TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO ĐỒ ÁN

QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

MÃ LỚP: NT207.N11.ATCL – NHÓM 3

GVHD: ThS. Nguyễn Duy

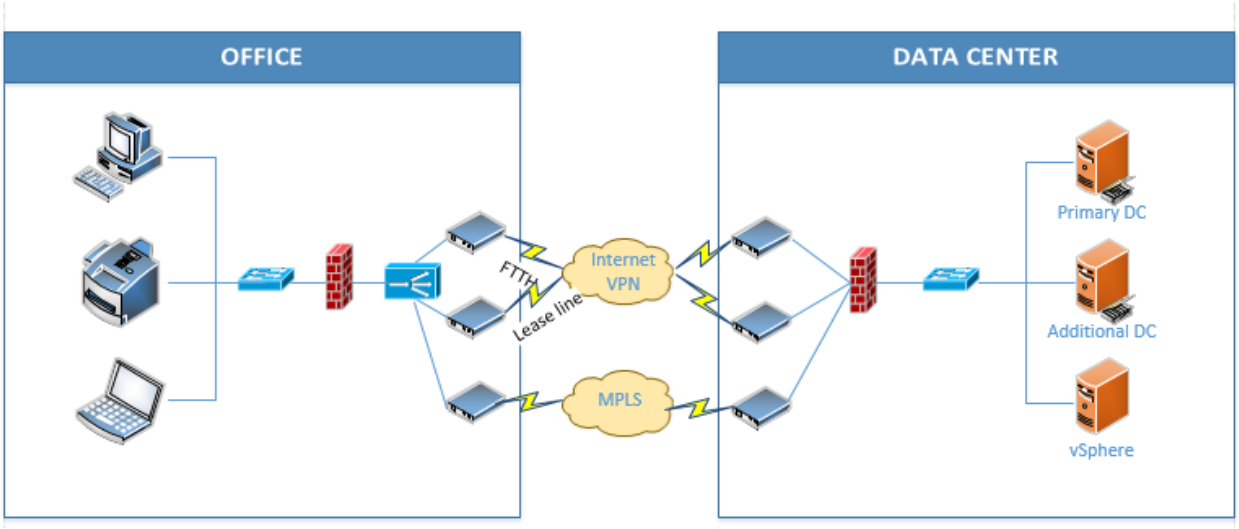
Các thành viên trong nhóm:

1. Trần Nguyễn Minh Triết – 19522398
2. Huỳnh Lê Hữu Phước – 19522053
3. Bùi Đức Anh – 19521190
4. Vũ Trung Kiên – 19521722
5. Võ Hoài Nam - 19521876

Tháng 1 năm 2023

Mục Lục

I. Phân tích những điểm yếu trong mô hình mạng hiện tại



A. Tính bảo mật kém

- Không có anti virus dễ bị đánh cắp dữ liệu cũng như lây lan mã độc qua các thiết bị chung mạng.
- Không có firewall chuyên dụng dễ bị tấn công DDOS dễ bị đánh cắp dữ liệu.
- Không có chính sách an ninh, dẫn đến nhân viên có thể tuỳ ý gửi thông tin cũng như phát tán dữ liệu qua internet mà không bị phát hiện.
- Không có hệ thống chủ động tìm kiếm, phát hiện và ngăn ngừa xâm nhập.
- Không có cơ chế bảo mật web, mail tại gateway dễ gây ra thất thoát dữ liệu
- Không có sự quản lý truy cập theo thời gian, cũng như không đáp ứng được các phân tích lưu lượng truy cập internet theo thời gian thực khiến cho việc điều tra sự cố trở nên khó khăn.
- Không có sự phân chia hệ thống mạng giữa các phòng ban.
- Thiếu cơ chế đảm bảo an toàn và quản lý nhân viên truy cập từ xa.
- Thiếu hệ thống giám sát, theo dõi, ghi log mạng cũng như từng thành phần trong hệ thống.
- Không có cơ chế quản lý CSDL dễ gây thất thoát dữ liệu cũng như khó khăn trong việc tìm kiếm dữ liệu.

B. Tính sẵn sàng và mở rộng kém

- Hệ thống chỉ sử dụng một đường truyền mạng điều này có thể dẫn đến việc gián đoạn khi có lỗi phát sinh.
- Không có hệ thống dự phòng điều này có thể gây ra một số vấn đề về latancy cũng như là high-availability khiến người dùng không có trải nghiệm tốt.
- Không có backup dữ liệu khiến cho việc lưu trữ và recovery dữ liệu khi gặp sự cố trở nên khó khăn.
- Khó mở rộng mô hình, thay đổi tài nguyên khi cần thiết khiến cho việc update và upgrade trở nên khó khăn.

II. Phân tích những rủi ro liên quan tới mất mát dữ liệu

Để phân tích những rủi ra có thể xảy ra, ta xét đến các tiêu chí: Thread, Vulnerability và sử dụng công thức để tính điểm của từng rủi ro dựa trên mức độ ảnh hưởng (Impact) và khả năng (likelihood) nó có thể xảy ra.

- Impact là mức độ ảnh hưởng của rủi ro nếu nó xảy ra dựa trên tính bí mật (Confidentiality), tính toàn vẹn (Integrity), tính sẵn sàng (Availability). Để tính mức độ ảnh hưởng ta có công thức sau: Impact Score = Max(C, I, A).
- Likelihood là khả năng mà rủi ro có thể xảy ra dựa trên tính phơi bày (Exposure), tần suất xuất hiện (Frequency), và khả năng điều khiển (Control). Ta có công thức như sau: Likelihood Score = (E + F)/2*R với R(Reverse) là ngược lại của Control.
    - Điểm Confidentiality (C), Integrity (I), Availability(A), Exposure (E) được xác định theo bảng:

Score	Description
5	Rất cao
4	Cao
3	Trung bình
2	Thấp
1	Rất thấp

    - Điểm Frequency (F) được xác định theo bảng:

Score	Description	Criteria
5	Rất thường xuyên	Hằng ngày
4	Thường xuyên	Hàng tuần
3	Thi thoảng	Hàng tháng
2	Ít gặp	1-2 năm
1	Hiếm khi	5-10 năm

- Reverse (R) được xác định theo bảng:

Control	Reverse
5	0,2
4	0,4
3	0,6
2	0,8
1	1

- Sau đó điểm rủi ra được theo công thức: Risk Score = Impact Score * Likelihood

A. Mức độ ảnh hưởng

Impact						
Threat (Agent and Action)		**Vulnerability**	**C**	**I**	**A**	**Impact Score**
Nhân viên	Install, Download file	Download cái file phần mềm không rõ nguồn gốc, có chứa mã độc, rasomware,…	5	5	0	5
	Xâm nhập hệ thống trái phép	Vô tình không log out máy khi rời khỏi bàn, cho phép người dùng khác truy cập trái phép	5	4	0	5
	Tiết lộ thông tin	Đưa dữ liệu của công ty ra bên ngoài	5	3	0	5

	Tác động vật lý	Vô tính hoặc cố tình tác động vật lý lên các thiết bị	0	0	5	5
	Thiết bị không an toàn	Sử dụng các thiết bị như máy in, fax, usb … lỗi thời, không an toàn trong việc bảo mật dữ liệu	5	3	0	5
	Dùng internet không đáng tin cây	Bị tấn công nghe lén, lộ dữ liệu	5	5	2	5
	Sửa, xóa file	Không có backup	0	0	5	5
Attacker	Tấn công vào lỗ hổng bảo mật	Tấn công vào lỗ hổng SQL injection của máy chủ để lấy database	5	5	0	5
	Tấn công mật khẩu	Mật khẩu yếu, có thể bị brute force hoặc crack dễ dàng	5	5	0	5
	Virus, Worm, Trojan, Ransomeware	Mã hóa dữ liệu, tạo backdoor lên máy chủ để reverse shell, chỉnh sửa các file trong hệ thống và lây lan sang các máy khác	5	5	5	5
	Data, thiết bị không được mã hóa	Dữ liệu bị sniffing có thể dễ dàng đọc được	2	5	1	5
	Tấn công nghe lén	Xen vào giữa đường truyền để đọc và bắt gói tin giữa các thiết bị	2	3	0	3
	Phising	Dùng mail để yêu cầu nhân viên cung cấp thông tin	3	0	0	3

		nhạy cảm như username, password				
	Không quản lý và giới hạn truy cập	DoS, DDOS, Brute force Attack	1	2	5	5
	Không phân quyền người dùng	Sau khi chiếm đoạt tài khoản nhân viên sau đó leo thang đặc quyền để lấy dữ liệu quan trọng	5	4	1	5

B. Khả năng xảy ra

Likelihood							
Threat (Agent and Action)		**Vulnerability**	**E**	**F**	**C**	**R**	**Impact Score**
Nhân viên	Install, Download file	Download cái file phần mềm không rõ nguồn gốc, có chứa mã độc, rasomware,…	5	4	2	0.8	3.6
	Xâm nhập hệ thống trái phép	Vô tình không log out máy khi rời khỏi bàn, cho phép người dùng khác truy cập trái phép	5	4	3	0.6	2.7
	Tiết lộ thông tin	Đưa dữ liệu của công ty ra bên ngoài	5	2	3	0.6	3
	Tác động vật lý	Vô tính hoặc cố tình tác động vật lý lên các thiết bị	3	1	3	0.6	1.2
	Thiết bị không an toàn	Sử dụng các thiết bị như máy in, fax, usb … lỗi thời, không an toàn	4	5	3	0.6	2.7

		trong việc bảo mật dữ liệu					
	Dùng internet không đáng tin cây	Bị tấn công nghe lén, lộ dữ liệu	5	3	3	0.6	2.4
	Sửa, xóa file	Không có backup	0	2	2	0.8	0.8
Attacker	Tấn công vào lỗ hổng bảo mật	Tấn công vào lỗ hổng SQL injection của máy chủ để lấy database	4	2	3	0.6	1.8
	Tấn công mật khẩu	Mật khẩu yếu, có thể bị brute force hoặc crack dễ dàng	3	5	4	0.4	1.6
	Virus, Worm, Trojan, Ransomeware	Mã hóa dữ liệu, tạo backdoor lên máy chủ để reverse shell, chỉnh sửa các file trong hệ thống và lây lan sang các máy khác	5	3	4	0.4	1.6
	Data, thiết bị không được mã hóa	Dữ liệu bị sniffing có thể dễ dàng đọc được	4	3	1	1	3.5
	Tấn công nghe lén	Xen vào giữa đường truyền để đọc và bắt gói tin giữa các thiết bị	2	3	1	1	2.5
	Phising	Dùng mail để yêu cầu nhân viên cung cấp thông tin nhạy cảm như username, password	2	4	2	0.8	2.4

	Không quản lý và giới hạn truy cập	DoS, DDOS, Brute force Attack	2	3	4	0.4	1
	Không phân quyền người dùng	Sau khi chiếm đoạt tài khoản nhân viên sau đó leo thang đặc quyền để lấy dữ liệu quan trọng	5	2	1	1	3.5

C. Đánh giá chung

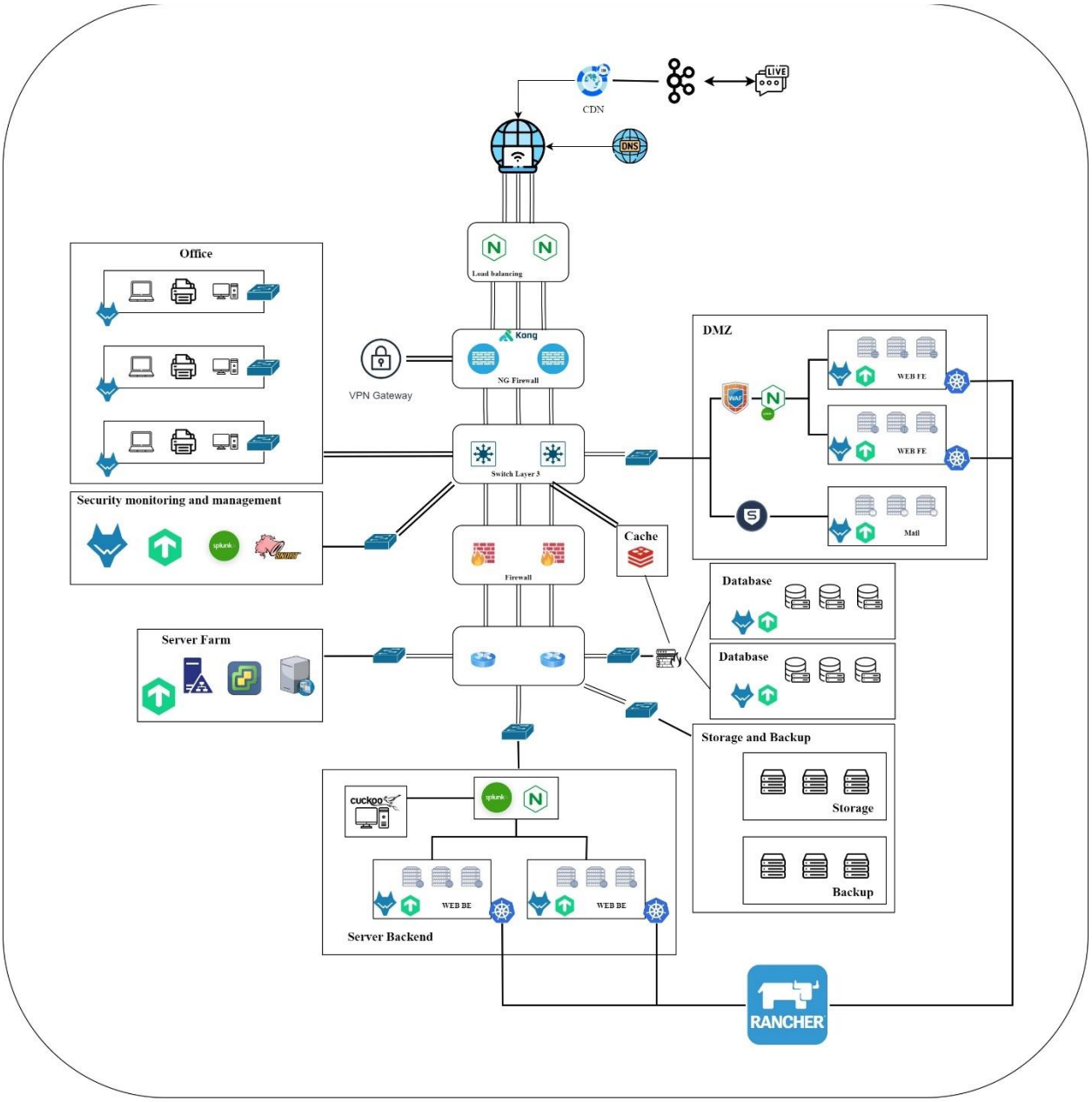
Risk Score					
Threat (Agent and Action)		**Vulnerability**	**Impact**	**Likelihood**	**Risk Score**
Nhân viên	Install, Download file	Download cái file phần mềm không rõ nguồn gốc, có chứa mã độc, rasomware,…	5	3.6	18
	Xâm nhập hệ thống trái phép	Vô tình không log out máy khi rời khỏi bàn, cho phép người dùng khác truy cập trái phép	5	2.7	13.5
	Tiết lộ thông tin	Đưa dữ liệu của công ty ra bên ngoài	5	3	15
	Tác động vật lý	Vô tính hoặc cố tình tác động vật lý lên các thiết bị	5	1.2	6
	Thiết bị không an toàn	Sử dụng các thiết bị như máy in, fax, usb … lỗi thời, không an	5	2.7	13.5

		toàn trong việc bảo mật dữ liệu			
	Dùng internet không đáng tin cây	Bị tấn công nghe lén, lộ dữ liệu	5	2.4	12
	Sửa, xóa file	Không có backup	5	0.8	4
Attacker	Tấn công vào lỗ hổng bảo mật	Tấn công vào lỗ hổng SQL injection của máy chủ để lấy database	5	1.8	9
	Tấn công mật khẩu	Mật khẩu yếu, có thể bị brute force hoặc crack dễ dàng	5	1.6	8
	Virus, Worm, Trojan, Ransomeware	Mã hóa dữ liệu, tạo backdoor lên máy chủ để reverse shell, chỉnh sửa các file trong hệ thống và lây lan sang các máy khác	5	1.6	8
	Data, thiết bị không được mã hóa	Dữ liệu bị sniffing có thể dễ dàng đọc được	5	3.5	17.5
	Tấn công nghe lén	Xen vào giữa đường truyền để đọc và bắt gói tin giữa các thiết bị	3	2.5	7.5
	Phising	Dùng mail để yêu cầu nhân viên cung cấp thông tin nhạy cảm như username, password	3	2.4	7.2

	Không quản lý và giới hạn truy cập	DoS, DDOS, Brute force Attack	5	1	5
	Không phân quyền người dùng	Sau khi chiếm đoạt tài khoản nhân viên sau đó leo thang đặc quyền để lấy dữ liệu quan trọng	5	3.5	17.5

III. Thiết kế lại hệ thống – mạng với tính bảo mật tốt nhất có thể

A. Mô hình tổng thể



B. Mô hình chi tiết

- **Mô hình xây dựng lại được chia làm các khu:**
  - Văn phòng
  - Quản lý và giám sát an ninh
  - Server Farm
  - Lưu trữ và Backup
  - Database
  - DMZ

- **Các khu vực được chia có nhiệm vụ, chức năng riêng:**

  - Khu vực quản lý và giám sát an ninh có nhiệm vụ theo dõi, quan sát các thất thường trên các server và các hosts khác. Wazuh được áp dụng nhằm quan sát và phát hiện lỗ hổng, các hành vi tấn công thất thường lên network, Checkmk có vai trò theo dõi hiệu năng và network của các host bên dưới. Splunk hỗ trợ quản lý log, đồ thị hoá các thông số.

  - Khu vực Server Farm có nhiệm vụ quản lý các host.

  - Khu vực Backend Server có vai trò xử lý logic của ứng dụng web đi từ bên ngoài vào. Nginx được sử dụng nhằm hỗ trợ Load Balancing, giúp tăng tính sẵn sàng của server; Splunk có vai trò thu thập log từ Nginx. Bên cạnh đó, Cuckoo sandbox được đưa vào nhằm hỗ trợ việc phân tích các file được tải về để phát hiện Virus. Các server backend đều được theo dõi thông qua Wazuh và Checkmk. Có 2 server Backend, để load balancing, tăng cường tính sẵn sàng.

  - Khu vực Storage và Backup hỗ trợ lưu trữ và backup dữ liệu (TBA)

  - Khu vực Database có 2 khu giống nhau, được ngăn cách bởi Database Firewall. Các Database có 1 Cache, sử dụng công nghệ Redis để lưu bản tạm thời của Database, để giúp việc truy vấn được nhanh hơn.

- Khu vực DMZ có 2 server Frontend, có load balancing là Nginx. Được bảo vệ bởi WAF, kèm với các dịch vụ như Checkmk, Wazuh để giám sát các server. Ngoài ra, trong DMZ còn có Mail Server, được bảo vệ bởi Sophos

- **Các dịch vụ khác trong Network:**

  - Từ bên ngoài vào trong network được ngăn cách bởi Next Generation Firewall, với Kong API Gateway để quản lý API. Có Nginx hỗ trợ Load Balancing cho Network

  - Bên ngoài bố trí các CDN để tăng tính sẵn sàng của dịch vụ và dịch vụ Kafka hỗ trợ theo dõi các thay đổi của Live Video.

C. Các công nghệ được sử dụng

- **Wazuh:**
  - Wazuh là một nền tảng bảo mật mã nguồn mở, được sử dụng cho ngăn chặn, phát hiện và phản hồi trước các mối đe doạ. Có khả năng bảo vệ công việc trực tiếp, ảo hoá và môi trường Cloud

  - Wazuh bao gồm endpoint security agent được triển khai trên hệ thống cần theo dõi, và một server để theo dõi, có khả năng thu thập và phân tích các dữ liệu lấy được từ các agent. Ngoài ra, Wazuh còn được tích hợp thêm Elastic Stack, cung cấp search engine và đồ thị cho phép người dùng dễ theo dõi các thông báo bảo mật hơn

  - Các chức năng chính của Wazuh là:

    - Phát hiện xâm nhập
    - Phân tích log
    - Bảo toàn tính nguyên vẹn của file
    - Phát hiện lỗ hổng
    - Đánh giá cấu hình
    - Phản ứng trước các cuộc tấn công
    - Đảm bảo theo sát quy trình bảo mật

    - Bảo mật Cloud
    - Bảo mật Container (đối với Docker)

- **CheckMK:**
  - Là một phần mềm giám sát, Checkmk cung cấp các giải pháp toàn diện và chuyên biệt để xử lý các môi trường cơ sở hạ tầng CNTT như Server, App, Cloud, Network, Database, Cloud, Container, Storage và IoT.
  - Các thông số có thể quan sát được trên CheckMK bao gồm hiệu năng của các máy, lưu lượng network, hoạt động của các dịch vụ mạng, ứng dụng….
  - CheckMK hỗ trợ theo dõi các máy thông qua các giao thức như SNMP, SSH, HTTP, IPMI

- **Splunk:**
  - Splunk là một phần mềm giám sát mạng dựa trên sức mạnh của việc phân tích Log. Splunk thực hiện các công việc tìm kiếm, giám sát và phân tích các dữ liệu lớn được sinh ra từ các ứng dụng, các hệ thống và các thiết bị hạ tầng mạng. Nó có thể thao tác tốt với nhiều loại dịnh dạng dữ liệu khác nhau
  - Splunk bao gồm các tính năng:
    - Định dạng Log
    - Các hình thức thu thập dữ liệu
    - Cập nhật dữ liệu
    - Đánh chỉ mục dữ liệu
    - Tìm kiếm thông tin
    - Giám sát và cảnh báo
    - Hiển thị thông tin
    - Phát triển

- **Snort:**
  - Snort là dịch vụ IDS/IPS open source và miễn phí, được sử dụng để thực hiện phân tích các traffic, giao thức; nhận diện nội dung; phát hiện và ngăn ngừa một số các loại tấn công mạng dựa trên một số rule đã được định sẵn
  - Snort có 3 chế độ hoạt động chính:
    - Packet Sniffing

    - Packet Logging
    - Network Intrusion Detection

- **Rancher:**
  - Rancher là công cụ nguồn mở, giao diện nền web, để quản lý Kubernetes Cluster, triển khai ứng dụng trên Kubernetes cho dù Cluster của chạy ở đâu, cung cấp bởi dịch vụ nào (AWS, GCP, Azure ...). Từ một Server cài đặt Rancher có thể quản lý một hay nhiều Kubernetes Cluster trên cùng một giao diện.
  - Rancher cho phép theo dõi, giám sát tình trạng của Kubernetes Cluster, nhận các cảnh bảo về sử dụng tài nguyên ...

- **Cuckoo:**
  - Cuckoo là một môi trường sandbox, dùng trong phân tích Malware thông qua việc cung cấp một môi trường ảo để thực thi Virus trong đó, từ các hành vi nó đã thực hiện đó, Cuckoo sẽ ghi lại và tạo ra report để báo lại cho người dùng. Việc submit sample lên để phân tích khá đơn giản, chỉ với 1 dòng lệnh submit hay thông qua web interface của Cuckoo
  - Các thông số, thông tin thu thập được từ Cuckoo Sandbox:
    - Các lời gọi hàm được thực hiện bởi malware
    - File được tạo, xoá, chỉnh sửa khi malware đang chạy
    - Memory dump của process của malware
    - Network traffic ở dạng PCAP
    - Một số ảnh chụp màn hình malware khi đang chạy
    - Memory dump của toàn máy

- **Kong Gateway**
  - Kong Gateway cũng giống như các API Gateway khác nó làm nhiệm vụ định tuyến các yêu cầu, kết hợp và chuyển đổi các giao thức. Kong nhẹ, được dùng cho microservices, có độ trễ thấp, hiệu suất cao và scalability. Kong server là stateless, chúng ta có thể thêm hoặc xóa bao nhiêu nodes tùy ý, miễn là chúng trỏ vào 1 datastores. Kong Datastore có thể chọn 1 trong 2 loại DB: Postgres, Cassandra.
  - Các tính năng mà Kong Gateway mang lại:
    - Che dấu được cấu trúc của hệ thống microservices với bên ngoài

    - Phần code phía frontend sẽ gọn gàng hơn
    - Dễ dàng theo dõi và quản lý traffic.
    - Requests caching và cân bằng tải.
    - Thêm một lớp bảo mật nữa cho hệ thống.
    - Thay thế authentication services

- **WAF**
  - WAF (Web Application Firewall) còn gọi là tường lửa ứng dụng web. WAF là một thiết bị proxy có thể xử lý giao thức HTTP nhằm bảo vệ ứng dụng web. WAF kiểm tra lượng truy cập và sẽ lọc ra các yêu cầu có mối đe dọa xâm hại đến website trước khi đến ứng dụng web.
  - Tường lửa ứng dụng Web (Web Application Firewall – WAF) được triển khai ở đường biên mạng (Network Edge). Nó thực hiện việc kiểm tra lưu lượng truy cập đến và đi khỏi các ứng dụng Web. WAF có thể lọc và giám sát lưu lượng truy cập để bảo vệ chống lại các cuộc tấn công như SQL Injection, Cross Site Scripting (XSS) hay Cross-site Request Forgery – CSRF (tấn công giả mạo yêu cầu Cross-site).
  - Các tính năng mà WAF mang lại:
    - Che dấu được cấu trúc của hệ thống microservices với bên ngoài
    - WAF được triển khai trước các ứng dụng web và phân tích lưu lượng HTTP – kiểm tra cả request GET và POST nhằm phát hiện và chặn bất kỳ thứ gì độc hại.
    - Không giống như tường lửa (Firewall) thông thường chỉ đóng vai trò như một cổng an toàn giữa các server, WAF là một biện pháp bảo mật ứng dụng được đặt giữa Web Client và Web Server.
    - Các cuộc tấn công độc hại đến máy tính thường được tự động hóa. Những loại tấn công này rất khó phát hiện vì chúng thường được thiết kế để bắt chước giống lưu lượng truy cập của con người và không bị phát hiện.
    - WAF thực hiện kiểm tra chi tiết mọi request và response đối với tất cả các dạng lưu lượng truy cập web phổ biến. Việc kiểm tra này giúp WAF xác định và chặn các mối đe dọa, ngăn chúng xâm nhập vào server.

- **NGINX**

- Nginx là một máy chủ Web Server mã nguồn mở. Dự án Nginx được phát hành và sử dụng như một web server được thiết kế hướng đến mục đích cải thiện tối đa hiệu năng và sự ổn định. Bên cạnh đó, nhờ vào các khả năng của máy chủ HTTP mà NGINX còn có thể hoạt dộng như một proxy server cho email (IMAP, POP3, và SMTP), reverse proxy, và trung gian để cân bằng tải cho các máy chủ HTTP, TCP, và UDP.
- Các tính năng mà WAF mang lại:
    - Che dấu được cấu trúc của hệ thống microservices với bên ngoài
    - Tạo ra khả năng xử lý hơn đến 10.000 kết nối cùng một lúc với các bộ nhớ thấp.
    - Hỗ trợ phục vụ các tập tin tĩnh và lập ra các chỉ mục tập tin phù hợp.
    - Có khả năng tăng tốc reverse proxy bằng các bộ nhớ đệm giúp cân bằng tải đơn giản hơn với khả năng chịu lỗi vô cùng cao.
    - Nginx có thể hỗ trợ tăng tốc cùng với bộ nhớ FastCGI, uwsgi, SCGI và những máy chủ memcached vô cùng hiệu quả.
    - Kiến trúc modular cho phép gia tăng tốc độ nạp trang bằng biện pháp nén gzip một cách tự động.
    - Nginx có khả năng hỗ trợ thực hiện mã hóa SSL và TLS.
    - Cấu hình của Nginx vô cùng linh hoạt giúp lưu lại nhật ký truy vấn một cách dễ dàng.
    - Nginx có khả năng chuyển hướng lỗi 3XX-5XX.
    - Rewrite URL có thể sử dụng expression.
    - Nginx có thể hạn chế tỷ lệ đáp ứng của truy vấn.
    - Nginx giúp giới hạn số kết nối đồng thời cũng như truy vấn từ 1 địa chỉ.
    - Nginx có khả năng nhúng mã PERL một cách dễ dàng.
    - Nginx có thể hỗ trợ và tương thích hoàn toàn với IPv6.
    - Nginx có thể hỗ trợ cho websockets.
    - Nginx hỗ trợ truyền tải các file FLV và MP4.

- **Redis:**
    - Redis được viết tắt từ Remote Dictionary Server là hệ thống lưu trữ dữ liệu in-memory dưới dạng key-value với tốc độ nhanh, mã nguồn mở, được sử dụng để lưu trữ dữ liệu, cache, message broker và queue. Redis hỗ trợ nhiều cấu trúc dữ liệu cơ bản như string, hash, list, set, sorted set.

Bên cạnh lưu trữ key-value trên RAM với hiệu năng cao, redis còn hỗ trợ lưu trữ dữ liệu trên đĩa cứng cho phép phục hồi dữ liệu khi gặp sự cố. Redis hiện cung cấp thời gian phản hồi dưới một phần nghìn giây cho phép hàng triệu yêu cầu mỗi giây cho các ứng dụng real time trong Gaming, Ad-Tech, Dịch vụ tài chính, Chăm sóc sức khỏe và IoT. Redis là một lựa chọn phổ biến cho caching, session management, gaming, leaderboards, hệ thống real-time.

- **NextGen Firewall:**
  - Tường lửa thế hệ tiếp theo (NGFW) là một phần của công nghệ tường lửa thế hệ thứ ba, kết hợp tường lửa truyền thống với các chức năng lọc thiết bị mạng khác, chẳng hạn như tường lửa ứng dụng sử dụng kiểm tra gói sâu nội tuyến (DPI), hệ thống ngăn chặn xâm nhập (IPS). Các kỹ thuật khác cũng có thể được sử dụng, chẳng hạn như kiểm tra lưu lượng truy cập được mã hóa TLS/SSL, lọc trang web, quản lý QoS/băng thông, kiểm tra chống vi-rút, tích hợp quản lý danh tính bên thứ ba (tức là LDAP, RADIUS, Active Directory) và giải mã SSL
  - NGFW bao gồm các chức năng điển hình của tường lửa truyền thống như lọc gói, dịch địa chỉ mạng và cổng (NAT), kiểm tra trạng thái và hỗ trợ mạng riêng ảo (VPN). Mục tiêu của tường lửa thế hệ tiếp theo là bao gồm nhiều lớp hơn của mô hình OSI, cải thiện khả năng lọc lưu lượng mạng phụ thuộc vào nội dung gói.

- **Amazon S3:**
  - Amazon S3 hoặc Amazon Simple Storage Service là một "dịch vụ lưu trữ đơn giản" được cung cấp bởi Amazon Web Services (AWS) cung cấp lưu trữ đối tượng thông qua giao diện dịch vụ web. Amazon S3 sử dụng cơ sở hạ tầng lưu trữ có thể mở rộng tương tự mà Amazon.com sử dụng để chạy mạng thương mại điện tử toàn cầu của mình.

  - Amazon S3 có thể được sử dụng để lưu trữ bất kỳ loại đối tượng nào cho phép sử dụng như lưu trữ cho các ứng dụng Internet, sao lưu và phục hồi, phục hồi thảm họa, lưu trữ dữ liệu, hồ dữ liệu để phân tích và lưu trữ đám mây hỗn hợp. Trong thỏa thuận cấp độ dịch vụ của mình, Amazon S3 đảm bảo 99,9% thời gian hoạt động hàng tháng, hoạt động trong thời gian ngừng hoạt động dưới 43 phút mỗi tháng.

- AWS đã ra mắt Amazon S3 tại Hoa Kỳ vào ngày 14 tháng 3 năm 2006, sau đó tại Châu Âu vào tháng 11 năm 2007

- **Kubernetes:**
  - Kubernetes là một nền tảng nguồn mở, khả chuyển, có thể mở rộng để quản lý các ứng dụng được đóng gói và các service, giúp thuận lợi trong việc cấu hình và tự động hoá việc triển khai ứng dụng. Kubernetes là một hệ sinh thái lớn và phát triển nhanh chóng. Các dịch vụ, sự hỗ trợ và công cụ có sẵn rộng rãi
  - Kubernetes cung cấp:
    - Service discovery và cân bằng tải: Kubernetes có thể expose một container sử dụng DNS hoặc địa chỉ IP của riêng nó. Nếu lượng traffic truy cập đến một container cao, Kubernetes có thể cân bằng tải và phân phối lưu lượng mạng (network traffic) để việc triển khai được ổn định
    - Điều phối bộ nhớ: Kubernetes cho phép tự động mount một hệ thống lưu trữ mà chọn, như local storages, public cloud providers, v.v.
    - Tự động rollouts và rollbacks: Kubernetes có thể mô tả trạng thái mong muốn cho các container được triển khai dùng Kubernetes và nó có thể thay đổi trạng thái thực tế sang trạng thái mong muốn với tần suất được kiểm soát.
    - Đóng gói tự động: Người dùng có thể cung cấp cho Kubernetes một cluster gồm các node mà nó có thể sử dụng để chạy các tác vụ được đóng gói (containerized task). Cho Kubernetes biết mỗi container cần bao nhiêu CPU và bộ nhớ (RAM). Kubernetes có thể điều phối các container đến các node để tận dụng tốt nhất các resource.
    - Tự phục hồi Kubernetes: khởi động lại các containers bị lỗi, thay thế các container, xoá các container không phản hồi lại cấu hình health check do người dùng xác định và không cho các client biết đến chúng cho đến khi chúng sẵn sàng hoạt động.
    - Quản lý cấu hình và bảo mật: Kubernetes cho phép lưu trữ và quản lý các thông tin nhạy cảm như: password, OAuth token và SSH key. Người dùng có thể triển khai và cập nhật lại secret và cấu hình ứng dụng mà không cần build lại các container image và không để lộ secret trong cấu hình stack.

- **Kafka:**

- Kafka là dự án mã nguồn mở, đã được đóng gói hoàn chỉnh, khả năng chịu lỗi cao và là hệ thống nhắn tin nhanh. Vì tính đáng tin cậy của nó, Kafka đang dần được thay thế cho hệ thống nhắn tin truyền thống. Nó được sử dụng cho các hệ thống nhắn tin thông thường trong các ngữ cảnh khác nhau. Đây là hệ quả khi khả năng mở rộng ngang và chuyển giao dữ liệu đáng tin cậy là những yêu cầu quan trọng nhất. Kafka được sử dụng để:
    - Website Activity Monitoring: theo dõi hoạt động của website
    - Stream Processing: xử lý stream
    - Log Aggregation: tổng hợp log
    - Metrics Collection: thu thập dữ liệu

D. Bảng Risk Score

1. Mức độ ảnh hưởng

Impact						
Threat (Agent and Action)		**Vulnerability**	**C**	**I**	**A**	**Impact Score**
Nhân viên	Install, Download file	Download cái file phần mềm không rõ nguồn gốc, có chứa mã độc, rasomware,…	1	0	0	1
	Xâm nhập hệ thống trái phép	Vô tình không log out máy khi rời khỏi bàn, cho phép người dùng khác truy cập trái phép	1	0	0	1
	Tiết lộ thông tin	Đưa dữ liệu của công ty ra bên ngoài	1	0	0	1
	Tác động vật lý	Vô tính hoặc cố tình tác động vật lý lên các thiết bị	0	0	0	0
	Thiết bị không an toàn	Sử dụng các thiết bị như máy in, fax, usb … lỗi thời,	1	0	0	1

		không an toàn trong việc bảo mật dữ liệu				
	Dùng internet không đáng tin cây	Bị tấn công nghe lén, lộ dữ liệu	1	1	1	1
	Sửa, xóa file	Không có backup	0	0	0	0
Attacker	Tấn công vào lỗ hổng bảo mật	Tấn công vào lỗ hổng SQL injection của máy chủ để lấy database	1	1	0	1
	Tấn công mật khẩu	Mật khẩu yếu, có thể bị brute force hoặc crack dễ dàng	1	1	0	1
	Virus, Worm, Trojan, Ransomeware	Mã hóa dữ liệu, tạo backdoor lên máy chủ để reverse shell, chỉnh sửa các file trong hệ thống và lây lan sang các máy khác	1	1	1	1
	Data, thiết bị không được mã hóa	Dữ liệu bị sniffing có thể dễ dàng đọc được	0	1	0	1
	Tấn công nghe lén	Xen vào giữa đường truyền để đọc và bắt gói tin giữa các thiết bị	0	0	0	0
	Phising	Dùng mail để yêu cầu nhân viên cung cấp thông tin nhạy cảm như username, password	0	0	0	0
	Không quản lý và giới hạn truy cập	DoS, DDOS, Brute force Attack	0	0	1	1

	Không phân quyền người dùng	Sau khi chiếm đoạt tài khoản nhân viên sau đó leo thang đặc quyền để lấy dữ liệu quan trọng	1	1	0	0

2. Khả năng xảy ra

Likelihood							
Threat (Agent and Action)		**Vulnerability**	**E**	**F**	**C**	**R**	**Impact Score**
Nhân viên	Install, Download file	Download cái file phần mềm không rõ nguồn gốc, có chứa mã độc, rasomware,…	1	0	5	0.2	0.1
	Xâm nhập hệ thống trái phép	Vô tình không log out máy khi rời khỏi bàn, cho phép người dùng khác truy cập trái phép	1	2	5	0.2	0.3
	Tiết lộ thông tin	Đưa dữ liệu của công ty ra bên ngoài	1	1	4	0.4	0.4
	Tác động vật lý	Vô tính hoặc cố tình tác động vật lý lên các thiết bị	1	0	5	0.2	0.1
	Thiết bị không an toàn	Sử dụng các thiết bị như máy in, fax, usb … lỗi thời, không an toàn trong việc bảo mật dữ liệu	0	1	5	0.2	0.1
	Dùng internet không đáng tin cây	Bị tấn công nghe lén, lộ dữ liệu	1	1	5	0.2	0.2

	Sửa, xóa file	Không có backup	0	0	5	0.2	0
Attacker	Tấn công vào lỗ hổng bảo mật	Tấn công vào lỗ hổng SQL injection của máy chủ để lấy database	0	1	5	0.2	0.1
	Tấn công mật khẩu	Mật khẩu yếu, có thể bị brute force hoặc crack dễ dàng	1	1	5	0.2	0.2
	Virus, Worm, Trojan, Ransomeware	Mã hóa dữ liệu, tạo backdoor lên máy chủ để reverse shell, chỉnh sửa các file trong hệ thống và lây lan sang các máy khác	0	0	5	0.2	0
	Data, thiết bị không được mã hóa	Dữ liệu bị sniffing có thể dễ dàng đọc được	0	0	5	0.2	0
	Tấn công nghe lén	Xen vào giữa đường truyền để đọc và bắt gói tin giữa các thiết bị	0	0	5	0.2	0
	Phising	Dùng mail để yêu cầu nhân viên cung cấp thông tin nhạy cảm như username, password	1	2	4	0.4	0.6
	Không quản lý và giới hạn truy cập	DoS, DDOS, Brute force Attack	0	0	5	0.2	0
	Không phân quyền người dùng	Sau khi chiếm đoạt tài khoản nhân viên sau đó leo thang đặc quyền để lấy dữ liệu quan trọng	1	1	5	0.2	0.2

3. Đánh giá chung

Risk Score					
Threat (Agent and Action)		**Vulnerability**	**Impact**	**Likelihood**	**Risk Score**
Nhân viên	Install, Download file	Download cái file phần mềm không rõ nguồn gốc, có chứa mã độc, rasomware,…	1	0.1	0.1
	Xâm nhập hệ thống trái phép	Vô tình không log out máy khi rời khỏi bàn, cho phép người dùng khác truy cập trái phép	1	0.3	0.3
	Tiết lộ thông tin	Đưa dữ liệu của công ty ra bên ngoài	1	0.4	0.4
	Tác động vật lý	Vô tính hoặc cố tình tác động vật lý lên các thiết bị	0	0.1	0
	Thiết bị không an toàn	Sử dụng các thiết bị như máy in, fax, usb … lỗi thời, không an toàn trong việc bảo mật dữ liệu	1	0.1	0.1
	Dùng internet không đáng tin cây	Bị tấn công nghe lén, lộ dữ liệu	1	0.2	0.2
	Sửa, xóa file	Không có backup	0	0	0

Attacker	Tấn công vào lỗ hổng bảo mật	Tấn công vào lỗ hổng SQL injection của máy chủ để lấy database	1	0.1	0.1
	Tấn công mật khẩu	Mật khẩu yếu, có thể bị brute force hoặc crack dễ dàng	1	0.2	0.2
	Virus, Worm, Trojan, Ransomeware	Mã hóa dữ liệu, tạo backdoor lên máy chủ để reverse shell, chỉnh sửa các file trong hệ thống và lây lan sang các máy khác	1	0	0
	Data, thiết bị không được mã hóa	Dữ liệu bị sniffing có thể dễ dàng đọc được	1	0	0
	Tấn công nghe lén	Xen vào giữa đường truyền để đọc và bắt gói tin giữa các thiết bị	0	0	0
	Phising	Dùng mail để yêu cầu nhân viên cung cấp thông tin nhạy cảm như username, password	0	0.6	0
	Không quản lý và giới hạn truy cập	DoS, DDOS, Brute force Attack	1	0	0
	Không phân quyền người dùng	Sau khi chiếm đoạt tài khoản nhân viên sau đó leo thang đặc	0	0.2	0

		quyền để lấy dữ liệu quan trọng			

IV. Xây dựng qui trình và chính sách

A. Nhân sự

- Có quy trình tuyển dụng nhân sự: Chính sách tuyển chọn, định hướng cho nhân viên, thử việc
- Hợp đồng rõ ràng với nhân viên
- Thực hiện đánh giá nhân viên trong công ty theo tiêu chuẩn
- Lên kế hoạch đào tạo, phát triển. Đề xuất các chế độ đãi ngộ, hoạt động gắn kết nhân viên, xây dựng văn hóa doanh nghiệp.
- Xây dựng bộ quy tắc ứng xử giữa các thành viên trong công ty.
- Nhân viên có trách nhiệm và nhận thức bảo đảm an toàn thông tin dữ liệu tài sản trong công ty. Tuyệt đối giữ bí mật các dữ liệu trong công ty, trong làm lộ thất thoát dữ liệu dưới mọi hình thức.
- *Đối với các bộ phận IT:*
    - Cần thực hiện giám sát chặt chẽ các hoạt động Internet của nhân viên trong công ty.
    - Không tùy tiện sử dụng máy tính công ty ngoài công việc.
    - Chịu trách nhiệm quản lý các tài nguyên của công ty, backup dữ liệu theo định kỳ, xử lý các sự cố xảy ra.
- *Đối với các phòng ban khác:*
    - Chỉ sử dụng máy tính công ty phục vụ công việc, không sử dụng cho mục đích cái nhân.
    - Chỉ truy cập vào vùng tài nguyên cho phép. Nếu cần truy cập cần có sự cho phép của cấp trên.
    - Nếu phát hiện sự bất cần báo nay cho các bộ phận cần thiết.
    - Không sử dụng mạng internet của công ty nếu không cần thiết
- *Đối với phòng giám đốc:*
    - Hiểu được quyền hạn mà tài khoản của mình có thể thao tác với thông tin của công ty, bảo vệ nó một cách chặt chẽ.
    - Có trách nhiệm giám sát các nhân viên cấp dưới.
    - Có trách nhiệm bảo vệ các thông tin quan trọng của công ty, các tài liệu quan trọng phải cất giữ và bảo vệ an toàn tối đa tránh thất thoát dữ liệu.

- *Chính sách đối với các nhân viên nghỉ việc:* Cam kết không tiết lộ thông tin của công ty ra bên ngoài.

B. Quản lý truy cập Internet

- Giám sát truy cập:
    - Bộ phận IT theo dõi giám sát việc sử dụng Internet của nhân viên trong công ty bao gồm cả lưu lượng mạng.
    - Lưu lại hồ sơ sử dụng Internet theo thời gian quy định
    - Xử lý các trường hợp truy cập bất thường.
    - Luôn luôn xác thực các truy cập từ xa.
    - Giới hạn quyền truy cập.
- Filter Internet: Ngăn chặn truy cập các trang web, giao thức không phù hợp với công việc.
- Quản lý upload, download, install:
    - Kiểm thử các phần mềm được cài đặt vào các máy tính công ty.
    - Hạn chế các file được download và upload lên theo bất kì giao thức nào.
    - Đảm bảo giao thức mã hóa, truyền thông tin.

C. Các tài sản vật lý

- Các thiết bị data center, các thiết bị quan trong cần được đặt tại 1 khu vực an toàn, được kiểm soát an ninh nghiêm ngặt.
- Chỉ có những người được cho phép mới được phép tiếp cận, ra vào.
- Kiểm tra, bảo trì theo đúng lịch.
- Có các hệ thống phòng chóng cháy nổ, thiên tai.
- Cần có người giám sát 24/7.

D. Chính sách quản lý thông tin

Đối với thông tin bình thường: nhân viên được tùy ý sử dụng, trao đổi ngoài giờ làm việc.

Đối với thông tin nhạy cảm:

- 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 cá nhân của nhân viên phải được khoá lại khi không làm việc và được tắt hoàn toàn khi hết giờ làm.
- Các tài liệu nội bộ phải được cất vào nơi bảo quản được khoá lại khi nhân viên không sử dụng đến hoặc đi ra ngoài và khi hết giờ làm việc.
- Nhân viên bị cấm trong việc tiết lộ các thông tin bí mật của công ty trên các trang blog, trên các mạng xã hội như Facebook, Twitter, Google Plus,…

- 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.

Đối với thông tin mật:

- Bao gồm tất cả chính sách trên.
- 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 đ~~ư~~ợc phép tiếp cận.
- 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 khoá cẩn thận.
- Các văn bản, giấy tờ quan trọng khi không dùng nữa phải được tiêu huỷ đúng cách ngay lập tức tránh để lộ thông tin mật.
- Tất cả dữ liệu mật được lưu trữ trong các thiết bị ngoại vi như CD-ROM, DVD hay USB đều phải được mã hóa và đặt password.

Đối với thông tin tuyệt mật:

- Bao gồm tất cả chính sách trên.
- 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 file server, được phân quyền, gán nhãn tự động bằng Windows Server Dynamic Access Control kết hợp Right Management Services (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. Không có nhân viên nào được phép truy xuất những thông tin này trừ ban lãnh đạo của công ty.