**Quản lý rủi ro và an toàn thông tin trong doanh nghiệp**

**Chương 1: Tổng quan về an toàn thông tin**

|  |  |
| --- | --- |
| Information Security | * Confidentiality |
| * Integrity |
| * Availability |
| * Authorization |
| * Non-repudiation |

* Khái niệm:

Bảo mật thông tin là đảm bảo **tính bí mật, tính toàn vẹn** và **tính sẵn sàng** của thông tin trên các thiết bị lưu trữ, trong quá trình sử dụng và truyền thông.

* + Products (physical security)
  + People (personal security)
  + Procedures (organizational security)
* Security types:
* Physical Security
* Network Security
* Communication Security
* Software Security (OS & Application security) = built in security + secure operation
* Operation security
* Personal security
* Information security
* Risk là gì?

**Asse**t là bất kỳ dữ liệu, thiết bị hoặc thành phần nào khác của hệ thống trong một tổ chức có giá trị – thường là do nó chứa dữ liệu nhạy cảm hoặc có thể được sử dụng để truy cập thông tin như vậy.

Ví dụ, máy tính để bàn, laptop hoặc điện thoại công ty của nhân viên được coi là tài sản, cũng như các ứng dụng trên những thiết bị này. Tương tự, cơ sở hạ tầng quan trọng như máy chủ và hệ thống hỗ trợ cũng được coi là tài sản.

**Threat** là bất kỳ sự cố nào có thể ảnh hưởng tiêu cực đến một tài sản – ví dụ, nếu tài sản bị mất, bị gián đoạn hoạt động hoặc bị truy cập bởi một bên không được phép.

**Vulnerability** là một sai sót, lỗ hỏng trong tổ chức có thể bị khai thác bởi một mối đe dọa để phá hủy, làm hỏng hoặc gây tổn hại đến một tài sản.

* Một rủi ro an ninh thông tin (risk) phải bao gồm một thứ gì đó đang bị đe dọa (tài sản- asset), một tác nhân có thể khai thác nó (mối đe dọa - threat) và một cách mà điều đó có thể xảy ra (lỗ hổng - vulnerability).

A hand drawing a diagram

Description automatically generated

Risk Assessment:

1. Xác định các mối nguy tiềm ẩn
2. Xác định ai có thể bị ảnh hưởng bởi các mối nguy đó
3. Đánh giá rủi ro (mức độ nghiêm trọng và khả năng xảy ra) và thiết lập các biện pháp phòng ngừa phù hợp
4. Thực hiện các biện pháp kiểm soát và ghi lại kết quả
5. Diagram of a risk management diagram

   Description automatically generatedXem xét lại đánh giá của bạn và thực hiện đánh giá lại nếu cần thiết.

Risk Management:

* Xác định rủi ro.
* Đánh giá rủi ro.
* Lập kế hoạch rủi ro.
* Giám sát rủi ro

**Chương 2: Tổng quan về quản lý rủi ro an toàn thông tin**

* Rủi ro là gì?

Aprobability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities.

* Một khả năng hoặc mối đe dọa về thiệt hại, chấn thương, trách nhiệm pháp lý, tổn thất hoặc bất kỳ sự việc tiêu cực nào khác gây ra bởi các lỗ hổng bên ngoài hoặc bên trong.

A black arrow pointing towards an object

Description automatically generatedA black arrow pointing to a black arrow

Description automatically generated

* Sự tương tác giữa các thành phần

A diagram of a risk management

Description automatically generated

A diagram of a computer security system

Description automatically generated

* Đánh giá rủi ro trong an toàn thông tin:
* Xác định những tài sản nào cần bảo vệ

Database / Application / Hardware / Software / Processes / People / **impact** is the outcome, typically harmful, of a threat applied to an asset (Tác động là kết quả, thường mang tính chất gây hại, của một mối đe dọa được áp dụng lên một tài sản).

* Xác định lỗ hổng: vulnerability from Application / Operating Systems / Hardware Devices
* Xác định mối đe dọa
* Xác định khả năng xảy ra

**Likelihood** is the probability that a threat would exploit a vulnerability to affect an asset.

* Khả năng xảy ra (Likelihood) là xác suất mà một mối đe dọa sẽ khai thác một lỗ hổng để ảnh hưởng đến một tài sản.
* Xác định cơ chế kiểm soát

**Controls** are mechanisms that detect or prevent threats sources from leveraging vulnerabilities and thus are closely tied to likelihood as it affects the probability of a risk.

* Các biện pháp kiểm soát (Controls) là các cơ chế giúp phát hiện hoặc ngăn chặn nguồn đe dọa lợi dụng các lỗ hổng, do đó chúng có liên quan chặt chẽ đến khả năng xảy ra (Likelihood) vì ảnh hưởng đến xác suất của một rủi ro.
* Xác định mức độ rủi ro của các loại tài sản ➢ Xác định phương pháp bảo vệ tài sản ➢ Xác định nguồn lực cần bảo vệ tài sản ➢ Xác định ngân sách để triển khai chương trình bảo mật (security program)
* Những công việc quan trọng:

A diagram of a diagram

Description automatically generated with medium confidence

* Mục tiêu của đánh giá rủi ro

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

* Quá trình xác định các rủi ro đối với bảo mật hệ thống và đánh giá xác suất xảy ra, tác động kết quả, cũng như các biện pháp bảo vệ bổ sung nhằm giảm thiểu tác động này.
* Quy trình đánh giá rủi ro

A diagram of a risk assessment

Description automatically generated

A diagram of a risk assessment

Description automatically generated

* Drivers (trình điều khiển), Laws (luật), và Regulations (qui tắc)

A diagram of risk assessment

Description automatically generated

**FISMA** (Federal Information Security Modernization Act) là một đạo luật của Mỹ được ban hành vào năm 2002, yêu cầu các cơ quan liên bang và các tổ chức hợp đồng với chính phủ phải bảo vệ các hệ thống thông tin và dữ liệu của họ khỏi các mối đe dọa và lỗ hổng bảo mật.

**GLBA** (Gramm-Leach-Bliley Act) là một đạo luật của Mỹ được ban hành vào năm 1999, nhằm bảo vệ thông tin tài chính cá nhân của khách hàng. Đạo luật này yêu cầu các tổ chức tài chính (ngân hàng, công ty bảo hiểm, công ty chứng khoán, v.v.) phải có các biện pháp bảo mật và bảo vệ thông tin cá nhân của khách hàng.

**HIPAA** (Health Insurance Portability and Accountability Act) là một đạo luật của Mỹ được ban hành vào năm 1996, nhằm bảo vệ thông tin sức khỏe cá nhân của bệnh nhân và cải thiện hiệu quả của hệ thống chăm sóc sức khỏe.

* Quy trình quản lý rủi ro an toàn thông tin

A diagram of information security

Description automatically generated

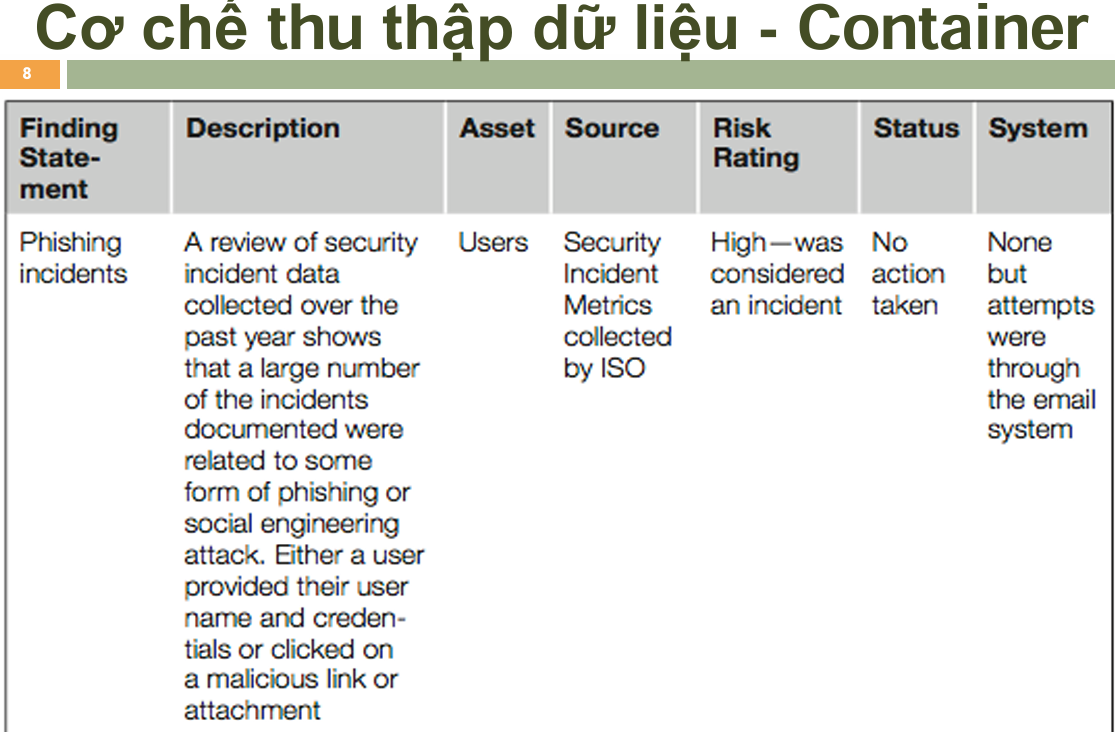
1. **Hồ sơ tài nguyên:** mô tả tài nguyên và đánh giá mức độ nhạy cảm với rủi ro (chủ sở hữu doanh nghiệp).
2. **Đánh giá rủi ro:** xác định và đánh giá các mối đe dọa, lỗ hổng và rủi ro (an ninh thông tin).
3. **Đánh giá rủi ro:** quyết định chấp nhận, tránh, chuyển giao hoặc giảm thiểu rủi ro (an ninh thông tin và chủ sở hữu doanh nghiệp).
4. **Tài liệu:** ghi lại các quyết định liên quan đến rủi ro, bao gồm các ngoại lệ và kế hoạch giảm thiểu (an ninh thông tin và chủ sở hữu doanh nghiệp).
5. **Giảm thiểu rủi ro:** triển khai các kế hoạch giảm thiểu với các biện pháp kiểm soát được chỉ định (người quản lý tài nguyên).
6. **Xác nhận:** kiểm tra các biện pháp kiểm soát để đảm bảo mức độ rủi ro thực tế phù hợp với các mức độ rủi ro mong muốn (an ninh thông tin).
7. **Giám sát và kiểm toán:** liên tục theo dõi các thay đổi đối với hệ thống có thể ảnh hưởng đến hồ sơ rủi ro và thực hiện các cuộc kiểm toán định kỳ (an ninh thông tin và chủ sở hữu doanh nghiệp).

**Chương 3: QUI TRÌNH ĐÁNH GIÁ RỦI RO (RISK ASSESSMENT)**

* Cơ chế thu thập dữ liệu – Những loại dữ liệu cần được thu thập:
  + System profiles
  + Control profiles
  + Audit report
  + Vulnerability assessments
  + Various information security event and metrics
* Phương pháp thu thập: Yêu cầu tài liệu, Khảo sát, Phỏng vấn

Container là những tài nguyên mà ở đó dữ liệu thu thập được lưu trữ. Ví dụ: Table of Database, Spreadsheet,…

4 container phổ biến: ➢ Finding ➢ Assets ➢ Risk ➢ Reference data



Assets gồm có ➢ Asset Name. ➢ Asset Classification. ➢ Control Information (multiple sub-elements).

A screenshot of a computer

Description automatically generated

* Phân tích dữ liệu
  + Phân tích và thiết kế tác động

Confidentiality

A close-up of a list

Description automatically generated

Integrity

A screen shot of a matrix

Description automatically generated

Availability

A screen shot of a computer

Description automatically generated

* + Phân tích và thiết kế cơ chế kiểm soát

|  |  |
| --- | --- |
| Bảo vệ dữ liệu | Cấp quyền người dùng |
| Quản lý bản vá | Mã hóa truyền dữ liệu |
| Mật khẩu phức tạp | Phần mềm diệt virus/HIPS |
| Quản lý lỗ hổng | Quản lý tài khoản |
| Cấu hình bảo mật | Cách ly bảo mật |
| Kiểm soát xác thực | Ghi nhật ký và giám sát |
| Giám sát IDS/IPS | Mã hóa lưu trữ |
| Sao lưu doanh nghiệp | Dự phòng và chuyển đổi dự phòng |
| Kế hoạch BCP/DR (Kế hoạch Kinh doanh Liên tục/Phục hồi sau Thảm họa) | Kiểm soát Thay đổi |
| Nâng cao nhận thức về an ninh |  |

* + Phân tích và thiết kế xác suất có thể xảy ra

**Mức độ Phơi nhiễm (Exposure)**

➢ Mức độ phơi nhiễm là khả năng hệ thống dễ bị ảnh hưởng bởi mối đe dọa dựa trên các yếu tố môi trường.  
➢ Ví dụ, nếu một tài sản được kết nối với Internet, thì xác suất bị xâm nhập hệ thống bởi những kẻ tấn công bên ngoài sẽ tăng lên.

**Chương 4: Access Control**

* Tổng quan về kiểm soát truy cập

**Kiểm soát truy cập** là kiểm soát cách người dùng và hệ thống giao tiếp và tương tác với các hệ thống và các tài nguyên khác.

Mục đích: bảo vệ hệ thống và các tài nguyên từ các truy cập trái phép.

Được chia thành 2 phần: Access và Control

* + Access là quá trình truy cập các tài nguyên của một chủ thể (Subject) tới một đối tượng (Object)
  + Control là hành động cho phép hoặc không cho phép truy cập, cũng như các phương thức áp dụng cho Access Control

4 bước diễn ra trong quá trình Subject truy cập Object:

1. **Identification (định danh)**

* Subjects cung cấp thông tin nhận dạng
* Username, userID, account number, …

1. **Authentication (xác thực)**

* Xác minh thông tin định danh
* Passphrase, PIN value, biometric, one-time password, password, …

1. **Authorization (Phân quyền)**

* Mức độ truy cập của các Subject lên các Object

1. **Accountability (Theo vết)**

* Theo dõi các hành động của các Subject lên các Object

Những câu hỏi phổ biến các doanh nghiệp ngày nay thường đặt ra để quản lý kiểm soát quyền truy cập vào tài sản:

* Phân loại đối tượng truy cập (nhân viên, khách hàng và đối tác,…)
* Yếu tố dùng để xác minh khi truy cập?
* Phương thức xác thực khi truy cập?
* Người dùng được truy cập vào đâu?
* Ai là người phê duyệt cho phép truy cập?
* Theo dõi quá trình truy cập của người dùng
* Cách thức thu hồi quyền truy cập
* Mô hình kiểm soát truy cập

Mô hình kiểm soát truy cập là một khuôn khổ (framework) dùng để qui định như thế nào Subject truy cập Object.

Có 3 mô hình kiểm soát truy cập chính

* Discretionary Access Control
* Mandatory Access Control
* Role-Based Access Control

Những mô hình này được xây dựng tích hợp vào lõi hoặc hạt nhân của hệ điều hành.

* Discretionary Access Control (DAC)

Cho phép chủ sở hữu của tài nguyên chỉ định các đối tượng có thể truy cập tài nguyên của mình.

Mô hình này được gọi là tùy ý (Discretionary) vì sự kiểm soát truy cập dựa trên quyết định của chủ sở hữu.

* Network: ACLs, Rule of Firewall, …
* System: Sharing Permission, NTFS, …
* Mandatory Access Control (MAC)

Một hệ điều hành dựa trên một mô hình MAC làm giảm đáng kể số lượng quyền, quyền hạn, chức năng của người sử dụng cho các mục đích an ninh.

* Người dùng bình thường không thể cài phần mềm
* Không thể tạo, xóa và sửa thông tin người dùng khác
* Không thể thay đổi cấu hình: IP, quyền hạn trên tài nguyên dùng chung, …
* Role-Based Access Control (RBAC)

Mô hình quản lý tập trung và phân nhóm các quyền truy cập

A diagram of access control

Description automatically generated

* Kỹ thuật kiểm soát truy cập

Sau khi quyết định hình mô hình kiểm soát truy cập sẽ sử dụng trong hệ thống bước tiếp theo cần phải xác định các kĩ thuật và công nghệ để hỗ trợ mô hình đó.

* Rule-BasedAccessControl

Sử dụng quy tắc cụ thể để chỉ định những gì có thể và không có thể xảy ra giữa một chủ thể và một đối tượng.

A diagram of a person's life cycle

Description automatically generated

* Constrained User Interfaces

Hạn chế khả năng truy cập của người sử dụng bằng cách không cho phép họ yêu cầu chức năng hoặc thông tin nào đó, hoặc có quyền truy cập vào tài nguyên hệ thống cụ thể.

Ba loại chính của Constrained User Interfaces:

* Menus và shells
* Database views
* Physically constrained interfaces
* Access Control Matrix

Ma trận kiểm soát tru y cập là một bảng của các chủ thể và các đối tượng cho thấy những hành động chủ thể cá nhân có thể thao tác trên đối tượng cá nhân.

A table with text on it

Description automatically generated

* Content-Dependent Access Control

Kiểm soát việc truy cập vào đối tượng dựa vào nội dung của đối tượng đó.

Dựa vào ngữ cảnh và thông tin thu thập được để kiểm soát truy cập

Thường chỉ có ở những công nghệ mới sau này: Next Generation Firewall, IDS/IPS, Unified Threat Management,

* Quản trị kiểm soát truy cập

Đầu tiên một tổ chức phải lựa chọn mô hình điều khiển truy cập (DAC, MAC, RBAC)

Sau đó tổ chức phải lựa chọn và thực hiện công nghệ kiểm soát truy cập

Quản lý điều khiển truy cập có hai hình thức cơ bản:

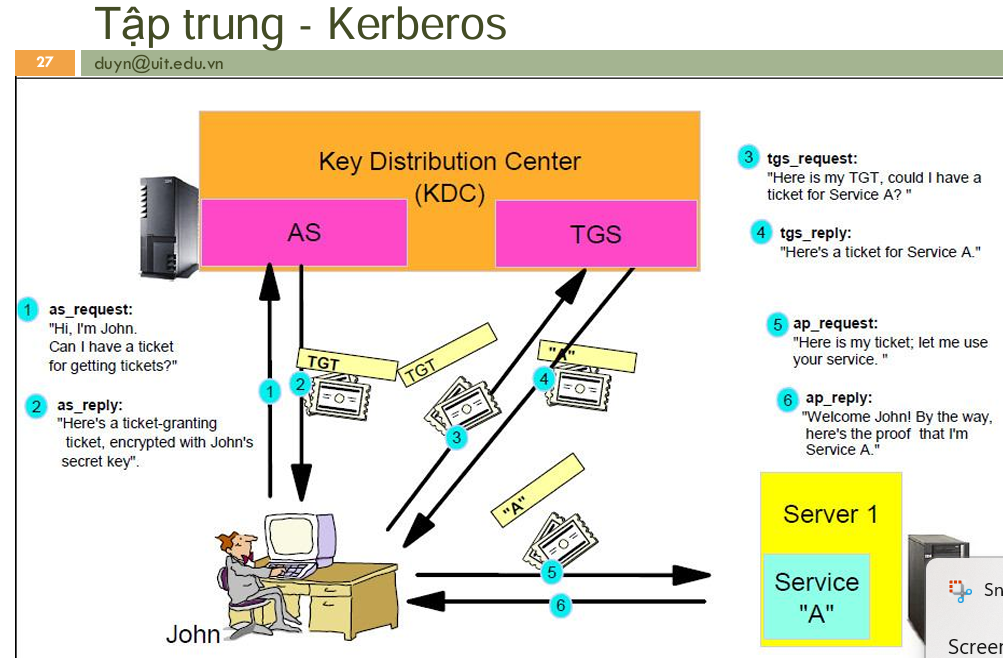
* Centralized (tập trung)
* Decentralized (không tập trung)
* Quản trị kiểm soát truy cập **Tập trung**

Một thực thể có trách nhiệm giám sát truy cập vào tất cả các tài nguyên của tổ chức.

Cung cấp một phương pháp phù hợp và thống nhất kiểm soát quyền truy cập.

Mỗi một giao thức xác thực cần tham chiếu tới giao thức AAA (authentication, authorization, và auditing)

Kiến trúc Client/Server: Kerberos, RADIUS, Terminal Access Controller Access Control System(TACACS), …



* Quản trị kiểm soát truy cập **Không tập trung**

Cho phép người dùng tự kiểm soát truy cập => Tự chia sẽ dữ liệu

Không có phương pháp kiểm soát phù hợp và thiếu nhất quán.

* Phương thức kiểm soát truy cập

Kiểm soát truy cập có thể được thực hiện ở các tầng khác nhau của một tổ chức, mạng lưới và hệ thống cá nhân.

* Phương thức kiểm soát truy cập **Hành chính**
  + Chính sách và qui trình truy cập
  + Kiểm soát con người
  + Cơ cấu giám sát
  + Đào tạo nâng cao nhận thức an ninh
  + Kiểm tra
* Phương thức kiểm soát truy cập **Vật lý**
  + Network Segregation
  + Perimeter Security
  + Computer Controls
  + Work Area Separation
  + Data Backups
  + Cabling
  + Control Zone
* Phương thức kiểm soát truy cập **Kĩ thuật (logic)** 
  + System Access
  + Network Access
  + Network Architecture
  + Encryption and protocols
  + Auditing
* Theo vết (Accountability) truy cập

Quá trình theo dõi hành động của Users, System và Applications

Quá trình theo dõi hành động này sẽ được thực thi bởi hệ điều hành và ứng dụng

Kết quả của quá trình theo dõi:

* Phải được lưu trữ
* Dung lượng lưu trữ
* Thời gian lưu trữ
* Ai được quyền truy cập
* Ai được quyền xóa

System-level events: log, Devices used, Functions performed

Application-level events: Error messages, Files opened and closed, Modifications of files

User-level events: Identification and authentication attempts, Files, services, and resources used

* Giám sát truy cập

Giám sát kiểm soát truy cập là một phương pháp theo dõi của những chủ thể (người dùng và ứng dụng) cố gắng để truy cập tài nguyên. Một trong những giải pháp giám sát truy cập nổi tiếng

* Intrusion Detection
* IntrusionPrevention
* Honeypot
* Packet Sniffer
* Networking Activities

|  |  |
| --- | --- |
| Intrusion Detection có 3 thành phần chính   * Sensor * Analyzers * Administrator Interface   Intrusion Detection có 2 loại chính:   * Network Based (NIDS) * Host Based (HIDS)   Nhiệm vụ chính của IDS:   * Giám sát * Phân tích * Cảnh báo * Báo cáo | Intrusion Prevention có 3 thành phần chính   * Sensor * Analyzers * Administrator Interface   Intrusion Prevention có 2 loại chính:   * Network Based (NIDS) * Host Based (HIDS)   Nhiệm vụ chính của IDS:   * Giám sát * Phân tích * Cảnh báo * Báo cáo * Phản ứng |
| Honeypots   * Một máy tính được sử dụng để thu hút người tấn công * Thu thập thông tin cuộc tấn công | Network sniffers   * Các chương trình hoặc các thiết bị có khả năng kiểm tra gói tintrên một phân đoạn mạng LAN. |

* Những mối đe dọa với kiểm soát truy cập

Dictionary Attack

Một số chương trình có thể cho phép kẻ tấn công (hoặc quản trị viên chủ động) xác định người sử dụng thông tin

Biện pháp đối phó:

* Mã hóa password (lưu trữ và khi truyền)
* Băm password (hashing)
* One-time password
* Chính sách thay đổi password và lịch sử thay đổi
* Bảo vệ hệ thống lưu trữ password
* Giới hạn số lần logon sai
* IDS

BruteForce Attacks

Cố gắng kết hợp tất cả các yếu tố có thể cho đến khi Password được xác định

Biện pháp đối phó:

* Mã hóa password (lưu trữ và khi truyền)
* Băm password (hashing)
* One-time password
* Chính sách thay đổi password và lịch sử thay đổi
* Bảo vệ hệ thống lưu trữ password
* Giới hạn số lần logon sai
* IDS

Spoofing at Logon

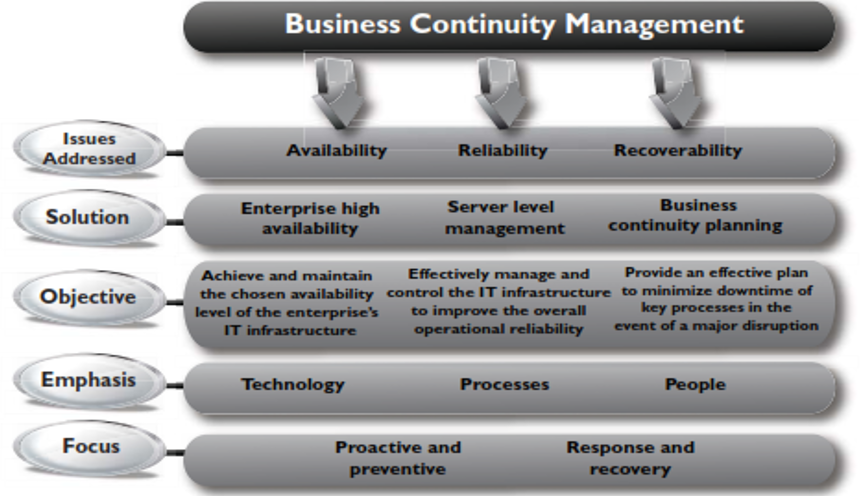
Người tấn công sử dụng chương trình để đưa người dùng đến màn hình logon giả mạo với mục đích đánh lừa người dùng logon. Sau khi logon thì thông tin tài khoản đã được lưu trữ trên hệ thống của attacker.

Biện pháp đối phó:

* IP Security
* SSL
* Mutual authentication

**Chương 5:** **Quản lí tính liên tục của hệ thống và khôi phục hệ thống sau thảm họa**

* Business Continuity Planning (BCP)



* Disaster Recovery Planning (DRP)

A screenshot of a white paper

Description automatically generated

* Các giai đoạn trong BCP
* Project management & initiation
  + Phân tích rủi ro
  + Hỗ trợ quản lý
  + Thành lập nhóm
  + Lên kế hoạch (phạm vi, mục tiêu, phương án và thời gian)
* Business Impact Analysis (BIA)
  + Mục tiêu:
    - Có được thỏa thuận chính thức với các quản lý cấp cao với MTD cho mỗi nguồn tài nguyên kinh doanh quan trọng
    - MTD - thời gian chết tối đa chấp nhận được, còn được gọi là MAO (tối đa cho phép Cúp)
  + Định lượng tổn thất do mất điện (tài chính và thêm chi phí phục hồi)
  + Không đánh giá khả năng của các loại sự cố, chỉ định lượng những hậu quả
  + Những giai đoạn trong BIA
    - Chọn phương pháp thu thập thông tin (điều tra, phỏng vấn, các công cụ phần mềm)
    - Chọn người được phỏng vấn
    - Tùy chỉnh các câu hỏi
    - Phân tích thông tin
    - Xác định thời điểm quan trọng trong hoạt động kinh doanh
* A diagram of a process

  Description automatically generatedRecovery strategies (hình kế bên)
  + Chiến lược phục hồi dựa trên MTDs
  + Được xác định trước
  + Quản lý chấp thuận
* Plan design & development
  + Kế hoạch chi tiết cho việc phục hồi
  + Nâng cao nhận thức và đào tạo
  + Thử nghiệm
* Testing, maintenance, awareness, training

**Chương 6: PCI DSS**

Có ba bước liên tục cần thực hiện để tuân thủ PCI DSS:

1. **Đánh giá (Assess)** – Xác định tất cả các vị trí lưu trữ dữ liệu chủ thẻ, kiểm kê tài sản CNTT và các quy trình kinh doanh liên quan đến xử lý thẻ thanh toán, đồng thời phân tích các lỗ hổng có thể gây rò rỉ dữ liệu chủ thẻ.
2. **Sửa chữa (Repair)** – Khắc phục các lỗ hổng đã xác định, loại bỏ một cách an toàn mọi dữ liệu chủ thẻ không cần thiết và triển khai các quy trình kinh doanh an toàn.
3. **Báo cáo (Report)** – Lập tài liệu chi tiết về quá trình đánh giá và khắc phục, sau đó gửi báo cáo tuân thủ đến ngân hàng chấp nhận thanh toán và các thương hiệu thẻ (hoặc các bên yêu cầu nếu bạn là nhà cung cấp dịch vụ).

Các tiêu chuẩn bảo mật PCI là những yêu cầu kỹ thuật và vận hành được thiết lập bởi Hội đồng Tiêu chuẩn Bảo mật PCI (**PCI Security Standards Council** - PCI SSC) nhằm bảo vệ dữ liệu chủ thẻ. protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted.

* **Tiêu chuẩn Bảo mật Dữ liệu PCI (PCI DSS)**

PCI DSS áp dụng cho tất cả các tổ chức lưu trữ, xử lý và/hoặc truyền dữ liệu chủ thẻ.

* **Yêu cầu về Bảo mật Giao dịch PIN (PTS)**

PCI PTS là một bộ yêu cầu bảo mật tập trung vào các đặc điểm và quản lý thiết bị được sử dụng để bảo vệ mã PIN của chủ thẻ và các hoạt động liên quan đến xử lý thanh toán. Tiêu chuẩn PTS bao gồm:

* Yêu cầu Bảo mật PIN - PIN Security Requirements
* Yêu cầu Bảo mật Modun Tương tác Điểm (POI) - Point of Interaction (POI) Modular Security Requirements
* Yêu cầu Bảo mật Modun Phần cứng (HSM) - Hardware Security Module (HSM) Security Requirements
* **Tiêu chuẩn Bảo mật Dữ liệu Ứng dụng Thanh toán (PA-DSS)**

PA-DSS được thiết kế cho các nhà cung cấp phần mềm và những cá nhân phát triển ứng dụng thanh toán có chức năng lưu trữ, xử lý hoặc truyền dữ liệu chủ thẻ và/hoặc dữ liệu xác thực nhạy cảm như một phần của quá trình ủy quyền hoặc thanh toán.

* **Tiêu chuẩn Mã hóa Point – to – Point PCI (P2PE)**

Tiêu chuẩn Mã hóa Điểm-điểm (P2PE) cung cấp một bộ yêu cầu bảo mật toàn diện cho các nhà cung cấp giải pháp P2PE nhằm xác thực các giải pháp của họ. P2PE là một chương trình đa chức năng, dẫn đến việc xác thực các giải pháp tích hợp các tiêu chuẩn PTS, PA-DSS, PCI DSS và Tiêu chuẩn Bảo mật PIN PCI.

* **Yêu cầu Bảo mật Logic và Bảo mật Vật lý trong Sản xuất Thẻ PCI**

Các yêu cầu Bảo mật Logic và Bảo mật Vật lý trong Sản xuất Thẻ đề cập đến các hoạt động sản xuất thẻ bao gồm: sản xuất thẻ, gắn chip, chuẩn bị dữ liệu, …

* **Yêu cầu Bảo mật cho Nhà cung cấp Dịch vụ Mã hóa Thẻ PCI (Token Service Provider - TSP)**

Yêu cầu Bảo mật cho Nhà cung cấp Dịch vụ Mã hóa Thẻ được thiết kế dành cho các Nhà cung cấp TSP, chịu trách nhiệm tạo và phát hành Mã hóa Thanh toán EMV, theo định nghĩa trong Khung Kỹ thuật Tiêu chuẩn Mã hóa Thanh toán EMV.

* **Tiêu chuẩn Bảo mật Dữ liệu PCI (PCI DSS)**

PCI DSS là tiêu chuẩn bảo mật dữ liệu toàn cầu được các thương hiệu thẻ thanh toán áp dụng cho tất cả các tổ chức xử lý, lưu trữ hoặc truyền dữ liệu chủ thẻ và/hoặc dữ liệu xác thực nhạy cảm.

A table with text on it

Description automatically generated

**Build and Maintain a Secure Network and Systems**

**Yêu cầu 1: Cài đặt và duy trì cấu hình tường lửa để bảo vệ dữ liệu chủ thẻ**

Tường lửa là các thiết bị kiểm soát lưu lượng máy tính được phép vào và ra khỏi mạng của tổ chức, cũng như vào các khu vực nhạy cảm trong mạng nội bộ. Bộ định tuyến (router) là phần cứng hoặc phần mềm kết nối hai hoặc nhiều mạng.

1. **Cấu hình tiêu chuẩn**: Thiết lập tiêu chuẩn cấu hình cho tường lửa và bộ định tuyến, kiểm tra khi có thay đổi, tài liệu hóa kết nối và luồng dữ liệu. Xem xét định kỳ 6 tháng một lần.
2. **Hạn chế lưu lượng**: Chỉ cho phép lưu lượng cần thiết cho môi trường dữ liệu chủ thẻ, từ chối tất cả các lưu lượng không tin cậy.
3. **Cấm truy cập công khai**: Không cho phép kết nối trực tiếp từ Internet đến các hệ thống trong môi trường dữ liệu chủ thẻ.
4. **Tường lửa cá nhân**: Cài đặt tường lửa cá nhân trên các thiết bị truy cập Internet bên ngoài mạng nội bộ nhưng có kết nối với dữ liệu chủ thẻ.
5. **Chính sách và quy trình**: Đảm bảo các chính sách bảo mật và quy trình vận hành được tài liệu hóa, thực thi và phổ biến tới tất cả các bên liên quan.

**Yêu cầu 2: Không sử dụng mật khẩu mặc định của nhà cung cấp cho hệ thống và các tham số bảo mật khác**

Việc giữ nguyên mật khẩu hoặc cài đặt mặc định của hệ thống là một trong những cách dễ dàng nhất để hacker xâm nhập vào mạng nội bộ của bạn.

**Tóm tắt Yêu cầu 2: Không sử dụng cài đặt mặc định của nhà cung cấp**

1. **Thay đổi mặc định**: Luôn thay đổi mật khẩu mặc định và gỡ bỏ/vô hiệu hóa tài khoản không cần thiết trước khi triển khai hệ thống.
2. **Tiêu chuẩn cấu hình**: Xây dựng và cập nhật tiêu chuẩn cấu hình hệ thống để xử lý các lỗ hổng bảo mật đã biết.
3. **Mã hóa truy cập quản trị**: Mã hóa tất cả truy cập quản trị không qua giao diện điều khiển bằng mật mã mạnh.
4. **Quản lý tài sản**: Duy trì danh sách các thành phần hệ thống liên quan đến PCI DSS.
5. **Chính sách bảo mật**: Đảm bảo các chính sách và quy trình bảo mật được tài liệu hóa, thực thi và phổ biến.
6. **Dịch vụ lưu trữ chia sẻ**: Nhà cung cấp lưu trữ chia sẻ phải bảo vệ môi trường của từng thực thể và dữ liệu chủ thẻ.

**Protect Cardholder Data**

Dữ liệu chủ thẻ là bất kỳ thông tin nào được in, xử lý, truyền tải hoặc lưu trữ dưới bất kỳ hình thức nào trên thẻ thanh toán.

**Yêu cầu 3: Bảo vệ dữ liệu chủ thẻ đã lưu trữ**

Dữ liệu chủ thẻ không nên được lưu trữ trừ khi cần thiết cho các nhu cầu kinh doanh. Dữ liệu nhạy cảm trên dải từ hoặc chip không bao giờ được lưu trữ sau khi xác thực. Nếu tổ chức của bạn lưu trữ PAN (Số tài khoản chủ thẻ), cần phải làm cho nó không thể đọc được

1. **Giới hạn lưu trữ**: Chỉ lưu trữ dữ liệu chủ thẻ khi cần thiết cho mục đích kinh doanh, pháp lý hoặc quy định, và xóa dữ liệu không cần thiết ít nhất mỗi quý.
2. **Không lưu trữ dữ liệu xác thực nhạy cảm**: Dữ liệu xác thực nhạy cảm phải được xóa ngay sau khi xác thực, ngay cả khi đã mã hóa.
3. **Mã hóa và ẩn dữ liệu**: Mã hóa PAN khi hiển thị và chỉ hiển thị tối đa sáu chữ số đầu và bốn chữ số cuối. Đảm bảo PAN không thể đọc được khi lưu trữ.
4. **Quản lý khóa mã hóa**: Tài liệu hóa và triển khai quy trình quản lý khóa mã hóa dữ liệu chủ thẻ, bảo vệ khỏi việc tiết lộ và lạm dụng.
5. **Chính sách và quy trình bảo mật**: Đảm bảo các chính sách và quy trình bảo mật được tài liệu hóa, thực thi và phổ biến đến tất cả các bên liên quan.

**Yêu cầu 4: Mã hóa truyền tải dữ liệu chủ thẻ qua các mạng mở và công cộng**

Tội phạm mạng có thể chặn các luồng dữ liệu chủ thẻ qua các mạng mở và công cộng, vì vậy việc ngăn chặn khả năng xem dữ liệu này là rất quan trọng. Mã hóa là một công nghệ có thể được sử dụng để làm cho dữ liệu truyền tải không thể đọc được bởi bất kỳ ai không được phép.

1. **Mã hóa mạnh**: Sử dụng mã hóa mạnh và các giao thức bảo mật để bảo vệ dữ liệu chủ thẻ trong quá trình truyền tải qua các mạng công cộng như Internet, mạng không dây và di động.
2. **Không gửi PAN chưa bảo vệ**: Không bao giờ gửi PAN qua các phương tiện nhắn tin không bảo vệ như email, SMS, hoặc chat.
3. **Chính sách bảo mật**: Đảm bảo các chính sách và quy trình bảo mật liên quan được tài liệu hóa, thực thi và phổ biến đến tất cả các bên liên quan.

**Duy trì Chương trình Quản lý Lỗ hổng**

Quản lý lỗ hổng là quá trình tìm kiếm có hệ thống và liên tục các điểm yếu trong hệ thống cơ sở hạ tầng thẻ thanh toán của một tổ chức. Điều này bao gồm các quy trình bảo mật, thiết kế hệ thống, triển khai hoặc các kiểm soát nội bộ có thể bị lợi dụng để vi phạm chính sách bảo mật hệ thống.

**Yêu cầu 5: Bảo vệ tất cả hệ thống khỏi phần mềm độc hại và thường xuyên cập nhật phần mềm diệt virus hoặc chương trình**

Phần mềm độc hại (hay còn gọi là "malware") khai thác lỗ hổng hệ thống sau khi xâm nhập vào mạng qua email của người dùng và các hoạt động kinh doanh trực tuyến khác. Phần mềm diệt virus phải được sử dụng trên tất cả các hệ thống thường xuyên bị ảnh hưởng bởi phần mềm độc hại để bảo vệ hệ thống khỏi các mối đe dọa phần mềm độc hại hiện tại và đang phát triển.

1. **Triển khai phần mềm diệt virus**: Cài đặt phần mềm diệt virus trên tất cả các hệ thống dễ bị phần mềm độc hại, như máy tính cá nhân và máy chủ, và đánh giá định kỳ đối với những hệ thống ít bị ảnh hưởng.
2. **Cập nhật và quét định kỳ**: Đảm bảo phần mềm diệt virus luôn cập nhật, thực hiện quét định kỳ và lưu trữ nhật ký kiểm tra theo yêu cầu của PCI DSS.
3. **Ngừng tắt hoặc thay đổi phần mềm diệt virus**: Đảm bảo phần mềm diệt virus không thể bị vô hiệu hóa hoặc thay đổi bởi người dùng, trừ khi có sự cho phép của quản lý.
4. **Chính sách bảo mật**: Đảm bảo các chính sách và quy trình bảo mật được tài liệu hóa, thực thi và được tất cả các bên liên quan biết đến.

**Yêu cầu 6: Phát triển và duy trì hệ thống và ứng dụng an toàn**

Các lỗ hổng bảo mật trong hệ thống và ứng dụng có thể tạo điều kiện cho tội phạm xâm nhập vào PAN và dữ liệu chủ thẻ khác. Nhiều lỗ hổng này có thể được khắc phục bằng cách cài đặt các bản vá bảo mật do nhà cung cấp cung cấp, giúp sửa chữa nhanh chóng mã lập trình cụ thể. Tất cả các hệ thống quan trọng phải được cài đặt các bản vá phần mềm mới nhất để ngăn chặn khai thác. Các tổ chức nên áp dụng các bản vá cho các hệ thống ít quan trọng hơn ngay khi có thể, dựa trên chương trình quản lý lỗ hổng dựa trên rủi ro. Các thực tiễn mã hóa an toàn khi phát triển ứng dụng, quy trình kiểm soát thay đổi và các phương pháp phát triển phần mềm an toàn khác cần luôn được tuân thủ.

**Triển khai các Biện pháp Kiểm Soát Truy Cập Mạnh Mẽ**

Kiểm soát truy cập cho phép các nhà bán lẻ cấp phép hoặc từ chối việc sử dụng các phương tiện vật lý hoặc kỹ thuật để truy cập vào PAN và các dữ liệu chủ thẻ khác.

* Kiểm soát truy cập vật lý bao gồm việc sử dụng khóa hoặc các phương tiện khác để hạn chế truy cập vào phương tiện máy tính, hồ sơ giấy hoặc phần cứng hệ thống.
* Kiểm soát truy cập logic cho phép hoặc từ chối việc sử dụng các thiết bị thanh toán, mạng không dây, máy tính cá nhân và các thiết bị tính toán khác, đồng thời kiểm soát truy cập vào các tệp số chứa dữ liệu chủ thẻ.

**Yêu cầu 7: Hạn chế quyền truy cập vào dữ liệu chủ thẻ theo nhu cầu công việc**

Để đảm bảo dữ liệu quan trọng chỉ có thể được truy cập bởi nhân viên được ủy quyền, các hệ thống và quy trình phải được thiết lập để giới hạn quyền truy cập dựa trên nhu cầu công việc và trách nhiệm công việc. "Nhu cầu công việc" có nghĩa là quyền truy cập chỉ được cấp cho một lượng dữ liệu và quyền hạn tối thiểu cần thiết để thực hiện công việc.

**Yêu cầu 8: Xác định và xác thực quyền truy cập vào các thành phần hệ thống**

Việc cấp một mã định danh (ID) duy nhất cho mỗi người có quyền truy cập giúp đảm bảo rằng các hành động thực hiện trên dữ liệu và hệ thống quan trọng được thực hiện bởi người dùng đã được xác thực và có thể truy dấu. Yêu cầu này áp dụng cho tất cả các tài khoản, bao gồm tài khoản điểm bán, tài khoản có quyền quản trị và tất cả các tài khoản có quyền truy cập vào dữ liệu chủ thẻ đã được lưu trữ. Yêu cầu này không áp dụng cho các tài khoản của người tiêu dùng (ví dụ, chủ thẻ).

1. Quản lý ID người dùng
2. Sử dụng ít nhất một trong các phương pháp xác thực (mật khẩu, thiết bị mã hóa, hoặc sinh trắc học) và mã hóa mạnh để bảo vệ mật khẩu trong quá trình truyền và lưu trữ.
3. Xác thực nhiều yếu tố

**Yêu cầu 9: Hạn chế quyền truy cập vật lý vào dữ liệu chủ thẻ**

Bất kỳ quyền truy cập vật lý nào vào dữ liệu hoặc hệ thống chứa dữ liệu chủ thẻ đều tạo cơ hội cho những người không được phép truy cập và/hoặc lấy thiết bị, dữ liệu, hệ thống hoặc bản sao cứng, và cần phải được hạn chế một cách thích hợp.

* "Nhân viên tại chỗ - onesite personnel" bao gồm nhân viên toàn thời gian, bán thời gian, nhân viên tạm thời, nhà thầu và tư vấn viên có mặt trực tiếp tại cơ sở của tổ chức.
* "Khách thăm – visitors” là các nhà cung cấp và khách tham quan vào cơ sở trong thời gian ngắn – thường là trong một ngày.
* "Phương tiện - media" là tất cả các phương tiện giấy và điện tử chứa dữ liệu chủ thẻ.

1. **Kiểm soát quyền truy cập cơ sở vật chất**: Sử dụng các biện pháp kiểm soát quyền truy cập phù hợp để giới hạn và giám sát quyền truy cập vật lý vào các hệ thống trong môi trường dữ liệu chủ thẻ.
2. **Phân biệt nhân viên và khách thăm**: Xây dựng quy trình để dễ dàng phân biệt giữa nhân viên và khách thăm, ví dụ bằng cách cấp thẻ ID.
3. **Đảm bảo khách thăm được cấp phép trước khi vào khu vực xử lý hoặc lưu trữ dữ liệu chủ thẻ**: Cấp thẻ nhận dạng và yêu cầu khách thăm trả lại thẻ khi rời đi hoặc hết hạn. Ghi chép thông tin khách thăm vào sổ đăng ký.

**Giám sát và Kiểm tra Mạng Định kỳ**

Mạng vật lý và mạng không dây là thành phần kết nối tất cả các điểm cuối và máy chủ trong hạ tầng thanh toán. Các lỗ hổng trong thiết bị và hệ thống mạng tạo ra cơ hội cho tội phạm truy cập trái phép vào các ứng dụng thẻ thanh toán và dữ liệu chủ thẻ. Để ngăn chặn việc khai thác, các tổ chức phải giám sát và kiểm tra mạng định kỳ để phát hiện và khắc phục các lỗ hổng.

**Yêu cầu 10: Theo dõi và giám sát tất cả quyền truy cập vào tài nguyên mạng và dữ liệu chủ thẻ**

Cơ chế ghi nhật ký và khả năng theo dõi hoạt động của người dùng là rất quan trọng để phục vụ cho công tác điều tra và quản lý lỗ hổng. Sự hiện diện của các nhật ký trong tất cả các môi trường cho phép theo dõi và phân tích kỹ lưỡng nếu có sự cố xảy ra.

* 1. **Triển khai các dấu vết kiểm tra** để liên kết mọi quyền truy cập vào các thành phần hệ thống với từng người dùng.
  2. **Cung cấp các dấu vết kiểm tra tự động** cho tất cả các thành phần hệ thống, ghi lại các sự kiện như truy cập dữ liệu chủ thẻ, hành động của người có quyền root hoặc quản trị, thay đổi quyền truy cập, cố gắng truy cập trái phép, và các thay đổi đối với tài khoản quản trị.
  3. **Ghi lại các mục nhật ký** cho tất cả các thành phần hệ thống, bao gồm thông tin về người dùng, loại sự kiện, thời gian, kết quả (thành công hoặc thất bại), nguồn gốc sự kiện và đối tượng liên quan.

**Yêu cầu 11: Kiểm tra định kỳ các hệ thống và quy trình bảo mật**

Lỗ hổng bảo mật liên tục được phát hiện bởi các cá nhân ác ý và các nhà nghiên cứu, và cũng có thể được tạo ra bởi phần mềm mới. Các thành phần hệ thống, quy trình và phần mềm tùy chỉnh cần được kiểm tra thường xuyên để đảm bảo rằng bảo mật được duy trì theo thời gian.

1. Kiểm tra sự hiện diện của các điểm truy cập không dây hàng quý và duy trì danh mục các điểm truy cập hợp pháp.
2. Quét lỗ hổng mạng nội bộ và ngoại vi ít nhất mỗi quý và sau khi thay đổi mạng, giải quyết các lỗ hổng cho đến khi quét thành công.
3. Kiểm tra xâm nhập nội bộ và bên ngoài ít nhất hàng năm và sau mỗi thay đổi quan trọng, xác nhận hiệu quả của phân đoạn nếu sử dụng.

**Duy trì Chính sách Bảo mật Thông tin**

Một chính sách bảo mật mạnh mẽ thiết lập tông màu cho bảo mật ảnh hưởng đến toàn bộ công ty và thông báo cho nhân viên về các nghĩa vụ của họ liên quan đến bảo mật. Tất cả nhân viên nên nhận thức được tính nhạy cảm của dữ liệu chủ thẻ và trách nhiệm của họ trong việc bảo vệ nó.

**Requirement 12: Duy trì chính sách bảo mật thông tin cho tất cả nhân viên:**

1. **Xây dựng và cập nhật chính sách bảo mật:** Cần có chính sách bảo mật rõ ràng, được công bố và duy trì, được xem xét hàng năm và cập nhật khi môi trường thay đổi.
2. **Quy trình đánh giá rủi ro:** Thực hiện đánh giá rủi ro hàng năm hoặc khi có thay đổi lớn, xác định tài sản quan trọng, mối đe dọa và lỗ hổng.
3. **Chính sách sử dụng công nghệ:** Phát triển chính sách sử dụng cho các công nghệ quan trọng như truy cập từ xa, mạng không dây, thiết bị di động, email và Internet.

**CHUẨN BỊ ĐÁNH GIÁ PCI DSS**

1. **Scope - Phạm vi** – Xác định các thành phần hệ thống và mạng nào thuộc phạm vi PCI DSS.
2. **Assess - Đánh giá** – Kiểm tra sự tuân thủ của các thành phần hệ thống trong phạm vi theo các quy trình kiểm tra cho từng yêu cầu PCI DSS.
3. **Report - Báo cáo** – Người đánh giá và/hoặc tổ chức hoàn thành tài liệu cần thiết (ví dụ: Bảng câu hỏi tự đánh giá (SAQ) hoặc Báo cáo về Tuân thủ (ROC)), bao gồm tài liệu hóa tất cả các biện pháp kiểm soát thay thế.
4. **Attest - Xác nhận** – Hoàn thành Tuyên bố Tuân thủ (AOC) thích hợp.
5. **Submit - Nộp** – Nộp SAQ, ROC, AOC và các tài liệu hỗ trợ khác như báo cáo quét ASV cho bên chấp nhận thanh toán (đối với thương nhân) hoặc cho thương hiệu thẻ yêu cầu (đối với nhà cung cấp dịch vụ).
6. **Remediate - Khắc phục** – Nếu cần, thực hiện các biện pháp khắc phục để giải quyết các yêu cầu chưa được thực hiện và cung cấp báo cáo cập nhật.

**Chương 7: ISO 27000**

A diagram of a company's process

Description automatically generatedISO27001 giúp xây dựng Hệ Thống Quản Lý Bảo Mật Thông Tin (Information Security Management System- ISMS)

**ISO 27001 & Risk Management**

**Plan:**

1. Xác định/đánh giá lại ranh giới an ninh
2. Thực hiện phân tích khoảng cách
3. Thực hiện đánh giá rủi ro
4. Xây dựng kế hoạch xử lý rủi ro
5. Cập nhật chính sách an ninh thông tin
6. Xin phê duyệt
7. Chuẩn bị Tuyên bố về khả năng áp dụng (Statement of Applicability)

**Do:**

1. Triển khai kế hoạch xử lý rủi ro và các biện pháp kiểm soát đã chọn
2. Triển khai các chương trình đào tạo và nâng cao nhận thức

**Check:**

1. Đo lường hiệu quả
2. Thực hiện các cuộc kiểm toán An ninh Thông tin

**Qui trình triển khai ISO27001**

1. Management Support (Sự hỗ trợ quản lý)

* Định hướng rõ ràng của công ty về việc hỗ trợ trong xây dựng giải pháp an toàn thông tin
* Sự cam kết và hỗ trợ của tổ chức trong quá trình triển khai giải pháp an toàn thông:
  + Cung cấp tài nguyên
  + Ban hành chính sách

1. Defining ISMS scope (Định nghĩa ISMS)

* Xác định phạm vi xây dựng hệ thống ISMS sao cho phù hợp nhất với doanh nghiệp (hoạt động kinh doanh, vị thế của doanh nghiệp, tài sản doanh nghiệp).
* Những gì không thực hiện được cần giải thích rõ ràng trong tài liệu Statement of Applicability (SOA)

1. Inventory of Assets (Thống kê tài sản)

* Thống kê tài sản quan trọng và thiết lập cơ chế sử dụng, theo dõi chi tiết:
  + Physical (phần cứng)
  + Software (phần mềm)
  + People (con người)
  + Services (dịch vụ)
  + Intangibles (vô hình)

1. Risk Assessment (Đánh giá rủi ro)

A diagram of a company

Description automatically generated

1. Prepare Statement of Applicability

* SOAlà tài liệu chính trong ISMS
* SOAlà kết quả của quá trình đánh giá rủi ro
* SOA liệt kê mục tiêu quan trọng cần làm trong quá trình bảo mật thông tin
* SOA liệt kê những qui trình thực hiện cần thực hiện những mục tiêu
* SOA liệt kê những giải pháp cần xử phạt khi vi phạm chính sách

Prepare Risk Treatment Plan

* Xác định thứ tự ưu tiên trong những rủi ro bảo mật.
* Phân tán trách nhiệm nhưng có sự quản lý một cách chặt chẽ.
* Chính sách ban hành toàn bộ công ty:
  + Người đứng đầu
  + ………………….
  + Người thấp nhất

1. The ISMS

* Mối quan hệ giữa cách thức quản lý, đánh giá rủi ro, xử lý rủi ro
* Tài liệu ISMS:
  + Chính sách và mục tiêu của ISMS
  + Phạm vi ISMS
  + Mô tả cách thức đánh giá rủi ro
  + Mô tả cách thức giảm thiểu, tránh rủi ro và kết quả
  + Sự ảnh hưởng của doanh nghiệp khi thực hiện ISMS

1. Compliance Review and Corrective Actions

* Xem lại qui trình áp dụng PDCA
* Cải tiến cho phù hợp với doanh nghiệp

1. Pre-Certification Assessment

* Đánh giá lợi ích

**ISO27002**

Có cái nhìn tổng quan về vấn đề ATTT

ISO 27002 là chuẩn quốc tế về hướng dẫn thực hiện quản lý an toàn thông tin và đề cập đến mọi thành phần trong doanh nghiệp có ảnh hưởng đến ATTT

1. **Organizing information security**

* Xác định các mục tiêu an ninh thông tin đáp ứng yêu cầu của tổ chức.
* Thiết lập phạm vi của ISMS Đảm bảo đủ nguồn lực được cung cấp để phát triển, thực hiện, vận hành và duy trì ISMS.
* Phương pháp đánh giá hiệu quả khi triển khai ISMS.
* Phân rõ vài trò và trách nhiệm của từng bộ phận, từng cá nhân trong qui trình đảm bảo an ninh thông tin.

1. **Asset management**

* Mục tiêu kiểm soát này là "để đạt được và duy trì mức độ bảo vệ thích hợp tài sản của tổ chức”
  + Thống kê tài sản
  + Chủ sở hữu tài sản
  + Mục tiêu sử dụng tài sản
  + Phân loại thông tin
    - Mức độ bảo mật cho từng trạng thái của dữ liệu

A diagram of data security lifecycles

Description automatically generated

1. **Human resources security**

* Trước khi tuyển dụng:
  + Đảm bảo rằng các nhân viên, nhà thầu và các bên thứ ba hiểu rõ trách nhiệm của mình và phù hợp với vai trò được giao, đồng thời giảm thiểu các rủi ro về việc đánh cắp, gian lận hoặc lạm dụng chức năng, quyền hạn
    - Điều khoản và điều kiện tuyển dụng
    - Vai trò và trách nhiệm
    - Sàng lọc
* Trong quá trình làm việc:
  + Đảm bảo rằng mọi nhân viên của tổ chức, nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan tới an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ, và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc, và giảm thiểu các rủi ro do con người gây ra
    - Trách nhiệm ban quản lý
    - Nhận thức, giáo dục và đào tạo về an toàn thông tin
    - Xử lý kỷ luật
* Sau quá trình làm việc:
  + Nhằm đảm bảo rằng các nhân viên của tổ chức, nhà thầu và các bên thứ ba nghỉ việc hoặc thay đổi vị trí một cách có tổ chức.
    - Trách nhiệm kết thúc hợp đồng
    - Bàn giao tài sản
    - Hủy bỏ quyền truy cập

1. **Physical and environmental security (và 5. Communication & Operations Management)**

* Theo dõi và giới hạn việc truy cập để phát hiện, tránh và giảm thiểu tối đa các truy cập trái phép làm ảnh hưởng đến hệ thống.
* Danh sách những người được truy cập vào những khu vực an toàn phải được xem xét và phê duyệt và phê duyệt bởi người quản trị, bộ phận bảo mật thiết bị và có sự kiểm tra chéo của những người quản lý giữa các bộ phận đó.
* Cấm chụp ảnh hoặc ghi hình
* Sử dụng thẻ từ và thời gian truy cập để kiểm soát việc truy cập.

1. **Access control**

* Nhằm đảm bảo người dùng hợp lệ được truy cập và ngăn chặn những người dùng không hợp lệ truy cập trái phép đến hệ thống thông tin.
  + Vật lý
  + Mạng
  + Hệ điều hành
  + Ứng dụng
* Quản lý truy cập mạng:
  + Phân vùng mạng
  + Bảo vệ cổng cấu hình
  + Định danh thiết bị trong các mạng
  + Chính sách sử dụng các dịch vụ mạng
  + Xác thực người dùng cho các kết nối bên ngoài
  + Quản lý kết nối mạng
  + Quản lý định tuyến mạng
  + Log
* Quản lý truy cập hệ điều hành và ứng dụng:
  + Các thủ tục đăng nhập an toàn
  + Định danh và xác thực người dùng
  + Hệ thống quản lý mật khẩu
  + Thời gian giới hạn của phiên làm việc
  + Giới hạn thời gian kết nối
  + Log

1. **Systems acquisition, development and maintenance (8. Incident Management)**

* Tính đúng đắn trong xử lý của các ứng dụng
  + Nhằm ngăn chặn các lỗi, mất mát, sửa đổi hoặc sử dụng trái phép thông tin trong các ứng dụng.
    - Kiểm tra tính hợp lệ của dữ liệu nhập vào
    - Kiểm soát việc xử lý nội bộ
    - Tính toàn vẹn thông điệp n Kiểm tra tính hợp lệ của dữ liệu đầu ra
* Quản lý CIA
  + Nhằm bảo vệ tính bí mật, xác thực hoặc toàn vẹn của thông tin bằng các biện pháp mã hóa.
    - Chính sách sử dụng các biện pháp quản lý mã hóa
    - Quản lý khóa
* Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển
  + Các thủ tục quản lý thay đổi
  + Kiểm soát kỹ thuật các ứng dụng sau thay đổi của hệ thống điều hành.
  + Hạn chế thay đổi các gói phần mềm
  + Sự rò rỉ thông tin
  + Phát triển phần mềm thuê khoán
* Quản lý các điểm yếu về kỹ thuật
  + Nhằm giảm thiểu các mối nguy hiểm xuất phát từ việc tin tặc khai thác các điểm yếu kỹ thuật đã được công bố

1. **Business continuity management**

* Chống lại các gián đoạn trong hoạt động nghiệp vụ và bảo vệ các quy trình hoạt động trọng yếu khỏi các ảnh hưởng do lỗi hệ thống thông tin hay các thảm hoạ và đảm bảo khả năng khôi phục các hoạt động bình thường đúng lúc.
  + Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức
  + Kiểm tra, bảo trì và đánh giá lại các kế hoạch đảm bảo sự liên tục trong hoạt động của tổ chức

1. **Compliance**

* Nhằm tránh sự vi phạm pháp luật, quy định, nghĩa vụ theo các hợp đồng đã ký kết, các yêu cầu về bảo đảm an toàn thông tin.
  + Xác định các điều luật hiện đang áp dụng được
  + Quyền sở hữu trí tuệ (IPR)
  + Bảo vệ các hồ sơ tổ chức
  + Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân
  + Ngăn ngừa việc lạm dụng phương tiện xử lý thông tin