, tập tin không an toàn hoặc không được phép hay từ nguồn không đáng tin cậy. Điều này tạo cơ hội cho malware xâm nhập vào hệ thống và thực hiện nhiều hành vi độc hại, từ ăn cắp thông tin đến điều khiển từ xa máy tính của nạn nhân.
- Người dùng kết nối và sử dụng các thiết bị như usb, thẻ nhớ, thiết bị lưu trữ di động khác... lỗi thời, không an toàn (có nhiễm malware) để copy dữ liệu. Khi kết nối vào hệ thống, malware có thể lây lan và ảnh hưởng đến toàn bộ mạng lưới, dẫn đến mất dữ liệu hoặc rò rỉ thông tin.
- Người dùng làm mất thiết bị (lap, điện thoại, USB,....) – thiết bị không có mã hoá dữ liệu, cài đặt mật khẩu hay kiểm soát truy cập thiết bị, bất kỳ ai tìm thấy thiết bị đều có thể truy cập vào dữ liệu nhạy cảm.
- Người dùng sử dụng thiết bị cá nhân không an toàn để truy cập hệ thống, có thể dẫn đến mất mát thông tin khi thiết bị này bị mất cắp hoặc bị tấn công.
- Người dùng chụp ảnh, nhắn tin, ghi màn hình, đính kèm tài liệu nội bộ gửi/chia sẻ ra bên ngoài (facebook, zalo,...) bằng mạng nội bộ. Kẻ tấn công có thể lợi dụng thông tin này để tấn công vào các hệ thống khác hoặc làm giảm uy tín của công ty.

- Người dùng sửa, xóa nhầm file của người dùng khác, chỉnh sửa hoặc xóa dữ liệu trong các tệp nhạy cảm mà không có sự phê duyệt hay sử dụng tài khoản không được phép để thay đổi tệp cấu hình hệ thống. Việc này không chỉ mất mát dữ liệu mà còn làm gián đoạn ảnh hưởng tính sẵn sàng của hệ thống, nếu hệ thống không có kiểm soát phiên bản hoặc sao lưu, việc khôi phục dữ liệu có thể trở nên rất khó khăn.
- Người dùng tải file có dung lượng quá lớn lên file server, sử dụng nhiều tài nguyên mạng và dung lượng của file server làm giảm hiệu suất của hệ thống, ảnh hưởng đến người dùng khác và gây ra tình trạng tắc nghẽn mạng.

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

- Sử dụng Windows Server 2003 và Windows 7, các phiên bản lỗi thời và không còn được hỗ trợ, tạo ra rủi ro về vấn đề bản vá bảo mật và cập nhật từ Microsoft. Điều này làm tăng nguy cơ bị tấn công qua các lỗ hổng như là "Token Kidnapping Local Privilege Escalation" có thể leo thang đặc quyền đối với Windows Server 2003 hay "Group Policy Privilege Escalation (MS16-072)" đối với Windows 7. Ngoài ra, nó cũng không đáp ứng được với thay đổi của công nghệ có thể trở nên không tương thích, ….
- Sử dụng dịch vụ Email Exchange 2007 đã lỗi thời và không còn được hỗ trợ, tạo ra rủi ro về vấn đề bản vá bảo mật và cập nhật, …
- Dữ liệu được sao lưu bằng Windows Backup và lưu trữ tại Storage, nhưng không cung cấp cơ chế sao lưu đồng thời và không có cơ chế kiểm tra tính toàn vẹn của dữ liệu sao lưu.
- Sử dụng chìa khóa để truy cập vào Data Center có thể tạo ra rủi ro khi không có sự kiểm soát chặt chẽ đối với việc quản lý chìa khóa và xác thực người dùng hay ghi log truy cập.
- Sử dụng modem Vigor làm firewall là một giải pháp bảo mật yếu, không đủ để ứng phó với các mối đe doạ hiện đại.
- Rủi ro từ dịch vụ in ấn khi client kết nối trực tiếp vào printer để in mà không có bất kì xác thực hay phân quyền:
    + Việc không xác thực kết nối dễ khiến cho attacker lời dụng để trà trộn vào khu vực nội bộ của công ty.

+ Vì không phân quyền nên attacker sau khi kết nối với máy in thì có thể dễ dàng để lại một số loại malware để thực hiện phá hoại và đánh cắp thông tin những người dùng khác.

- Rủi ro trong quy trình kết nối vào mạng nội bộ:

+ Sử dụng dây mạng: Gắn dây mạng và truy cập trực tiếp, thiếu cơ chế kiểm soát.

- Bất kỳ ai cũng có thể kết nối vào mạng nội bộ và có thể truy cập không ủy quyền vào các tài nguyên mạng quan trọng, dẫn đến việc đánh cắp thông tin, tiết lộ bí mật thương mại, hoặc thậm chí các hành vi phá hoại. Ví dụ: một thiết bị bên ngoài (laptop cá nhân, ...) được kết nối vào mạng, nó có thể chứa phần mềm độc hại, dẫn đến việc lây lan malware trong hệ thống.
- Nhân viên có thể sử dụng tài nguyên mạng cho các mục đích cá nhân, ảnh hưởng đến hiệu suất của hệ thống và vi phạm chính sách bảo mật của tổ chức.

+ Sử dụng mạng không dây: client truy cập vào mạng wifi sử dụng Key.

- Sử dụng mạng phẳng, không chia VLAN: Việc này làm tăng phạm vi tác động của malware nếu nó có tồn tại trên máy kết nối vào mạng nội bộ.
- Vì mã hóa dữ liệu không được đề cập nên mặc định là không có mã hóa dữ liệu, việc không có mã hóa dữ liệu làm cho dữ liệu được truyền ở dạng clear text, làm cho attacker có thể dễ dàng đọc được những thông tin nhạy cảm.
- Sử dụng key để đăng nhập: attacker tiến hành brute force hay social engineering để thu được key, hoặc cài key logger trên máy client để có được key cho từ đó attacker có thể truy cập vào mạng nội bộ. Ngoài ra, attacker có thể truy cập vào vùng máy chủ vì hệ thống sử dụng mạng phẳng, dẫn đến rủi ro cao nhất như làm sập hoàn toàn hệ thống và lấy hết thông tin hệ thống.

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

- Không rõ cơ chế Failover giữa Domain Controllers và thiếu kế hoạch khắc phục thảm họa cho Domain Controllers:

+ Không có cơ chế failover và sao lưu dữ liệu rõ ràng giữa Primary và Secondary Domain Controller, việc phục hồi khi xảy ra sự cố sẽ trở nên khó khăn hơn và có thể mất quyền truy cập vào các dịch vụ và dữ liệu quan trọng.

+ Không có đề cập nào đến kế hoạch khắc phục thảm họa cho domain controllers, không có backup/bản sao lưu khác cho Domain, nếu cả hai máy chủ đều gặp sự cố, hệ thống có thể ngừng hoạt động hoàn toàn.

- Hai file servers được đặt tại hai địa điểm khác nhau nhưng hoạt động độc lập, không có cơ chế backup/mirror lẫn nhau:

+ Nếu một trong hai máy chủ gặp sự cố, thông tin có thể bị mất mát hoặc bị hỏng và không thể khôi phục.

+ Việc không có cơ chế đồng bộ hóa giữa hai máy chủ có thể dẫn đến thông tin không nhất quán, gây khó khăn trong việc truy cập và sử dụng dữ liệu.

+ Không có chính sách quản lý và sao lưu dữ liệu giữa các chi nhánh (truy cập dữ liệu từ File tại Hồ Chí Minh hoặc Hà Nội) gây ra sự không đồng nhất có thể dẫn đến việc thiếu thông tin hoặc không chính xác khi cần phục hồi dữ liệu.

+ Không có file server backup, nếu cả hai máy chủ file đều gặp sự cố, các client tại vùng vị trí tương ứng sẽ không thể truy cập dữ liệu, dẫn đến downtime lớn, khó có thể khôi phục lại dữ liệu, ...

- Không có thông tin về máy chủ Email dự phòng hoặc cơ chế lưu trữ email làm cho dữ liệu email dễ bị mất mát trong trường hợp máy chủ gặp sự cố. Nếu không có bản sao lưu, các email quan trọng có thể không phục hồi được.

- Sử dụng Windows Backup để backup dữ liệu, dữ liệu backup lưu tại Storage có thể không đủ tài nguyên để phục hồi nhanh chóng:

+ Windows Backup quá cơ bản và không đủ, không có các tùy chọn sao lưu đồng thời hoặc không đáp ứng được các yêu cầu cụ thể về sao lưu dữ liệu hiệu quả trong một môi trường hệ thống lớn (sao lưu gia tăng, sao lưu dành riêng cho ứng dụng (ví dụ: dành cho Exchange hoặc SQL Server),...).

+ Quy trình sao lưu dữ liệu hiện tại không có sự linh hoạt trong việc xác định lớp ưu tiên cho dữ liệu. Điều này có thể dẫn đến việc mất dữ liệu quan trọng nếu không có chiến lược sao lưu đa lớp (như sao lưu định kỳ, sao lưu thường xuyên và sao lưu toàn bộ hệ thống).

+ Quy trình sao lưu hiện tại không được tự động hoá, có nguy cơ xảy ra lỗi hoặc do thiếu sót của con người dẫn đến các bản sao lưu bị lỗi thời hoặc bị thiếu, việc mất dữ

liệu đáng kể có thể xảy ra giữa lần sao lưu cuối cùng và khi xảy ra thảm họa, ảnh hưởng đến Recovery Time Objective (RTO) and Recovery Point Objective (RPO) → Quá trình phục hồi kéo dài có thể dẫn đến thời gian ngừng hoạt động không thể chấp nhận được đối với doanh nghiệp, ảnh hưởng đến hoạt động và năng suất.

+ Các bản sao lưu và quy trình khôi phục không được xác minh và kiểm tra thử nghiệm thường xuyên, không có gì đảm bảo rằng các bản sao lưu có thể phục hồi được khi có sự cố.

+ Không rõ ràng về môi trường lưu trữ dữ liệu sao lưu tại Storage. Không có biện pháp bảo vệ đối với Storage, dữ liệu sao lưu có thể dễ dàng bị mất hoặc hỏng khi xảy ra sự cố về an ninh hoặc hỏng hóc của thiết bị lưu trữ.

+ Không có cơ chế mã hoá cho các dữ liệu được sao lưu điều này gây rủi ro rò rỉ thông tin dữ liệu nếu phương tiện lưu trữ bị đánh cắp hoặc bị xâm phạm.

+ Không có đề cập đến việc kiểm soát quyền truy cập an toàn vào dữ liệu sao lưu, điều này chỉ được hạn chế đối với những người có thẩm quyền.

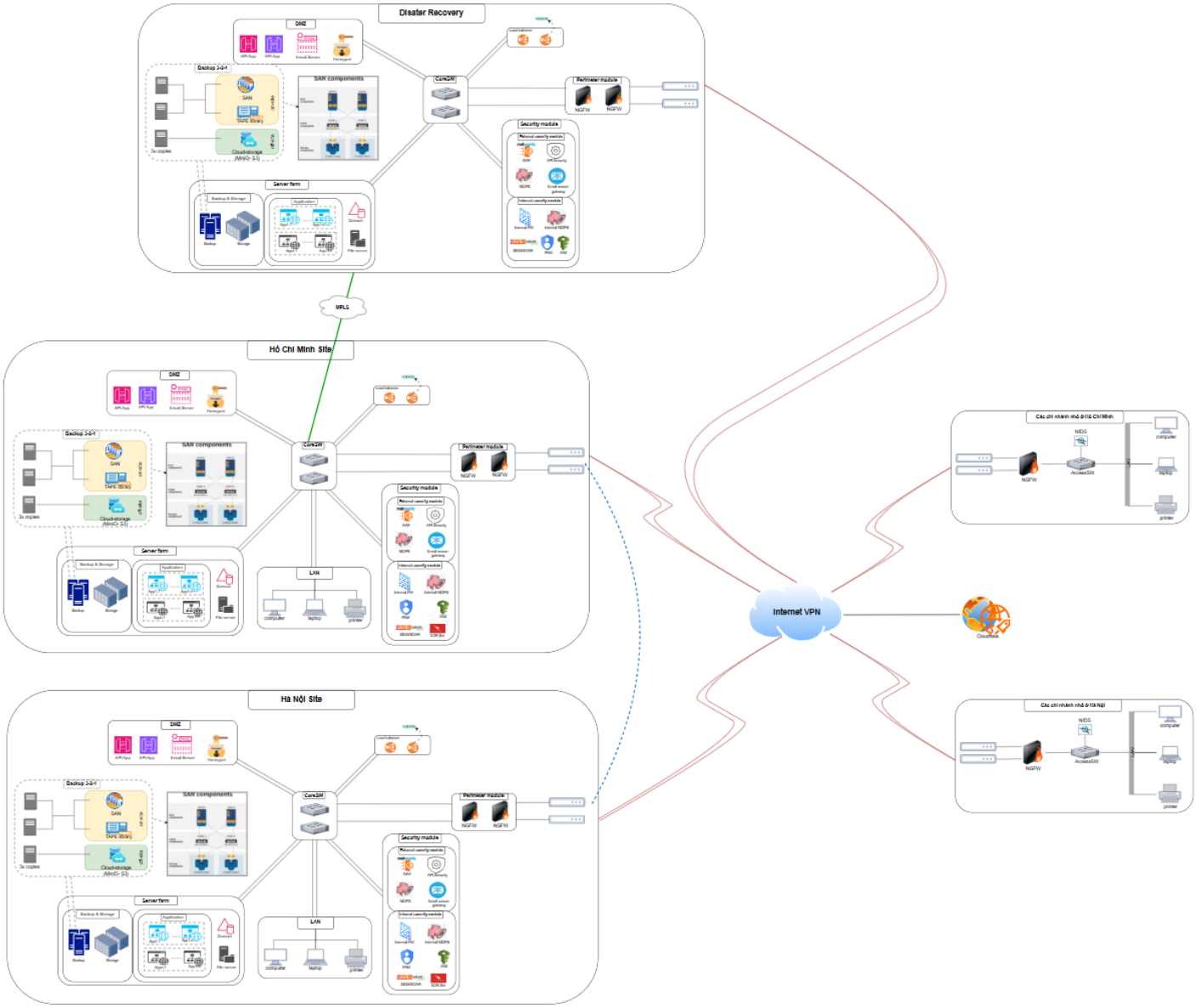
+ Không có cơ chế dự phòng khác cho Backup & Storage, các bản sao lưu được lưu trữ ở cùng một vị trí vật lý với dữ liệu gốc dễ bị ảnh hưởng bởi các thảm họa cụ thể tại địa điểm như hỏa hoạn, lũ lụt hoặc mất điện.

- Không có đề cập nào đến kế hoạch khắc phục thảm họa chính thức nêu ra các bước và thủ tục cụ thể cho các tình huống khác nhau, khó để ứng phó kịp thời và hiệu quả.

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

***a, Nhóm thực hiện đề xuất một mô hình khác như sau*:**

(https://app.diagrams.net/#G1saBLBtL06DJ9pfhK8O6YOlbzIYWV2X4Z#%7B%22pageId%22%3A%22pZI4d5OnLfmEyIZo0S2G%22%7D):



Hình 2 – Mô hình mới

→ Các thành phần trong mô hình mới như sau:

STT	Giải pháp	SL	Vị trí triển khai	Mục đích
1	Next Generation Firewall	01	Trong vùng mỗi chi nhánh	NGFW (Next-Generation Firewall) kết hợp nhiều tính năng của tường lửa truyền thống như lọc gói tin, NAT, PAT, chặn URL và VPN, đồng thời cung cấp QoS và các chức năng nâng cao khác như: ngăn chặn tấn công xâm nhập, kiểm tra SSL/SSH lưu lượng mã hoá, kiểm tra sâu gói tin (DPI) và phát hiện phần mềm độc
		03	Trong vùng mỗi Site và Disater Recovery 02 cái trước CoreSW, 01 cái	

			trong Internal Security Module	hại, quản lý lưu lượng ứng dụng và bảo vệ các Layer IOS 4-7, kiểm soát luồng thông tin,…
2	Load Balancer	02	Trong vùng mỗi Site và Disater Recovery	Phân phối đồng đều lưu lượng truy cập giữa nhiều máy chủ để giảm tải cho từng máy. Tự động chuyển hướng lưu lượng khi một máy chủ gặp sự cố, đảm bảo dịch vụ luôn hoạt động. Tối ưu hóa hiệu suất hệ thống, giảm độ trễ và nâng cao trải nghiệm người dùng.
3	IDS/IPS	01	Trong vùng mỗi chi nhánh, cài trên SW	Dùng để giám sát traffic đến và đi từ tất cả các thiết bị mạng trong vùng mỗi Chi nhánh, tích hợp với các bộ rule để cảnh báo và gửi log, netflow về SIEM.
		02	Trong vùng mỗi Site, tại Internal và External Security Module	IPDS chuyên dụng để theo dõi các hoạt động bất thường, xác định ai/như thế nào/vị trí nào trên hệ thống mạng bị tác động và kết hợp với firewall để ngăn chặn kịp thời các hoạt động xâm nhập hệ thống. Internal Security Module để cho vùng nội bộ (LAN, Server Farm), Internal Security Module cho DMZ…
		02	Trong vùng DR sau NGFW	
4	API Security		Trong External Security Module cho DMZ tại mỗi Site	API được đặt tại DMZ. API Security bảo vệ các API thông qua xác thực, mã hóa dữ liệu khi truyền tải, giới hạn tần suất để ngăn tấn công từ chối dịch vụ, và giám sát hành vi bất thường.
5	Email Secure Gateway		Trong External Security Module cho DMZ tại mỗi Site	Email Secure Gateway bảo vệ hệ thống email khỏi spam và phishing,… sử dụng mã hóa để bảo vệ thông tin nhạy cảm, chống virus và phần mềm độc hại, cùng với kiểm soát chính sách để thực thi các quy định bảo mật.

6	Web Application Firewall	01	Trong External Security Module cho DMZ tại mỗi Site	Vùng DMZ chứa các ứng dụng web và máy chủ public ra Internet, có nguy cơ cao bị khai thác. WAF theo dõi và bảo vệ lưu lượng HTTP/HTTPS, thực hiện chính sách bảo mật dựa trên dấu hiệu tấn công và lưu lượng truy cập, nhằm ngăn chặn các mối đe dọa cho ứng dụng web.
		01	Trong External Security Module cho DMZ tại DR	
7	SIEM/SOAR (Splunk/ Splunk Phantom)	01	Trong Internal Security Module cho vùng mạng nội bộ tại vùng mỗi Site và DR	SIEM thu thập, phân tích và lưu trữ dữ liệu security từ nhiều nguồn, giúp phát hiện và phản ứng với các mối đe dọa, cung cấp giám sát thời gian thực và báo cáo. SOAR giúp t ự động hóa quy trình phản ứng với sự cố an ninh, tích hợp với các công cụ để giảm thời gian phản ứng và cải thiện hiệu quả xử lý sự cố.
8	PAM/IAM	01	Trong Internal Security Module cho vùng mạng nội bộ tại vùng mỗi Site và DR	PAM quản lý quyền truy cập của người dùng có quyền cao, ngăn ngừa lạm dụng quyền và giám sát ghi lại hoạt động. IAM quản lý danh tính và quyền truy cập của người dùng trong tổ chức, đảm bảo rằng chỉ những người dùng được phép mới được truy cập vào các tài nguyên và dữ liệu nhạy cảm, cung cấp khả năng xác thực, phân quyền và theo dõi hoạt động người dùng.
9	Endpoint Security (EDR)		Agent - Trên tất cả các thiết bị endpoint (Printer không cài được)	Phòng chống Virus, Spyware và các phầm mềm độc hại khác. Phòng chống Virus, Spam và lọc nội dung Mail. Bảo vệ dữ liệu trước nguy cơ mất cắp thông qua các thiết bị ngoại vi (USB, DVDs,...). Cảnh báo người dùng về độ an toàn của Website khi truy cập

		01	Server - Trong Internal Security Module cho vùng mạng nội bộ tại vùng mỗi Site và DR	Xử lý và phân tích dữ liệu từ nhiều agent, phát hiện các mối đe dọa nâng cao, cung cấp báo cáo và cảnh báo, đồng thời hỗ trợ phản ứng tự động hoặc thủ công với các sự cố an ninh.
10	Honeypot	01	Trong DMZ tại mỗi vùng Site và DR	Honeypot giả lập môi trường dễ bị tấn công nhằm thu hút và phân tích hành vi của kẻ tấn công, phát hiện mối đe doạ và tăng cường an ninh cho hệ thống thực bằng cách phân tách hoạt động độc hại.
11	Storage	02	Trong DMZ tại mỗi vùng Site và DR	Dùng để lưu các mã nguồn của website, app, các dữ liệu khác,...
12	Backup		Trong DMZ tại mỗi vùng Site và DR	Đảm bảo khả năng phục hồi dữ liệu khi xảy ra sự cố, như tấn công ransomware hoặc lỗi phần cứng, giúp tổ chức duy trì hoạt động liên tục và bảo vệ thông tin quan trọng, sử dụng cơ chế Backup 3:2:1 và SAN (StorageAreaNetwork).
13	Cloudflare	01		Hạn chế được sự tấn công của DDoS, spam. Che giấu địa chỉ IP,...

→ Các điểm mới trong mô hình:

- Disaster recovery riêng biệt, giúp đảm bảo RPO và GPO của hệ thống trong trường hợp cả 2 bản backup ở 2 Site bị hư hại hay phá hoại.
- Load balancing và API ở các Site: đảm bảo tính khả dụng của hệ thống, cân bằng tải và tối ưu hóa hiệu suất hệ thống, giảm độ trễ và nâng cao trải nghiệm người dùng.
- Ban đầu cơ chế Windows Backup quá cơ bản và không đủ, không có các tùy chọn sao lưu đồng thời, sao lưu định kỳ,...vv... Cơ chế backup 3:2:1 với công nghệ SAN và Tape Library giúp đảm bảo an toàn cho dữ liệu backup, bản onsite hỗ trợ nhanh và kịp thời

khi có sự cố đồng thời suy trì phiên bản dự phòng offsite ở cloud giúp đáp ứng được khi 2 bản onsite gặp sự cố.

Nếu doanh nghiệp có khoảng 250 nhân viên và chủ yếu cần lưu trữ, chia sẻ file, thực hiện sao lưu dữ liệu, cũng như cung cấp truy cập thông qua mạng LAN, thì NAS có thể là lựa chọn phù hợp. NAS thường dễ cài đặt và quản lý, rất phổ biến trong các môi trường văn phòng nhỏ và vừa. Tuy nhiên, nếu doanh nghiệp cần lưu trữ dữ liệu cho các ứng dụng yêu cầu hiệu suất cao, như hệ thống cơ sở dữ liệu lớn, ảo hóa server, hoặc các ứng dụng cần I/O cao và khả năng mở rộng trong tương lai, thì SAN nên được ưu tiên. SAN (Storage Area Network) là một mạng chuyên dụng kết nối các thiết bị lưu trữ với máy chủ, cho phép nhiều máy chủ truy cập vào ổ đĩa cứng và băng từ qua mạng tốc độ cao và độ trễ thấp. SAN linh hoạt trong việc thêm hoặc bớt storage, đồng thời bảo vệ dữ liệu bằng các biện pháp như mã hóa, sao lưu, phục hồi và sao chép. Hệ thống này ngăn chặn sự can thiệp của người dùng hoặc máy chủ không được phép, đồng thời cho phép quản lý storage từ một điểm trung tâm, giúp giảm thiểu chi phí và công sức cho nhân viên IT. Ngoài ra, SAN còn hỗ trợ theo dõi và giám sát hiệu suất cũng như tình trạng của hệ thống lưu trữ

- Cloudflare: Che dấu địa chỉ IP, hạn chế các tấn công mạng như DDoS, spam,…
- Honeypot giả lập môi trường dễ bị tấn công nhằm thu hút và phân tích hành vi của kẻ tấn công, phát hiện mối đe doạ và tăng cường an ninh cho hệ thống thực bằng cách phân tách hoạt động độc hại.
- IAM/PAM siết chặt quản lý danh tính và quyền truy cập của toàn bộ người dùng trong hệ thống, phân quyền và hạn chế lạm dụng quyền hạn, bản vệ tài nguyên và thông tin.
- SIEM/SOAR: thu thập và phân tích dữ liệu từ nhiều nguồn để phát hiện các mối đe dọa an ninh trong thời gian thực và tự động hóa quy trình phản ứng với sự cố, giúp giảm thời gian phản ứng và tăng cường hiệu quả xử lý sự cố.
- EDR/Endpoint security: Phòng chống virus, spyware và phần mềm độc hại với phần mềm diệt virus. Lọc email để ngăn chặn spam và nội dung độc hại. Bảo vệ dữ liệu trên thiết bị ngoại vi như USB và DVDs. Cảnh báo người dùng về độ an toàn của các trang web. Phân tích dữ liệu từ nhiều nguồn để phát hiện mối đe dọa, cung cấp báo cáo và hỗ trợ phản ứng với sự cố an ninh.

b, Các chính sách đi kèm

- Chính sách nội bộ công ty:

+ Xây dựng được một document mô tả toàn bộ hệ thống mạng của công ty. Trong tài liệu phải đề cập đầy đủ và chi tiết về các thiết bị, các kết nối giữa các thiết bị, các địa chỉ IP trên các thiết bị, các giải thuật định tuyến sử dụng trong mạng,....

+ Tài liệu hoá và chi tiết hoá về việc truy cập vào dịch vụ mạng của các user như: các ứng dụng mạng được phép sử dụng, các trang web được phép truy cập, thời gian truy cập, ngăn chặn download các định dạng file cụ thể để tránh làm giảm hiệu năng mạng,...

+ Đào tạo nhân viên: Tổ chức các buổi đào tạo định kỳ cho nhân viên về chính sách bảo mật, quy trình sử dụng hệ thống và nhận thức về an ninh thông tin.

+ Cập nhật tài liệu: Đảm bảo tài liệu mô tả hệ thống mạng được cập nhật thường xuyên để phản ánh những thay đổi trong hạ tầng hoặc chính sách.

- Chính sách quản lý thông tin:

+ Thông tin bình thường:

- Sử dụng, truy xuất các thiết bị lưu trữ: Nhân viên được tùy ý sử dụng, trao đổi ngoài giờ làm việc.
- Hủy dữ liệu trong các thiết bị: Xóa bình thường, không bắt buộc phải format.

+ Thông tin nhạy cảm:

- Gán nhãn và lưu trữ: Do trưởng phòng, nhân viên được ủy quyền lưu trữ.
- Sử dụng, truy xuất các thiết bị lưu trữ: Cần phải có sự đồng ý của cấp trên của nhân viên mới có thể sử dụng hay mang ra ngoài.
- Hủy dữ liệu trong các thiết bị: Thiết bị lưu trữ cần được format lại, cần có quy trình huỷ rõ ràng với từng loại dữ liệu (dữ liệu phần mềm, dữ liệu phần cứng,...).
- Các nhân viên phải đảm bảo rằng tất cả các thông tin nhạy cảm ở dạng bản cứng hoặc tài liệu điện tử phải an toàn trong khu vực làm việc của mình.
- Máy tính của mỗi nhân viên phải được khóa lại khi không làm việc hoặc rời khỏi chỗ làm việc và được tắt hoàn toàn khi hết giờ làm việc.

- Những tài liệu lưu hành nội bộ không được để trên bàn làm việc mà phải được cất trong một ngăn kéo và được khóa cẩn thận khi nhân viên đi ra ngoài hoặc khi hết giờ làm việc.
- Nhân viên không được viết mật khẩu cá nhân của mình lên giấy dán, notebook, hay những vị trí dễ tiếp cận khác.
- Nhân viên không được phép tiết lộ mật khẩu tài khoản của mình cho người khác hoặc cho phép những người khác sử dụng tài khoản của minh, bao gồm cả gia đình khi đang thực hiện công việc tại nhà.
- Nhân viên không được tự ý tiết lộ các thông tin liên quan đến công ty trên các trang blog, trên các mạng xã hội như Facebook, Twitter,…
- Các văn bản, giấy tờ quan trọng phải được lấy ra khỏi máy in ngay lập tức sau khi in xong.
- Thiết lập hệ thống ghi nhận việc sử dụng và truy cập các thiết bị lưu trữ để đảm bảo tính minh bạch.

+ Thông tin mật:

- Gán nhãn và lưu trữ: Phó giám đốc trở lên hoặc người được ủy quyền lưu trữ.
- Sử dụng, truy xuất các thiết bị lưu trữ: Cần được xác nhận của Phó Giám đốc trở lên. Thiết lập quy trình phê duyệt rõ ràng cho việc truy cập và sử dụng thông tin nhạy cảm, bao gồm các hình thức yêu cầu và phê duyệt.
- Hủy dữ liệu trong các thiết bị: Cần có quy trình huỷ rõ ràng với từng loại dữ liệu (dữ liệu phần mềm, dữ liệu phần cứng,…), đảm bảo không thể khôi phục lại.
- Thông tin cá nhân, username, password được lưu trữ trong các server phải được đặt trong những phòng đặc biệt, được khóa chắc chắn và được giám sát liên tục qua camera, chỉ có nhân viên IT phụ trách mới được phép tiếp cận.
- Các văn bản, giấy tờ quan trọng phải được lấy ra khỏi máy in ngay lập tức sau khi in xong.
- Tất cả dữ liệu mật được lưu trữ trong các thiết bị ngoại vi đều phải được mã hóa và đặt password.

- Bảng trắng được sử dụng trong các cuộc hội họp cần phải được xóa sạch ngay sau khi cuộc họp kết thúc.
- Thực hiện mã hóa cho tất cả thông tin nhạy cảm khi lưu trữ và truyền tải, nhằm bảo vệ thông tin khỏi truy cập trái phép.
- Thiết lập hệ thống giám sát để theo dõi và ghi log các hoạt động truy cập vào thông tin mật, giúp phát hiện các hành vi bất thường.
- Thực hiện đánh giá định kỳ về quy trình quản lý thông tin mật để phát hiện và khắc phục các lỗ hổng bảo mật.

+ Thông tin tuyệt mật:

- Gán nhãn và lưu trữ: Giám đốc trở hoặc người được ủy quyền lưu trữ.
- Sử dụng, truy xuất các thiết bị lưu trữ: Chỉ có Giám đốc trở lên mới có thể quyết định.
- Thiết lập quy định nghiêm ngặt về việc chia sẻ thông tin tuyệt mật, chỉ cho phép những người có quyền truy cập thực hiện điều này.
- Hủy dữ liệu trong các thiết bị: Hủy cả dữ liệu lẫn thiết bị. Tất cả các tài liệu, giấy tờ sau khi không còn được sử dụng phải được băm nhỏ trong máy cắt giấy và thùng xử lý dữ liệu bí mật phải được khóa cẩn thận.
- Bảng trắng được sử dụng trong các cuộc hội họp cần phải được xóa sạch ngay sau khi cuộc họp kết thúc.
- Tất cả máy in và máy fax phải được xóa hết dữ liệu, giấy tờ ngay sau khi chúng được in.
- Tất cả thông tin tuyệt mật của công ty được lưu trữ phân tán trên hai fileserver, được phân quyền và giới hạn truy cập chặt chẽ, gán nhãn tự động, cho phép người gửi phân quyền tương tác với nội dung cho người nhận như: cấm in tài liệu, cấm chuyển email cho người khác, thiết lập thời gian hết hạn của tài liệu và được tự động mã hóa.
- Đặt hệ thống giám sát an ninh để theo dõi các khu vực lưu trữ thông tin tuyệt mật, đảm bảo không có truy cập trái phép.

- Chính sách quản lý truy cập:

+ Quản lý hệ điều hành và ứng dụng, các tài nguyên:

- Mỗi nhân viên trong công ty sẽ được cấp một tài khoản để đăng nhập vào hệ thống máy tính của công ty. Password để đăng nhập vào tài khoản máy tính của công ty phải đảm bảo đủ mạnh và phức tạp, không để mặc định và phải được đổi định kỳ; các nhân viên phải tự bảo quản không để mất mát, rò rỉ. Nếu bị mất hoặc bị lộ phải báo với nhân viên IT để giải quyết.
- Các nhân viên không được phép tiết lộ mật khẩu tài khoản của mình cho người khác hoặc cho phép những người khác sử dụng tài khoản của minh, bao gồm cả gia đình khi đang thực hiện công việc tại nhà. Nếu nhân viên không còn làm việc tại công ty nữa thì tài khoản của nhân viên đó sẽ bị xóa khỏi hệ thống/vô hiệu hoá hoàn toàn, toàn diện.
- Quy định rõ quy tắc kiểm soát truy cập và quyền cho từng người và từng nhóm. Tạo các chính sách cho các user và group trong domain theo từng phòng ban cụ thể. Đưa ra các mức độ cảnh cáo đối với các user cố tình sai quy định.
- Cấp quyền phù hợp với user dựa vào vị trí của nhân viên trong công ty, phòng ban làm việc, và nhu cầu của công việc đó, và mức độ bảo mật của tổ chức. Mức độ sử dụng mật khẩu phải tuân thủ các chính sách mật khẩu.
- Quy định số lần tối đa đăng nhập sai cho các user là 3 lần, nếu quá 3 lần thì user sẽ bị khóa trong 30 phút, ghi lại tất cả hoạt động để theo dõi.
- Thiết lập chặt các user nào chỉ được phép truy cập từ máy nào, và theo dõi hoạt động đăng nhập này, có cơ chế log off sau 5 phút user không hoạt động hoặc phù hợp hơn để tránh khỏi việc sử dụng trái phép user khác trên hệ thống.
- Xác định quyền cụ thể trên file server cho các phòng ban. Quy định phòng ban này không được phép truy cập vào tài nguyên, tài liệu của phòng ban khác. Điều này tiềm ẩn nguy cơ về đánh cắp thông tin nên phải có mức độ cảnh cáo phù hợp.
- Mọi hoạt động của người dùng trong hệ thống đều sẽ được ghi log lại.
- Cấp ID cho nhân viên khi mới vào làm. Có văn bản ký kết giữa nhân viên được cấp ID với tổ chức về việc hiểu rõ các quyền mà ID đó được phép, đảm bảo nó bị cấm trước khi được ký kết các điều khoản với người dùng. Kiểm tra đảm bảo chỉ cung cấp đủ các ID cần thiết cho mỗi nhân viên.
- Quản lý quyền vào ra các phòng ban, phòng máy với ID của nhân viên.

- Khi người dùng các ID thay đổi vị trí công tác, cần thay đổi ngay lập tức các quyền phù hợp với công việc hiện tại.

+ Quản lý truy cập mạng:

- Theo dõi về giờ đăng nhập hệ thống của user để ngăn chặn những truy cập không cần thiết ngoài giờ hành chính.
- Tắt các port không sử dụng tránh sự đột nhập trái phép.
- Thiết lập cơ chế mã hóa kênh truyền bằng IPSec,... policy để tăng tính bảo mật thông tin. Phân vùng mạng và thiết lập rule giữa các phòng ban.
- Xây dựng hệ thống chứng thực và cấp cho người dùng và các đối tác có nhu cầu trao đổi từ xa và giữa các chi nhánh tránh việc giả mạo.
- Thiết lập quy trình làm việc từ xa, quy định rõ những user nào được phép truy cập từ xa như giám đốc, quản trị viên, phải sử dụng VPN,....
- Chỉ cho phép truy cập từ các địa điểm cụ thể (ví dụ: văn phòng, địa điểm làm việc từ xa đã được phê duyệt).
- Khi user gửi nhận mail yêu cầu phải có mã hóa và sử dụng chữ ký số được cấp và attach file không quá dung lượng nhất định.
- Cấu hình định tuyến trên router đảm bảo cho luồng thông tin không vi phạm vào các chính sách.
- Khi các máy tính lạ được kết nối vào công ty phải đảm bảo máy tính đó là an toàn, cài đặt đầy đủ và có bản update mới nhất của phần mềm diệt virus.
- Thiết lập quy trình kiểm tra và xác minh thiết bị trước khi cho phép kết nối vào mạng công ty. Thực hiện chính sách BYOD (Bring Your Own Device) với quy định rõ ràng về bảo mật và quản lý thiết bị cá nhân kết nối vào mạng.
- Thiết lập hệ thống giám sát để ghi lại mọi hoạt động mạng, bao gồm thời gian đăng nhập, địa chỉ IP, và các hành động được thực hiện.

- Chính sách về quản lý thiết bị:

+ Đối với các hệ thống, giải pháp:

- Còn được hỗ trợ từ các nhà phân phối (thông tin vá lỗi, thời gian cập nhật, nâng cấp, kênh thông tin hỗ trợ kỹ thuật...), không sử dụng các phiên bản quá cũ đã ngưng hỗ trợ.

- Có khả năng tương thích với các sản phẩm của bên thứ 3, dễ mở rộng module.
- Phù hợp khả năng vận hành và sử dụng hệ thống của người quản trị (thói quen, kỹ năng sử dụng, tính tiện dụng).

+ Các yêu cầu về cài đặt, cấu hình khác:

- Xoá/Đặt lại hết tất cả các cấu hình setting hay mật khẩu mặc định.
- Đảm bảo về chính sách mật khẩu, mật khẩu phải phức tạm và được thay đổi định kỳ. Có thể sử dụng cơ chế MFA hay passwordless để thay thế nhằm giảm việc bị lộ password.
- Điều chỉnh, tối ưu hóa các thông số mạng, đóng các port không cần thiết.
- Gỡ bỏ, vô hiệu hóa các dịch vụ DHCP, DNS, FTP, WINS, SMTP, NNTP, Telnet và các dịch vụ không cần thiết khác nếu không có nhu cầu sử dụng.
- Có cơ chế điều khiển truy cập, giới hạn dung lượng upload file theo user/group.
- Các dịch vụ đang chạy thiết lập với tài khoản có quyền tối thiểu.
- Sử dụng kết nối SSH, SFTP,… thay cho các kênh kết nối không an toàn như Telnet, FTP, v.v...
- Gỡ bỏ các tài khoản chưa sử dụng khỏi máy chủ.
- Đổi tên tài khoản Administrator và thiết lập mật khẩu mạnh.
- Gỡ bỏ tất cả các chia sẻ không sử dụng, các chia sẻ khác phải được phân quyền cho user/group rõ ràng (trên các server).
- Tất cả hoạt động, thao tác đều được ghi log và lưu trữ cẩn thận, các file log được lưu riêng trong hệ thống, xác định rõ thời gian lưu trữ định kỳ.
- Thường xuyên cập nhật các phiên bản mới nhất cho các phần mềm.
- Theo dõi thông tin cập nhật từ nhiều nguồn khác nhau.
- Nên triển khai cập nhật trên hệ thống thử nghiệm trước khi cập nhật vào hệ thống thật.
- Chỉ có nhân viên quản trị hệ thống/quản trị mạng/kỹ thuật/bảo trì mới được thực hiện các công việc trên. Trong trường hợp nhân viên bảo trì từ ngoài tổ chức thì cần có người giám sát quá trình này.

+ Yêu cầu về vị trí khu vực triển khai:

- Đối với những thiết bị đặt trong công ty: Yêu cầu tách biệt về không gian, dành riêng 1 phòng để đặt. Thiết bị phải được duy trì hoạt động trong điều kiện nhiệt độ thấp, lắp đặt các hệ thống làm mát, tản nhiệt giúp thiết bị nâng cao tuổi thọ và hiệu năng làm việc cao hơn. Sử dụng hệ thống ổn áp và lưu điện và máy phát điện giúp cho hệ thống server và các thiết bị khác không bị ảnh hưởng khi có sự cố về điện.
- Đảm bảo tiêu chuẩn an toàn của data center trước khi thuê, hợp đồng rõ ràng về những rủi ro vật lý có thể xảy ra, có kênh liên lạc hỗ trợ giữa doanh nghiệp và data center.
- Quản lý, giám sát việc ra vào tại những khu vực riêng biệt này (bằng thẻ từ có ID được cấp cho nhân viên liên quan). Chỉ cho phép những người có trách nhiệm liên quan mới được phép vào. Mỗi lần ra vào phải có ghi chép thời gian, lý do (bảo trì, sữa chữa,…). Quản lý ra vào theo thời gian cụ thể là trong giờ hành chính thì mới có thể vào, ngoài giờ hành chính, mọi hành vi ra vào những khu vực trên phải có sự giám sát của người đại diện cao nhất trong tổ chức hoặc người được ủy quyền.
- Cấm chụp ảnh hoặc ghi hình trong khu vực triển khai.

+ Các thiết bị lưu trữ di động, máy tính dành riêng cho nhân viên:

- Ngăn chặn việc sử dụng thiết bị phần cứng bên ngoài, kết nối không dây (wireless) trên máy tính
- Chỉ cài đặt các phần mềm từ nguồn được công ty xác nhận, cập nhật bản vá lỗi thường xuyên. Quy định rõ ràng về việc không thay đổi cấu hình của các máy và cài đặt những phần mềm không được phép.
- Có Antivirus trên các máy tính, phân vùng mạng rõ ràng cho các phòng ban, quản lý truy xuất tài nguyên dữ liệu giữa các phòng ban
- Tất cả các thiết bị được quản lý bằng serial number, có CSDL dành cho danh mục các thiết bị bao gồm cả thông tin về vị trí đặt, nếu có di chuyển phải cập nhật ngay
- Các phương tiện lưu trữ di động phải được xác nhận trước. Các cá nhân được ủy quyền sử dụng các thiết bị di động, lưu trữ có trách nhiệm bảo quản các thiết bị đó. Không sử dụng các thiết bị đó lưu trữ các thông tin nội bộ, nhạy cảm của công ty mà không có sự cho phép tương ứng

- Thực hiện thu hồi các thiệt bị cấp cho nhân viên trong trường hợp sử dụng sai mục đích.

+ Các loại dây cáp điện, cáp quang, cáp thông tin,...

- Thuê nhiều đường điện của nhiều khu vực để đảm bảo thiết bị có thể hoạt động tốt.
- Cáp điện và cáp thông tin phải được tách riêng để tránh nhiễu và các sự cố xảy ra.
- Các loại cáp phải được gắn nhãn tên của các thiết bị mà nó được nối tới tránh gây nhầm lẫn giữa các thiết bị vì có thể gây hư hại tới các thiết bị.
- Sử dụng ống bảo vệ để đi cáp đối với các thiệt bị cần có bảo mật cao như cáp đến các server, cáp quang từ các chi nhánh khác tới.

- Chính sách bảo mật thông tin:

+ Tất cả thông tin nhạy cảm phải được mã hóa khi truyền tải và lưu trữ, bao gồm email và tài liệu quan trọng.

+ Thiết lập quy trình chia sẻ thông tin nội bộ, bao gồm việc xác nhận từ cấp quản lý trước khi chia sẻ thông tin nhạy cảm.

+ Chặn và yêu cầu chặt chẽ khi thực hiện chia sẻ ra bên ngoài, cấm các chia sẻ không tin cậy Dropbox,...

+ Không cho phép cài đặt các ứng dụng mà không có sự phê duyệt của quản trị viên,...

- Chính sách sao lưu và phục hồi dữ liệu:

+ Thiết lập cơ chế Failover và kế hoạch khắc phục thảm họa cho Domain Controllers, File Server,.....:

+ Phải có cơ chế đồng bộ hóa giữa các máy chủ tương ứng, có quy trình chính sách quản lý và sao lưu dữ liệu giữa các chi nhánh để đồng nhất và tránh việc thiếu thông tin hoặc không chính xác khi cần phục hồi dữ liệu.

+ Xác định lớp ưu tiên cho dữ liệu, thực hiện chiến lược sao lưu đa lớp (như sao lưu định kỳ, sao lưu thường xuyên và sao lưu toàn bộ hệ thống).

+ Quy trình sao lưu được tự động hoá.

+ Quy trình sao lưu và phục hồi phải được xác minh và kiểm tra thử nghiệm thường xuyên, đảm bảo rằng các bản sao lưu có thể phục hồi được khi có sự cố.

+ Dữ liệu sao lưu phải được lưu trữ ở vị trí khác với dữ liệu gốc, có thể là trên cloud hoặc tại một địa điểm vật lý khác.

+ Có cơ chế mã hoá cho các dữ liệu được sao lưu điều này gây rủi ro rò rỉ thông tin dữ liệu nếu phương tiện lưu trữ bị đánh cắp hoặc bị xâm phạm.

+ Kiểm soát quyền truy cập an toàn vào dữ liệu sao lưu, hạn chế đối với những người có thẩm quyền.

+ Thiết lập các kế hoạch khắc phục thảm họa chính thức nêu ra các bước và thủ tục cụ thể cho các tình huống khác nhau, khó để ứng phó kịp thời và hiệu quả.

+ Đánh giá chính sách sao lưu định kỳ để điều chỉnh và cải thiện quy trình sao lưu dựa trên phản hồi và thay đổi trong môi trường công nghệ.

+ Ghi lại và phân tích bất kỳ sự cố nào liên quan đến sao lưu để rút ra bài học và cải thiện quy trình.

- Chính sách quản lý con người:

+ Nhân viên bình thường:

- Mỗi nhân viên phải có nghĩa vụ và trách nhiệm bảo quản các thiết bị được công ty ủy quyền sử dụng, nếu có vấn đề xảy ra phải báo ngay với bộ phận IT để kịp thời xử lý.
- Các nhân viên không được cài đặt phần mềm không rõ nguồn gốc hoặc không có bản quyền ngoài các phần mềm phục vụ công việc được cài sẵn trên máy.
- Tất cả nhân viên phải được tập huấn quy trình bảo đảm an toàn thông tin từ khi bắt đầu trở thành nhân viên.
- Khi có bất kỳ sự cố nào, người trực tiếp gây ra nó sẽ chịu trách nhiệm, bị xử lý kỷ luật theo quy định. Người quản lý, giám sát của người đó cũng sẽ bị xử lý kỷ luật tùy trường hợp.
- Nhân viên không được cung cấp thông tin đăng nhập, mật khẩu email, các tài khoản kết nối với dữ liệu của công ty cho bất cứ ai, thậm chí là các thành viên trong gia đình.
- Khi nhân viên kết nối với dữ liệu của công ty phải chịu trách nhiệm về việc đảm bảo an toàn thông tin đó. Phải đảm bảo các giải pháp kết nối dữ liệu là đúng tiêu chuẩn, nếu không, phải có sự cho phép của công ty.

- Sau khi kết thúc hợp đồng, nhân viên có trách nhiệm bàn giao lại toàn bộ tài sản thuộc sở hữu của công ty. Có trách nhiệm đảm bảo việc hủy bỏ quyền truy cập trước khi kết thúc hợp đồng. Nếu chưa, phải báo ngay cho bộ phận chuyên trách.
- Khi nhân viên thay đổi vị trí làm việc trong công ty, nhân viên phải có trách nhiệm trả lại những bàn giao lại tài sản không thuộc sở hữu cá nhân cho nơi làm việc. Có trách nhiệm đảm bảo việc hủy bỏ quyền truy cập vào phòng ban, thông tin có liên quan đến vị trí cũ.

+ Nhân viên quản trị (phòng IT):

- Có trách nhiệm giám sát, theo dõi hoạt động của các nhân viên khác trong công ty sử dụng máy tính vào công việc mà không làm chuyện riêng. Đảm bảo dữ liệu của công ty được bảo mật tránh thất thoát ra ngoài.
- Khi xảy ra sự cố phải báo cáo tình hình và mức độ thiệt hại cho cấp trên được biết. Phải khắc phục sự cố với thời gian nhanh nhất có thể để đảm bảo hệ thống hoạt động thông suốt.
- Chịu sựquản lý và nghiêm chỉnh chấp hành yêu cầu của cấp trên.
- Quản lý các tài nguyên của công ty, chịu trách nhiệm backup dữ liệu của công ty theo định kỳ và giám sát việc đồng bộ dữ liệu giữa hội sở với các chi nhánh.
- Có quyền giám sát việc sử dụng internet của tất cả các thiết bị đang kết nối với mạng của công ty.
- Thông tin chi tiết về thời gian, nội dung của phiên kết nối mạng của nhân viên công ty với internet bao gồm: duyệt web, nhắn tin instant message, email, trao đổi, chia sẻ tập tin phải được cung cấp cho nhân viên của bộ phận IT khi có yêu cầu.
- Bộ phận IT có toàn quyền ngăn chặn, giới hạn các trang web, giao thức trao đổi thông tin không phù hợp với công ty. Nội dung và quy định ngăn chặn, giới hạn của bộ phận IT do ban Giám đốc công ty quy định chi tiết.
- Nếu nhân viên IT nghỉ làm việc tại công ty phải thông báo trước với cấp công ty và bàn giao toàn bộ công việc hiện thời đang làm và các thiết bị do mình quản lý cho nhân viên khác có cùng chuyên môn hoặc cho cấp trên.

+ Ban lãnh đạo/Giám đốc IT:

- Có toàn quyền quyết định các chính sách an ninh thông tin cho công ty.
- Không được truy xuất vào dữ liệu, tài nguyên nội bộ của các nhân viên khác ngoại trừ những trường hợp đặt biệt.
- Có trách nhiệm tự bản quản tài nguyên của công ty, các tài liệu cá nhân tránh để xảy ra tình trạng thất thoát dữ liệu.
- Có trách nhiệm giám sát các nhân viên cấp dưới.

---HẾT---