ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN

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

HỌC KỲ: I

NĂM HỌC: 2023-2024

Đề tài: Xây dựng giải pháp Data Loss Prevention cho doanh nghiệp

Giảng viên hướng dẫn: **ThS. Nguyễn Duy**

Lớp: NT207.O11.ANTT

Nhóm thực hiện: Nhóm 7

STT	Họ và tên	MSSV
1	Nguyễn Phúc Hải	20521281
2	Trần Xuân Nam	20521637
3	Đỗ Minh Thọ	20521972
4	Hà Minh Phúc	20521759

Thành phố Hồ Chí Minh, ngày 12 tháng 9 năm 2023

MỤC LỤC

I. LỜI MỞ ĐẦU

Trong môi trường kinh doanh hiện đại, dữ liệu đóng vai trò quan trọng như là tài sản vô hình của doanh nghiệp, đó cũng là lý do tại sao bảo vệ dữ liệu trở thành một ưu tiên hàng đầu. Tuy nhiên, nguy cơ mất mát dữ liệu ngày càng gia tăng do sự phát triển nhanh chóng của công nghệ và sự phổ cập hóa của các phương tiện truyền thông. Để đối mặt với thách thức này, việc xây dựng một giải pháp Data Loss Prevention (DLP) là không thể phủ nhận.

II. ĐẶT VẤN ĐỀ

Doanh nghiệp ngày nay đối diện với nhiều mối đe dọa đe dọa từ bên trong và bên ngoài, từ các hình thức tấn công mạng phức tạp đến nguy cơ lạc quan và sơ ý từ phía nhân viên. Mỗi sự cố mất mát dữ liệu không chỉ mang lại tổn thất về tài chính mà còn đặt ra những vấn đề nghiêm trọng liên quan đến uy tín và tuân thủ quy định.

III. MỤC TIÊU

Mục tiêu của đồ án này trong thời gian học tập môn Quản lý rủi ro và an toàn thông tin trong doanh nghiệp có thể tìm hiểu, nghiên cứu và xây dựng một giải pháp DLP toàn diện và hiệu quả cho doanh nghiệp, nhằm ngăn chặn hiện tượng mất mát dữ liệu, bảo vệ thông tin quan trọng, duy trì sự tin cậy của khách hàng và đối tác.

Hoàn thành tốt học phần, cũng cố thêm các kiên thức về quản lý rủi ro và chuẩn bị cho các học kỳ sắp tới.

IV. NỘI DUNG CHÍNH CỦA ĐỒ ÁN

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

- *Rủi ro 1: Hệ thống chưa có phần mềm Antivirus*

- Nguyên nhân:
  - Nhân viên truy cập các trang web không uy tín; cài các ứng dụng không rõ nguồn gốc
  - Tải về các file mã độc trong mail
- Hậu quả:
  - Lây nhiễm malware vào hệ thống
  - Mất mát dữ liệu

- *Rủi ro 2: Hệ thống chưa có các Firewall chuyên dụng*

- Nguyên nhân:
  - Attacker thực hiện tấn công SQLi, Command Injection, XSS, CSRF vào hệ thống
  - Tấn công từ chối dịch vụ
- Hậu quả:
  - Thông tin có thể bị đánh cắp
  - Hệ thống có thể bị mất kiểm soát
  - Ảnh hưởng đến tính sẵn sàng của hệ thống

- *Rủi ro 3: Hệ thống chưa có các phân vùng dữ liệu quan trọng*

- Nguyên nhân:
  - Ai cũng có thể truy cập vào mạng internal

- Hậu quả:
  + Dữ liệu bị đánh cắp bởi các người dùng không hợp pháp
  + Khó quản lý cũng như có chính sách thích hợp cho các dữ liệu quan trọng

- *Rủi ro 4: Hệ thống chưa có IDS/IPS*

- Nguyên nhân:
  + Attacker thực hiện các cuộc tấn công và có thể qua mặt hoặc Firewall chưa thể phát hiện
- Hậu quả:
  + Thông tin bị đánh cắp
  + Ảnh hưởng đến tính sẵn sàng và bảo mật của hệ thống

- *Rủi ro 5: Thiếu endpoint security*

- Nguyên nhân:
  + Nhân viên thực hiện các thao tác photocopy, in tài liệu, nhập dữ liệu từ bàn phím, ... bị lỗi
- Hậu quả:
  + Rò rỉ thông tin

- *Rủi ro 6: Hệ thống chưa có xác thực người dùng*

- Nguyên nhân:
  + User làm mất mail, hay bị attacker gửi các malicious qua mail chiếm quyền
- Hậu quả:
  + Mất các dữ liệu quan trọng trong mail

- *Rủi ro 7: Hệ thống chưa có chính sách phân quyền cho nhân viên*

- Nguyên nhân:
  + Nhân viên có thể chỉnh sửa, thay đổi các dữ liệu quan trọng của cấp trên
  + Nhân viên có thể xem các dữ liệu quan trọng
  + Rule kiểm tra quyền chưa được cài đặt đúng
- Hậu quả:
  + Dữ liệu không còn toàn vẹn
  + Dữ liệu bị mất an toàn
  + Bypass permission

- *Rủi ro 8: Chưa có hệ thống sao lưu và phục hồi dữ liệu khi gặp sự cố bất ngờ*

- Nguyên nhân:
  + Hệ thống điện của công ty bị ngắt đột xuất (mất điện)
  + Xảy ra thiên tai
- Hậu quả:
  + Dữ liệu có thể bị mất
  + Các dịch vụ của hệ thống bị tạm ngưng, mất tính sẵn sàng

- *Rủi ro 9: Chưa có các hệ thống mã hóa trong quá trình vận chuyển dữ liệu*

- Nguyên nhân:
  + Bị attacker tấn công nghe lén
  + Attacker chỉnh sửa các gói tin trên đường truyền mạng
- Hậu quả:
  + Thông tin bị tiết lộ
  + Thông tin bị sai lệch, mất tính bảo mật và toàn vẹn

- *Rủi ro 10: Nguy cơ khi sử dụng các thiết bị IoT*

- Nguyên nhân:
  + Các thiết bị IoT thường có bảo mật kém, dễ bị tấn công.
  + Các thiết bị IoT thường được kết nối với mạng nội bộ, tạo điều kiện cho kẻ xấu xâm nhập vào hệ thống.
- Hậu quả:
  + Dữ liệu có thể bị đánh cắp.
  + Hệ thống có thể bị mất kiểm soát.
  + Các dịch vụ của hệ thống có thể bị gián đoạn.

2. Những rủi ro liên quan tới mất mát dữ liệu

2.1. Rủi ro đến từ Attacker

- Tấn công Ransomware: Attacker có thể triển khai mã độc hại ransomware để mã hóa dữ liệu trên hệ thống và yêu cầu tiền chuộc để giải mã.
- Sử dụng Malware: Attacker triển khai malware để thực hiện các hoạt động gián điệp, đánh cắp thông tin.
- Lỗ hổng bảo mật phần mềm: Attacker khai thác lỗ hổng trong phần mềm để xâm nhập hệ thống.
- Tấn công Phishing: Attacker sử dụng email, tin nhắn giả mạo để lừa đảo người dùng tiết lộ thông tin cá nhân.
- Sử dụng kỹ thuật Social Engineering: Attacker sử dụng kỹ thuật xã hội để lừa đảo người dùng và thu thập thông tin quan trọng.
- Xâm nhập mạng nội bộ: Attacker xâm nhập vào mạng nội bộ để thực hiện các hoạt động gián điệp hoặc đánh cắp dữ liệu.

- Tấn công Zero-Day: Attacker tận dụng lỗ hổng bảo mật chưa được biết đến để thâm nhập vào hệ thống.

2.2. Rủi ro đến từ nhân viên

- Mất mật khẩu: Nhân viên sử dụng mật khẩu yếu, lưu mật khẩu ở nơi dễ truy cập hoặc chia sẻ mật khẩu với người khác.
- Chia sẻ dữ liệu nhạy cảm: Nhân viên chia sẻ dữ liệu nhạy cảm qua email không an toàn hoặc với người không được ủy quyền.
- Thiếu chính sách bảo mật: Nhân viên không tuân thủ chính sách bảo mật, như sử dụng thiết bị không an toàn, kết nối vào mạng không an toàn từ xa.
- Sử dụng USB không an toàn: Nhân viên sử dụng USB không an toàn hoặc chưa kiểm tra vệ sinh an ninh trước khi kết nối vào hệ thống.
- Thiếu chính sách phân quyền: Nhân viên có quyền truy cập không cần thiết đến dữ liệu quan trọng hoặc các khu vực hệ thống không liên quan đến công việc của họ.
- Mất thiết bị lưu trữ dữ liệu: Nhân viên mất điện thoại hoặc laptop chứa dữ liệu quan trọng mà không có biện pháp bảo vệ đủ.
- Không tuân thủ chính sách Backup: Nhân viên không thực hiện sao lưu dữ liệu đúng cách hoặc không thực hiện sao lưu định kỳ.

2.3. Bảng Risk Score của hệ thống hiện tại

Threat		Vulnerability	C	I	A	Imp	Exp	Fre	Ctrl	L	RS	RC
Agent	Action											
Attacker	Triển khai mã độc hại ransomware để mã hóa dữ liệu	Chưa có phần mềm quét các file hay nội dung độc hại	5	4	3	5	5	3	4	3	15	Cao

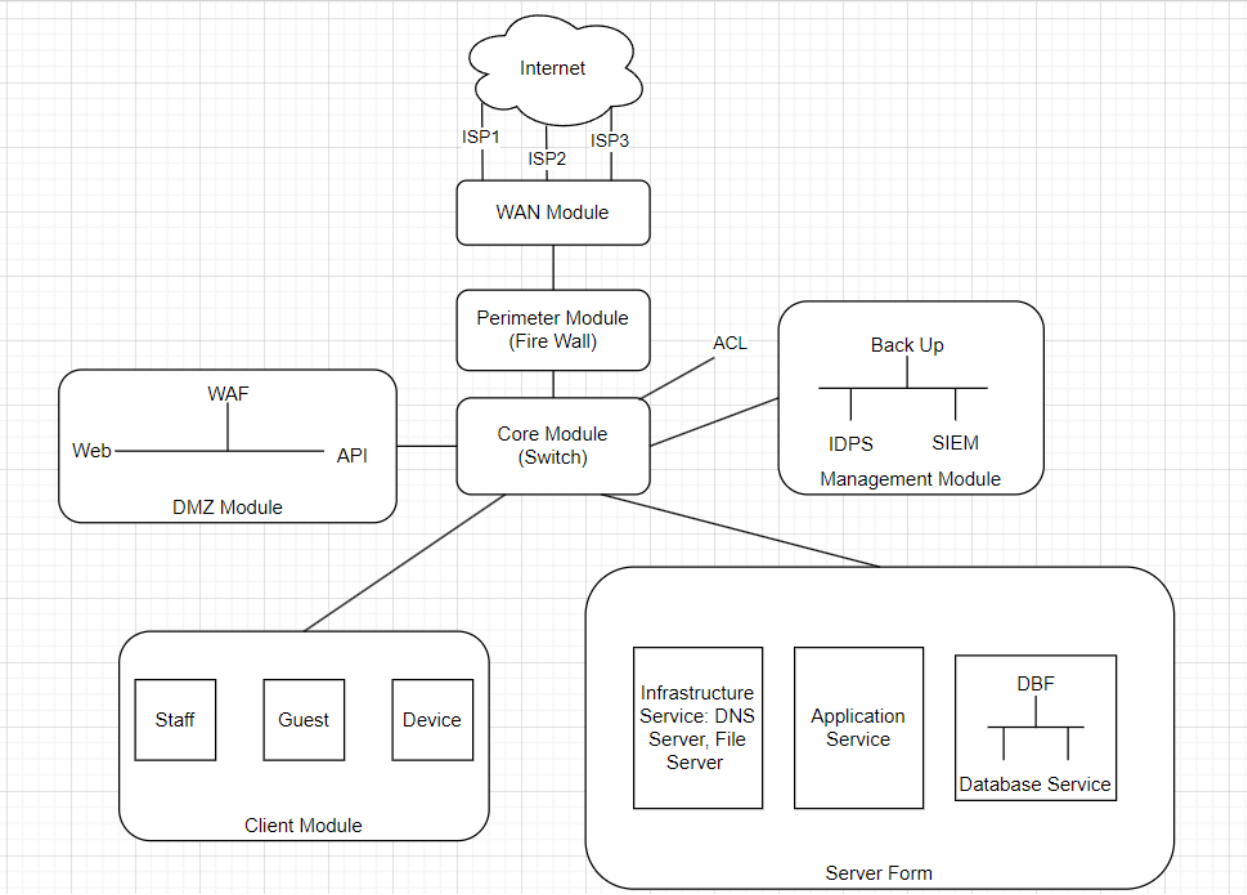
Attacker	Triển khai malware để thực hiện hoạt động gián điệp	Chưa có phần mềm quét các file hay nội dung độc hại	5	4	4	5	4	4	3	2	10	Trung bình
Attacker	Khai thác lỗ hổng phần mềm để xâm nhập hệ thống	Lỗ hổng phần mềm đang sử dụng	4	3	4	4	3	4	4	3	12	Trung bình
Attacker	Sử dụng email, tin nhắn giả mạo để lừa đảo người dùng	Thiếu nhận thức về an ninh	3	3	2	3	2	4	2	2	6	Thấp
Attacker	Sử dụng kỹ thuật xã hội để lừa đảo người dùng	Lừa đảo người dùng	2	3	3	3	3	3	3	1	3	Thấp
Attacker	Xâm nhập vào mạng nội bộ để thực hiện hoạt động gián điệp	Không chia VLAN cũng như phân vùng dữ liệu quan trọng	4	4	4	4	4	4	4	3	12	Trung bình
Attacker	Tận dụng lỗ hổng bảo mật	Lỗ hổng phần mềm đang sử dụng	4	4	4	4	4	2	3	3	12	Trung bình

	chưa được biết đến											
Attacker	Nghe lén	Chưa có các hệ thống mã hóa trong quá trình vận chuyển dữ liệu	4	3	3	4	4	4	4	3	12	Trung bình
User	Sử dụng mật khẩu yếu, lưu mật khẩu ở nơi dễ truy cập	Mật khẩu yếu nên dễ dàng bị brute - force	3	4	3	4	4	4	4	3	12	Trung Bình
User	Chia sẻ dữ liệu nhạy cảm qua email không an toàn	Quy trình chia sẻ dữ liệu không an toàn	3	3	2	3	2	3	2	3	9	Thấp
User	Không tuân thủ chính sách bảo mật	Thiếu các chính sách quản lý nhân sự về vấn để bảo mật thông tin	3	3	3	3	3	3	3	3	9	Thấp
User	Sử dụng USB không an toàn hoặc chưa kiểm tra	Không quét USB trước khi kết nối	5	3	3	5	4	4	4	3	15	Cao

	vệ sinh an ninh											
User	Bypass permission	Thiếu chính sách phân quyền	5	4	3	5	5	4	4	3	15	Cao
User	Mất điện thoại hoặc laptop chứa dữ liệu quan trọng	Thiểu khả năng bảo quản các thiết bị quan trọng	4	4	3	4	4	3	3	2	8	Trung bình
User	Không thực hiện sao lưu dữ liệu đúng cách	Không tuân thủ chính sách sao lưu	3	0	5	5	3	3	3	2	10	Trung Bình
Natural	Mất điện, thiên tai	Chưa có hệ thống backup dữ liệu và phục hồi dữ liệu sau thảm họa.	5	4	5	5	42	4	4	3	15	Cao

3. Các giải pháp bảo mật

3.1. Mô hình tổng thể



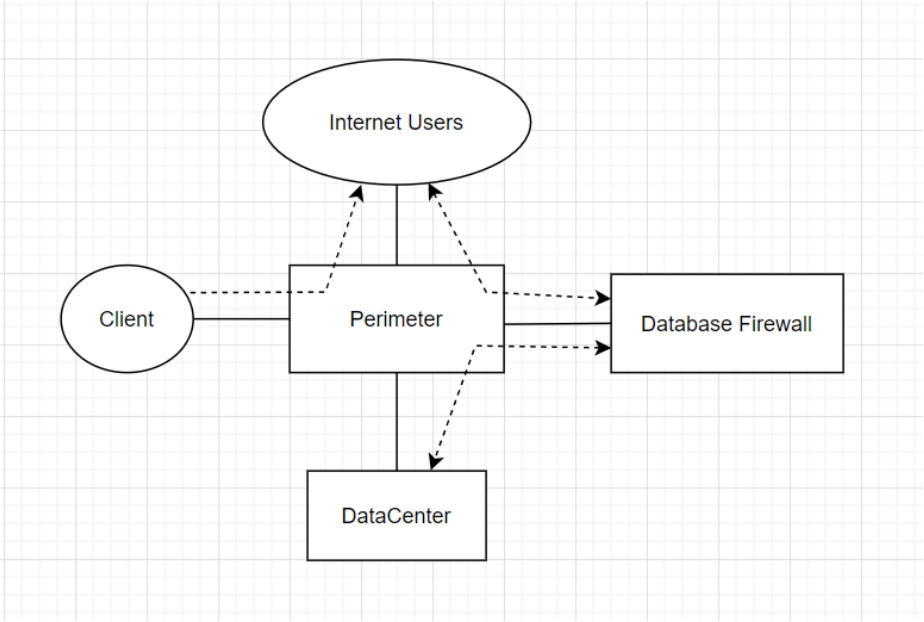
3.2. Thuyết minh giải pháp và vẽ mô hình chi tiết

3.2.1 Database Security (Bảo mật cơ sở dữ liệu):

- Tính năng:
  - + Mã hóa dữ liệu: Bảo vệ dữ liệu trong cơ sở dữ liệu bằng cách mã hóa nó để ngăn cản truy cập không ủy quyền.
  - + Quản lý quyền truy cập: Kiểm soát quyền truy cập vào cơ sở dữ liệu để đảm bảo chỉ người dùng có quyền được truy cập.

+ Giám sát hoạt động: Theo dõi và ghi lại các hoạt động trong cơ sở dữ liệu để phát hiện các sự cố bảo mật.
+ Kiểm tra và xác minh dữ liệu: Đảm bảo tính toàn vẹn của dữ liệu và kiểm tra xác thực.
+ Báo cáo và xử lý sự cố: Cung cấp khả năng báo cáo và xử lý sự cố liên quan đến cơ sở dữ liệu.

- Mô hình Database Security bằng Database Firewall:



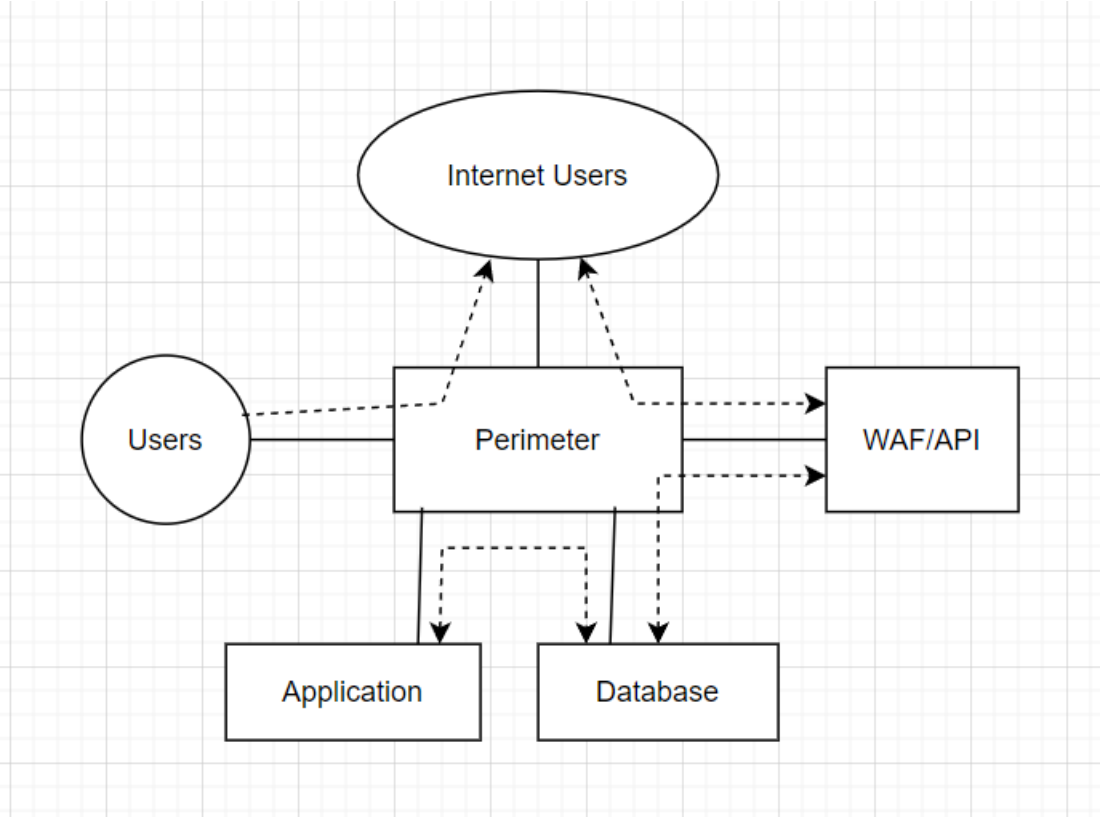
- Vị trí đặt: Database Firewall thường được triển khai ở cấp biên giới của mạng nội bộ và cơ sở dữ liệu. Nó giữ vai trò như một "lớp bảo vệ" cho cơ sở dữ liệu, kiểm soát lưu lượng truy cập và ngăn chặn các mối đe dọa như SQL injection.

3.2.2 Web Security (Bảo mật ứng dụng web):

- Tính năng:
  + Bộ lọc web và firewall ứng dụng web (WAF): Ngăn chặn các cuộc tấn công đối với ứng dụng web như SQL injection và XSS.

+ Quản lý phiên và xác thực: Đảm bảo xác thực người dùng và kiểm soát phiên làm việc.
+ Mã hóa kết nối: Sử dụng HTTPS để bảo vệ dữ liệu trên đường truyền.
+ Kiểm tra và lọc nội dung: Kiểm tra nội dung gửi và nhận trên ứng dụng web.
+ Giám sát hoạt động: Theo dõi hoạt động và lưu lượng truy cập ứng dụng web.

- Mô hình Web Security bằng WAP/API:



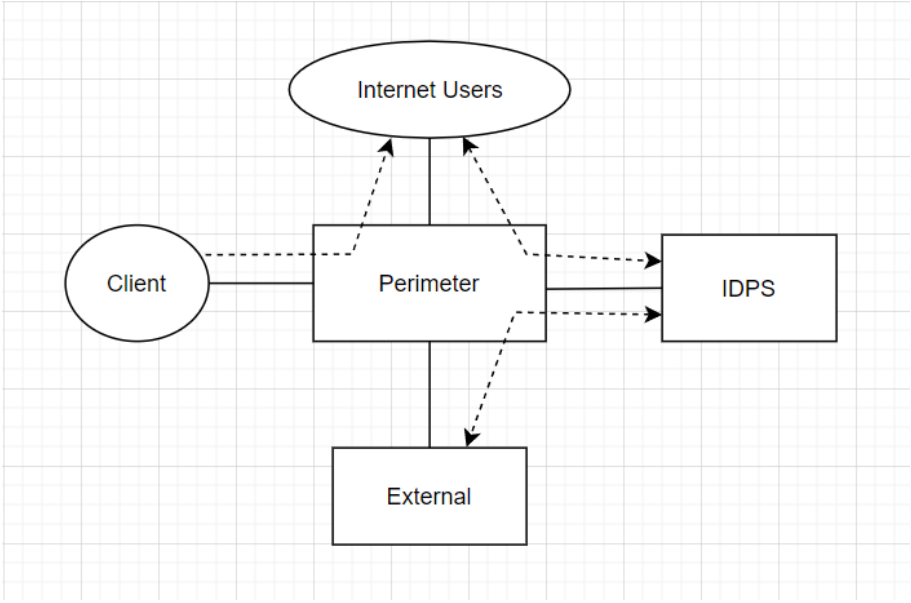
- Vị trí đặt: WAF/API thường được đặt ở phía trước ứng dụng web, giữa ứng dụng web và Internet. Cách đặt này giúp WAF/API có thể kiểm soát tất cả lưu lượng HTTP và HTTPS đi vào và đi ra khỏi ứng dụng web.

3.2.3 IDS/IPS Security (Bảo mật Hệ thống phát hiện và ngăn chặn xâm nhập):

- Tính năng:

+ Phát hiện xâm nhập: Theo dõi và phát hiện các hoạt động xâm nhập hoặc bất thường trong mạng.
+ Bảo vệ trước xâm nhập: Ngăn chặn các cuộc tấn công mạng và xâm nhập.
+ Kiểm tra và xác thực: Xác thực và kiểm tra các gói dữ liệu trên mạng.
+ Báo cáo và xử lý sự cố: Cung cấp cảnh báo và thông báo khi có sự xâm nhập và xử lý sự cố bảo mật.
+ Hạn chế hoặc ngăn chặn sự xâm nhập: Có thể kích hoạt các biện pháp tự động để ngăn chặn sự xâm nhập.

- Mô hình IDS/IPS Security bằng IDPS:



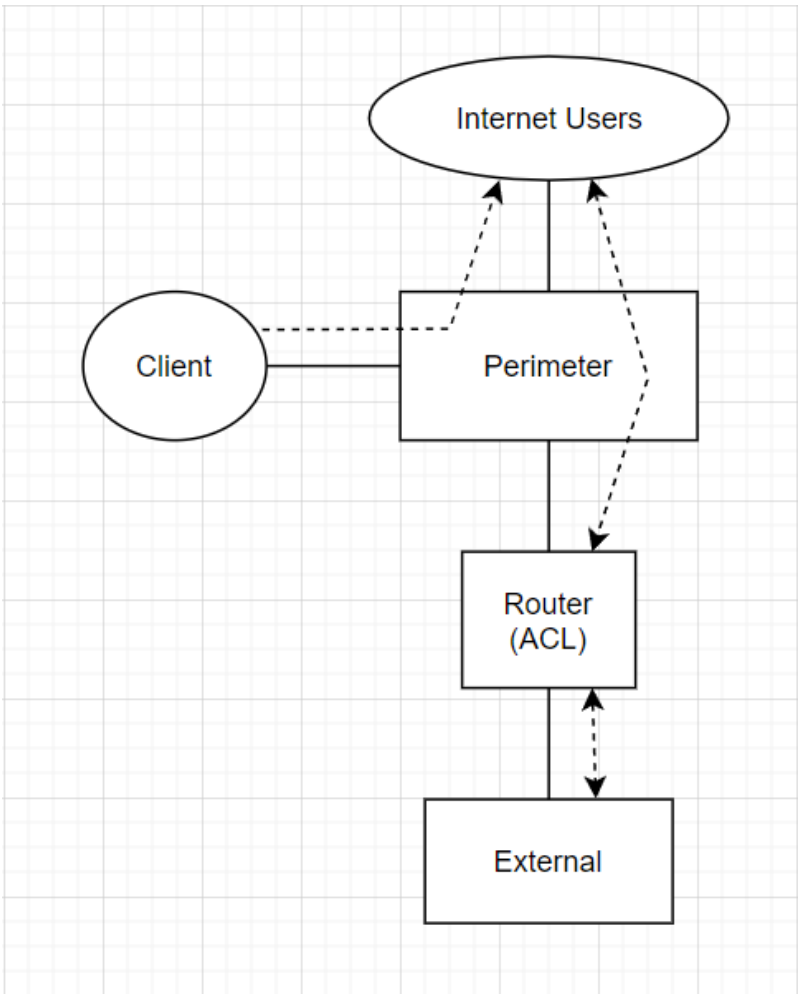
- Vị trí đặt: IDPS thường đặt ở nhiều điểm trong mạng, bao gồm cả biên giới và các điểm chiến lược như trước khi ra internet, trên các máy chủ chứa dữ liệu quan trọng để phát hiện và ngăn chặn các mô hình tấn công.

3.2.4 ACL Security (Bảo mật kiểm soát danh sách):

- Tính năng:

+ Kiểm soát quyền truy cập: Xác định và quản lý quyền truy cập vào các tài nguyên mạng dựa trên danh sách kiểm soát danh sách.
+ Ngăn chặn lưu lượng mạng không ủy quyền: Ngăn chặn truy cập không ủy quyền đối với mạng và tài nguyên.
+ Theo dõi và kiểm tra: Theo dõi lưu lượng mạng và kiểm tra tuân thủ chính sách kiểm soát danh sách.
+ Báo cáo và xử lý sự cố: Báo cáo về việc vi phạm và xử lý sự cố bảo mật.
+ Điều khiển lưu lượng: Kiểm soát lưu lượng mạng dựa trên danh sách kiểm soát danh sách.

- Mô hình ACL Security bằng ACL:



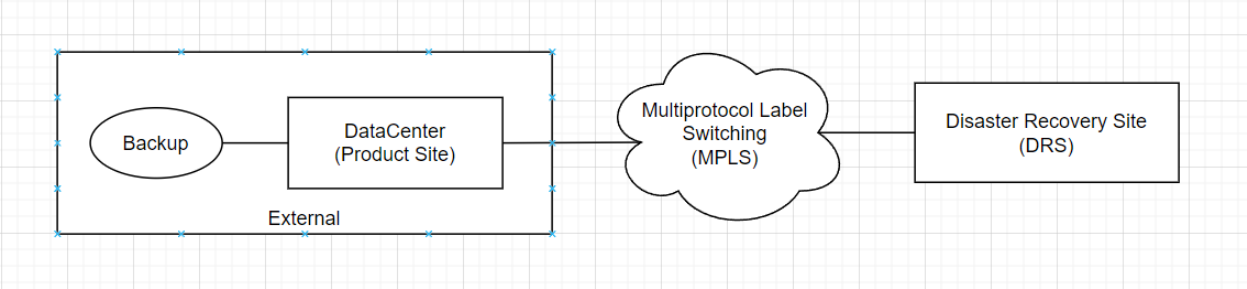
- Vị trí đặt: ACL thường được triển khai trên thiết bị mạng, chẳng hạn như router hoặc firewall. Nó kiểm soát quyền truy cập vào tài nguyên mạng dựa trên các quy tắc được đặt trước.

3.2.5 Backup và Phục Hồi Dữ Liệu:

- Tính Năng:
  + Sao Lưu Đầy Đủ và Tự Động: Tính năng này cho phép tự động tạo bản sao lưu đầy đủ của toàn bộ dữ liệu hệ thống, bao gồm cả cơ sở dữ liệu, tập tin hệ thống, và các tài nguyên khác.
  + Lập Kế Hoạch Sao Lưu Linh Hoạt: Cho phép lập kế hoạch sao lưu định kỳ theo các chu kỳ thời gian, đáp ứng nhu cầu của hệ thống và yêu cầu bảo mật dữ liệu.

+ Lưu Trữ An Toàn: Dữ liệu được sao lưu được lưu trữ một cách an toàn và có thể được giải mã chỉ bởi các người dùng được ủy quyền.
+ Kiểm Tra Tính Toàn Vẹn và Đảm Bảo: - Tính năng này kiểm tra tính toàn vẹn của dữ liệu sao lưu để đảm bảo rằng nó có thể phục hồi đúng đắn khi cần thiết.
+ Phục Hồi Linh Hoạt: Cung cấp khả năng phục hồi dữ liệu linh hoạt, từ toàn bộ hệ thống đến các phần cụ thể, để giảm thiểu thời gian tắt máy và mất mát dữ liệu.
+ Báo Cáo và Ghi Nhật Ký: Tạo báo cáo về quá trình sao lưu, bao gồm cả thông tin về thành công, thất bại, và bất thường. Ghi nhật ký giúp theo dõi và phân tích hoạt động sao lưu.
+ Nén Dữ Liệu: Tính năng này giúp giảm dung lượng lưu trữ bằng cách nén dữ liệu sao lưu mà không làm ảnh hưởng đến khả năng khôi phục.
+ Quản lý Phiên Bản: Hỗ trợ quản lý nhiều phiên bản sao lưu để người quản trị có thể chọn lựa phiên bản cụ thể để phục hồi, giúp đối phó với sự mất mát dữ liệu không mong muốn.
+ Bảo Mật: Các tùy chọn bảo mật như mã hóa và xác thực đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập và phục hồi dữ liệu sao lưu.

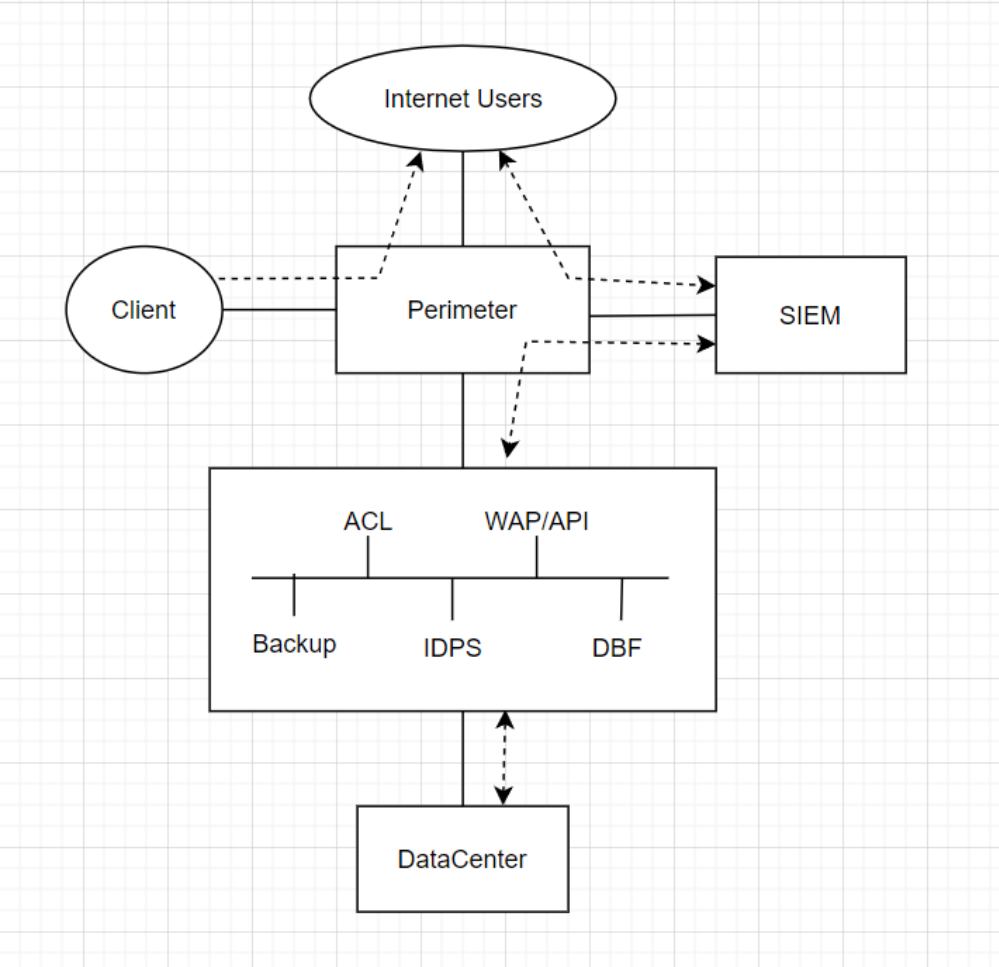
- Mô hình Database Security bằng Database Firewall:



- Vị trí đặt: DR Site nên được đặt ở một vị trí vật lý độc lập và có khoảng cách đủ xa đến primary site để tránh ảnh hưởng bởi cùng một thảm họa hay sự cố.

3.2.6 SIEM (Security Information and Event Management):

- Tính năng:
  - + Thu thập và tổng hợp dữ liệu bảo mật: Thu thập dữ liệu từ nhiều nguồn khác nhau để phân tích.
  - + Phát hiện và báo cáo sự cố bảo mật: Tìm kiếm các mẫu không bình thường và cảnh báo về sự cố bảo mật.
  - + Phân tích sự kiện: Phân tích các sự kiện và hoạt động bảo mật để xác định các hành vi đe dọa.
  - + Lưu trữ và xác minh sự kiện: Lưu trữ thông tin sự kiện để xác minh và điều tra sự cố.
  - + Tạo báo cáo và thông báo: Tạo báo cáo và thông báo cho người quản lý và nhân viên bảo mật.
- Mô hình SIEM:



- Vị trí đặt: SIEM thường được triển khai trên cấu trúc mạng để thu thập, tổng hợp, và phân tích dữ liệu từ nhiều nguồn khác nhau, bao gồm cả log của hệ thống, ứng dụng, và cơ sở dữ liệu.

4. *Xây dựng chính sách*

- Chính Sách An Toàn Thông Tin cho Bảo Mật Cơ Sở Dữ Liệu:
  - + Mã Hóa Dữ Liệu: Tất cả dữ liệu nhạy cảm phải được mã hóa cả khi đang được lưu trữ và khi truyền qua mạng.
  - + Quản Lý Quyền Truy Cập: Người dùng chỉ có quyền truy cập vào các phần cần thiết của cơ sở dữ liệu theo nguyên tắc "Least Privilege."

+ Giám Sát và Ghi Nhật Ký: Ghi lại mọi truy cập và thay đổi trong cơ sở dữ liệu, cảnh báo ngay lập tức khi có hoạt động đáng ngờ.

- Chính Sách An Toàn Thông Tin cho Bảo Mật Ứng Dụng Web:
  + Bộ Lọc Web và WAF: Ngăn chặn cuộc tấn công như SQL injection và XSS bằng cách sử dụng bộ lọc web và WAF.
  + Quản Lý Phiên và Xác Thực: Cài đặt cơ chế xác thực mạnh mẽ và quản lý phiên để đảm bảo chỉ có người dùng ủy quyền mới có thể truy cập.
  + Mã Hóa Kết Nối: Yêu cầu việc sử dụng HTTPS để bảo vệ dữ liệu truyền qua mạng.
  + Kiểm thử Bảo mật: Thường xuyên thực hiện các cuộc kiểm thử bảo mật ứng dụng web, bao gồm cả kiểm thử xâm nhập.
- Chính Sách An Toàn Thông Tin cho Bảo Mật Hệ Thống Phát Hiện và Ngăn Chặn Xâm Nhập (IDS/IPS Security):
  + Cấu hình Chuẩn: Cấu hình IPS/IDS để nhận biết và chặn các cuộc tấn công thông thường và phổ biến nhất đối với hệ thống ngân hàng.
  + Cập Nhật Thường Xuyên: Cập nhật định kỳ các chữ ký của hệ thống để nhận diện các mối đe dọa mới nhất.
  + Phản ứng Tự Động: Thiết lập hệ thống để tự động cách ly hoặc chặn lưu lượng mạng đáng ngờ.
  + Kiểm Tra và Xác Thực: Thực hiện kiểm tra và xác thực định kỳ trên các gói dữ liệu truyền qua mạng.
- Chính Sách An Toàn Thông Tin cho Bảo Mật Kiểm Soát Danh Sách (ACL Security):

+ Kiểm Soát Quyền Truy Cập: Xác định và quản lý quyền truy cập vào tài nguyên mạng dựa trên danh sách kiểm soát danh sách.
+ Ngăn Chặn Lưu Lượng Mạng Không Ủy Quyền: Kiểm soát và ngăn chặn lưu lượng mạng không ủy quyền đối với các tài nguyên.
+ Kiểm Tra Định Kỳ: Xem xét và cập nhật danh sách ACL định kỳ để đảm bảo rằng chúng vẫn phản ánh chính xác chính sách an ninh hiện hành.
+ Tối Thiểu Hóa Quyền Truy Cập: Theo nguyên tắc cấp quyền ít nhất cần thiết để thực hiện công việc.

- Chính Sách An Toàn Thông Tin cho SIEM (Quản Lý Thông Tin và Sự Kiện Bảo Mật):
  + Tập Trung Nhật Ký: Tập trung ghi nhật ký từ tất cả các hệ thống và thiết bị để giám sát hoạt động mạng toàn diện.
  + Phân Tích Thời Gian Thực: Phân tích dữ liệu nhật ký thời gian thực để phát hiện nhanh chóng các hoạt động đáng ngờ hoặc không bình thường.
  + Cảnh báo và Phản ứng: Cài đặt cảnh báo tự động cho các hoạt động đáng ngờ và tạo ra quy trình phản ứng sự cố tự động hoặc bán tự động.
- Chính Sách An Toàn Thông Tin cho Backup & Restore Data (Sao Lưu Và Phục Hồi Dữ Liệu):
  + Sao Lưu Dữ Liệu: Xác định tần suất và quy trình sao lưu dữ liệu từ primary site sang DR Site. Điều này bao gồm cả việc xác định RTO và RPO cho dữ liệu.
  + Đồng Bộ Dữ Liệu: Thiết lập quy tắc và tiêu chuẩn cho quá trình đồng bộ hóa dữ liệu giữa primary site và DR Site, đảm bảo tính tương đồng của dữ liệu.
  + Kiểm Tra và Bảo Duy Trì: Quy định các bài kiểm tra định kỳ và cuộc diễn tập để đảm bảo khả năng hoạt động của DR Site và chuẩn bị cho mọi tình huống khẩn cấp.

+ An Toàn và Bảo Mật: Thiết lập các biện pháp an toàn và bảo mật cho DR Site để ngăn chặn truy cập trái phép và bảo vệ dữ liệu khỏi mọi rủi ro.
+ Phục Hồi: Xác định quy trình cụ thể và trách nhiệm trong quá trình phục hồi tại DR Site. Bao gồm cả các bước cần thiết để khôi phục dữ liệu và hệ thống.
+ Giám Sát và Báo Cáo: Mô tả cách giám sát liên tục được thực hiện tại DR Site và cách thông tin cảnh báo và báo cáo được quản lý trong trường hợp sự cố.
+ Giao Tiếp Khẩn Cấp: Định rõ cách thông tin và giao tiếp được quản lý trong tình huống khẩn cấp, bao gồm cả việc thông báo cho nhân viên và các bên liên quan.
+ Bảo Dưỡng và Nâng Cấp: Quy định các kế hoạch bảo dưỡng định kỳ và nâng cấp cho DR Site để đảm bảo tính hiệu quả và đáng tin cậy.

V. LỜI CẢM ƠN

Trong thời gian học tập môn Quản lý rủi ro và an toàn thông tin trong doanh nghiệp, nhóm đã nhân được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, bạn bè. Với sự giúp đỡ này đã giúp nhóm rất nhiều trong việc cũng cố kiến thức và giải đáp những thắc mắc còn tồn đọng.

Nhóm xin gửi lời cám ơn chân thành đến thầy Nguyễn Duy, người đã tận tình hướng dẫn, chỉ bảo nhóm trong suốt quá trình làm đồ án.

Với những kiến thức đã được học tại môn này nhóm báo cáo có thể tự tin hơn trên chặng đường học tập sắp tới và trong cuộc sống sau này. Nhóm xin được chúc thầy và các cán bộ giảng viên đang công tác tại trường thật nhiều sức khỏe và thành công trong cuộc sống.

Hết !