**Tìm hiểu ISO 27001:2022**

MỤC LỤC

[**I.** **Tổng quan** 1](#_Toc196744218)

[**1.1.** **Hệ thống Quản lý An toàn Thông tin (Information Security Management System - ISMS)** 1](#_Toc196744219)

[**1.2.** **Mục tiêu của ISMS** 2](#_Toc196744220)

[**1.3.** **Các thành phần chính của ISMS** 2](#_Toc196744221)

[**1.4.** **Quy trình chứng nhận ISO 27001:2022** 2](#_Toc196744222)

[**1.4.1.** **Những ngành nào cần chứng nhận ISO/IEC 27001** 3](#_Toc196744223)

[**1.4.2.** **Lợi ích khi áp dụng ISO 27001** 4](#_Toc196744224)

[**1.4.3.** **Làm thế nào để đạt được chứng nhận ISO/IEC 27001** 5](#_Toc196744225)

[1.4.4. **Quy trình chứng nhận ISO 27001** 6](#_Toc196744226)

[**II.** **Cấu trúc của Tiêu chuẩn** 9](#_Toc196744227)

[**2.1.** **Phạm vi** 10](#_Toc196744228)

[**2.2.** **Tham chiếu tiêu chuẩn** 10](#_Toc196744229)

[**2.3.** **Thuật ngữ và định nghĩa** 11](#_Toc196744230)

[**2.4.** **Bối cảnh của tổ chức** 11](#_Toc196744231)

[**2.4.1.** **Hiểu tổ chức và bối cảnh của tổ chức** 11](#_Toc196744232)

[**2.4.2.** **Hiểu nhu cầu và mong đợi của các bên quan tâm** 11](#_Toc196744233)

[**2.4.3.** **Xác định phạm vi của ISMS** 12](#_Toc196744234)

[**2.4.4.** **Thiết lập hệ thống quản lý an toàn thông tin** 12](#_Toc196744235)

[**2.5.** **Sự lãnh đạo** 12](#_Toc196744236)

[**2.5.1.** **Sự lãnh đạo và sự cam kết** 12](#_Toc196744237)

[**2.5.2.** **Chính sách an toàn thông tin** 12](#_Toc196744238)

[**2.5.3.** **Vai trò, trách nhiệm và quyền hạn** 13](#_Toc196744239)

[**2.6.** **Hoạch định** 13](#_Toc196744240)

[**2.6.1.** **Hành động để giải quyết rủi ro và các cơ hội cải tiến** 13](#_Toc196744241)

[**2.6.2.** **Mục tiêu an toàn thông tin và hoạch định thực hiện** 14](#_Toc196744242)

[**2.6.3.** **Hoạch định các thay đổi** 14](#_Toc196744243)

[**2.7.** **Hỗ trợ** 14](#_Toc196744244)

[**2.7.1.** **Nguồn lực** 14](#_Toc196744245)

[**2.7.2.** **Năng lực** 14](#_Toc196744246)

[**2.7.3.** **Nhận thức** 15](#_Toc196744247)

[**2.7.4.** **Trao đổi thông tin** 15](#_Toc196744248)

[**2.7.5.** **Thông tin được lập văn bản** 15](#_Toc196744249)

[**2.8.** **Điều hành** 16](#_Toc196744250)

[**2.8.1.** **Hoạch định và kiểm soát hoạt động** 16](#_Toc196744251)

[**2.8.2.** **Đánh giá rủi ro an toàn thông tin** 16](#_Toc196744252)

[**2.8.3.** **Xử lý rủi ro an toàn thông tin** 16](#_Toc196744253)

[**2.9.** **Đánh giá hiệu quả** 16](#_Toc196744254)

[**2.9.1.** **Giám sát, đo lường, phân tích và đánh giá** 16](#_Toc196744255)

[**2.9.2.** **Đánh giá nội bộ** 17](#_Toc196744256)

[**2.9.3.** **Xem xét của lãnh đạo** 17](#_Toc196744257)

[**2.10.** **Cải tiến** 18](#_Toc196744258)

[**2.10.1.** **Cải tiến liên tục** 18](#_Toc196744259)

[**2.10.2.** **Sự không phù hợp và hành động khắc phục** 18](#_Toc196744260)

[**2.11.** **Phụ lục A (quy định)** 18](#_Toc196744261)

[**III.** **Hiểu cấu trúc tiêu chuẩn ISO/IEC 27001:2022** 24](#_Toc196744262)

[**IV.** **Mối đe dọa APT (Advanced Persistent Threat) và liên hệ với ISO/IEC 27001** 24](#_Toc196744263)

[**4.1.** **Tổng quan về APT** 25](#_Toc196744264)

[**4.2.** **Đặc điểm chính của APT** 25](#_Toc196744265)

[**4.3.** **Vòng đời của APT** 27](#_Toc196744266)

[**4.4.** **Quy trình tấn công** 28](#_Toc196744267)

[**4.5.** **Hậu quả của các cuộc tấn công** 30](#_Toc196744268)

[**4.6.** **Mối liên hệ giữa APT và tiêu chuẩn ISO/IEC 27001** 31](#_Toc196744269)

[**V.** **Các giải pháp phòng chống tấn công APT** 33](#_Toc196744270)

[**5.1.** **Triển khai Honeypot để bẫy và giám sát hành vi APT** 34](#_Toc196744271)

[**5.2.** **Tăng cường bảo vệ điểm cuối bằng EDR (Endpoint Detection and Response)** 34](#_Toc196744272)

[**5.3.** **Kết hợp IDS/IPS OPNsense với Threat Hunting** 35](#_Toc196744273)

[**5.4.** **Đào tạo nhận thức và xây dựng quy trình ứng phó sự cố** 36](#_Toc196744274)

[TÀI LIỆU THAM KHẢO 37](#_Toc196744275)

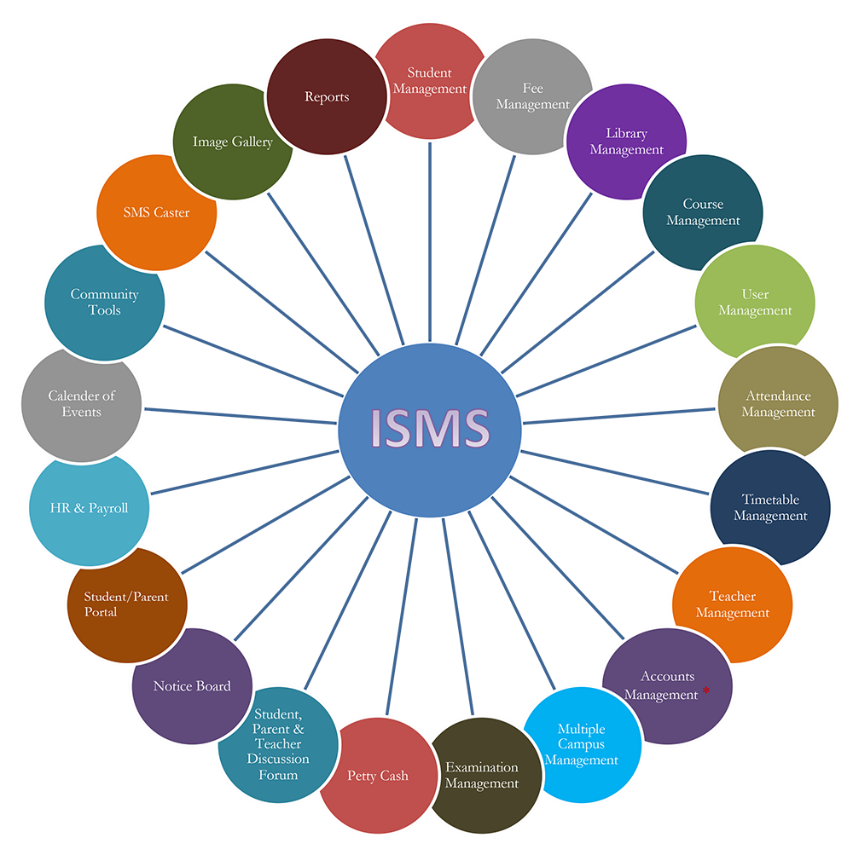
[PHỤ LỤC 38](#_Toc196744276)

1. **Tổng quan**

## **Hệ thống Quản lý An toàn Thông tin (Information Security Management System - ISMS)**

Hệ thống Quản lý An toàn Thông tin (ISMS - Information Security Management System) là một khuôn khổ bao gồm **chính sách, quy trình, thủ tục và các biện pháp kỹ thuật** được thiết kế để bảo vệ thông tin của tổ chức khỏi các mối đe dọa về bảo mật, toàn vẹn và sẵn sàng. Việc thiết lập và triển khai thực hiện hệ thống quản lý an toàn thông tin của một tổ chức chịu ảnh hưởng bới các nhu cầu và các mục tiêu của tổ chức, các yêu cầu an toàn, các quá trình được sử dụng và bởi quy mô, cấu trúc của tổ chức. Tất cả các yếu tố ảnh hưởng đó có thể xảy ra sự thay đổi theo thời gian.

ISO/IEC 27000 mô tả tổng quan và từ vựng của hệ thống quản lý an toàn thông tin, viện dẫn các tiêu chuẩn của bộ tiêu chuẩn về Hệ thống quản lý an toàn thông tin (bao gồm ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005), với các thuật ngữ và định nghĩa liên quan.



Hiểu đơn giản, ISMS là tổng thể các biện pháp và quy trình tổ chức áp dụng để đảm bảo an toàn thông tin ở mọi cấp độ.

Nó giống như một "bộ khung quản trị" mà doanh nghiệp xây dựng để đánh giá, kiểm soát và giảm thiểu rủi ro liên quan đến thông tin.

* 1. **Mục tiêu của ISMS**

Bảo mật (Confidentiality): Đảm bảo chỉ người được phép mới có thể truy cập thông tin.

Toàn vẹn (Integrity): Đảm bảo thông tin không bị thay đổi, chỉnh sửa trái phép.

Sẵn sàng (Availability): Đảm bảo thông tin luôn có thể truy cập khi cần thiết.

* 1. **Các thành phần chính của ISMS**

Chính sách an toàn thông tin → Định hướng và cam kết của lãnh đạo tổ chức.

Đánh giá rủi ro → Xác định những tài sản thông tin quan trọng, mối đe dọa và lỗ hổng.

Kiểm soát an toàn thông tin → Biện pháp tổ chức và kỹ thuật như phân quyền truy cập, mã hóa, giám sát, kiểm tra, v.v.

Đào tạo và nâng cao nhận thức → Giúp nhân viên hiểu và tuân thủ các quy định an ninh.

Giám sát và đánh giá → Theo dõi hiệu quả hệ thống và xử lý sự cố (incident management).

Cải tiến liên tục (PDCA) → Theo chu trình Plan – Do – Check – Act để cải thiện ISMS liên tục.

* 1. **Quy trình chứng nhận ISO 27001:2022**

ISO/IEC 27001 là tiêu chuẩn quốc tế về Hệ thống Quản lý An toàn Thông tin (Information Security Management System - ISMS). Đây là một tiêu chuẩn do Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Ủy ban Kỹ thuật Điện Quốc tế (IEC) cùng phát triển, nhằm giúp các tổ chức bảo vệ thông tin một cách có hệ thống và hiệu quả.

Là khung tiêu chuẩn giúp tổ chức đánh giá rủi ro bảo mật thông tin, thiết lập các biện pháp kiểm soát bảo mật và duy trì và cải tiến an ninh thông tin liên tục. Nhằm áp dụng cho mọi tổ chức, không phân biệt quy mô hay lĩnh vực hoạt động.

 ***Mẫu giấy chứng nhận ISO/IEC 27001 ISOCERT cấp, có mã QR tra cứu tiện lợi online mọi nơi***

* + 1. **Những ngành nào cần chứng nhận ISO/IEC 27001**

Chứng nhận ISO/IEC 27001 có thể áp dụng cho mọi loại hình tổ chức, không phân biệt quy mô hay lĩnh vực hoạt động. Tuy nhiên, tiêu chuẩn này đặc biệt cần thiết đối với các tổ chức mà việc bảo mật thông tin đóng vai trò then chốt, chẳng hạn như:

Trong lĩnh vực tài chính – ngân hàng, các tổ chức như ngân hàng, công ty tài chính, ví điện tử và nền tảng fintech thường xử lý khối lượng lớn dữ liệu nhạy cảm, bao gồm thông tin giao dịch và tài khoản người dùng. Việc áp dụng ISO/IEC 27001 giúp họ đảm bảo an toàn thông tin, đồng thời tăng cường uy tín với khách hàng và đối tác.

Đối với ngành y tế, từ bệnh viện, phòng khám đến công ty bảo hiểm sức khỏe, việc bảo vệ thông tin bệnh án và dữ liệu bệnh nhân là vô cùng quan trọng. ISO/IEC 27001 không chỉ hỗ trợ tuân thủ quy định pháp luật mà còn hạn chế rủi ro rò rỉ dữ liệu trong bối cảnh số hóa hồ sơ bệnh án ngày càng phổ biến.

Trong lĩnh vực công nghệ thông tin và viễn thông, các doanh nghiệp phát triển phần mềm, trung tâm dữ liệu (data center) hoặc nhà cung cấp dịch vụ CNTT đều có trách nhiệm quản lý và bảo mật dữ liệu của khách hàng. Chứng nhận ISO/IEC 27001 giúp họ xây dựng hệ thống kiểm soát truy cập, mã hóa dữ liệu và quản lý sự cố an ninh một cách bài bản.

Các cơ quan chính phủ, tổ chức khu vực công và đơn vị quốc phòng cũng cần áp dụng tiêu chuẩn này để bảo vệ thông tin công dân, dữ liệu mật và các tài liệu chiến lược quốc gia. Việc tuân thủ ISO/IEC 27001 giúp tăng tính minh bạch trong quản lý nhà nước và phòng chống rủi ro an ninh mạng.

Bên cạnh đó, các tổ chức trong lĩnh vực giáo dục và nghiên cứu, nơi lưu trữ dữ liệu cá nhân sinh viên, kết quả học tập và thông tin nghiên cứu có giá trị cao, cũng cần triển khai hệ thống quản lý an toàn thông tin theo ISO/IEC 27001 để tránh thất thoát dữ liệu và rò rỉ kết quả nghiên cứu.

Trong bối cảnh kinh doanh trực tuyến ngày càng phát triển, các nền tảng thương mại điện tử cũng là mục tiêu tấn công của tội phạm mạng. Việc đạt được chứng nhận ISO/IEC 27001 giúp họ khẳng định năng lực bảo mật, bảo vệ thông tin thanh toán và gia tăng sự tin tưởng từ phía người tiêu dùng.

Cuối cùng, các doanh nghiệp cung cấp dịch vụ gia công phần mềm, xử lý dữ liệu hoặc chăm sóc khách hàng thuê ngoài thường thay mặt đối tác quản lý thông tin. Do đó, họ cần chứng minh năng lực tuân thủ bảo mật thông tin để duy trì uy tín và đảm bảo yêu cầu hợp đồng với các đối tác lớn.

* + 1. **Lợi ích khi áp dụng ISO 27001**

Việc triển khai và đạt chứng nhận ISO/IEC 27001 mang lại nhiều lợi ích thiết thực cho doanh nghiệp, được phân chia theo các khía cạnh sau:

**1. Khía cạnh thương mại và cạnh tranh**

Tăng lợi thế cạnh tranh: Chứng nhận giúp doanh nghiệp thể hiện năng lực bảo mật thông tin, nâng cao uy tín thương hiệu và mở rộng cơ hội kinh doanh với khách hàng trong và ngoài nước.

Củng cố niềm tin đối tác và khách hàng: Đảm bảo thông tin cá nhân và dữ liệu quan trọng được bảo mật nghiêm ngặt, tạo sự tin tưởng khi hợp tác.

Công cụ marketing hiệu quả: ISO 27001 là bằng chứng rõ ràng về hệ thống bảo mật vững chắc, giúp quảng bá dịch vụ/sản phẩm chuyên nghiệp hơn.

**2. Khía cạnh vận hành và quản trị nội bộ**

Cải thiện hiệu quả quản lý thông tin: Chuẩn hóa quy trình, giảm thiểu nhầm lẫn trong phân quyền và quản lý tài sản thông tin.

Giảm thiểu rủi ro và gián đoạn hoạt động: Hệ thống ISMS giúp phát hiện và xử lý sớm các sai sót/lỗ hổng bảo mật.

Tăng khả năng phản ứng và cải tiến liên tục: Thông qua quy trình đánh giá định kỳ, tổ chức có thể điều chỉnh hệ thống để phù hợp với các mối đe dọa mới.

**3. Khía cạnh pháp lý và tuân thủ**

Đáp ứng yêu cầu pháp luật và hợp đồng: ISO 27001 giúp tổ chức tuân thủ các yêu cầu từ luật quốc gia, tiêu chuẩn ngành và hợp đồng với đối tác.

Giảm thiểu rủi ro pháp lý: Giúp tránh bị phạt hoặc tổn thất tài chính do vi phạm dữ liệu hoặc thiếu tuân thủ.

**4. Khía cạnh tài chính**

Giảm chi phí quản lý và xử lý sự cố: Nhờ khả năng phòng ngừa rủi ro, tổ chức tiết kiệm chi phí liên quan đến khắc phục vi phạm và gián đoạn hệ thống.

Giảm tần suất đánh giá bên ngoài: Có chứng nhận sẽ giảm số lượng kiểm tra từ đối tác/khách hàng bên thứ ba.

**5. Khía cạnh nhân sự**

Nâng cao nhận thức và trách nhiệm nhân viên: Nhân sự được đào tạo bài bản về bảo mật, hiểu rõ vai trò và nhiệm vụ trong việc bảo vệ thông tin.

Cải thiện hiệu suất làm việc: Tránh trùng lặp công việc, rõ ràng trong phân quyền và trách nhiệm, nâng cao hiệu quả hoạt động.

* + 1. **Làm thế nào để đạt được chứng nhận ISO/IEC 27001**

Việc đạt được chứng nhận ISO/IEC 27001 là một quá trình toàn diện và đòi hỏi sự tham gia tích cực của các bên liên quan trong và ngoài tổ chức. Đây không phải là một thủ tục đơn giản như việc điền vào một bảng kiểm tra và chờ phê duyệt, mà là một hành trình cải tiến liên tục nhằm xây dựng một hệ thống quản lý an toàn thông tin hiệu quả, đầy đủ và phù hợp với tổ chức.

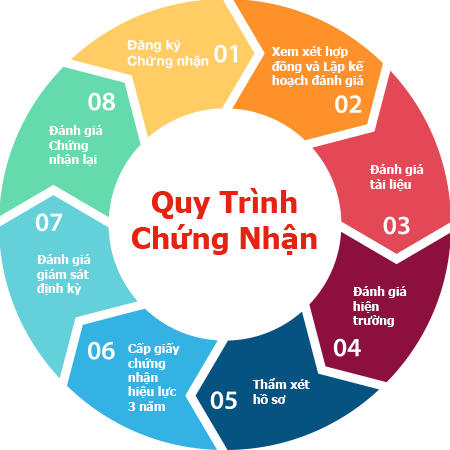
Trước khi đăng ký chứng nhận, tổ chức cần đảm bảo rằng Hệ thống Quản lý An toàn Thông tin (ISMS) đã được thiết kế và triển khai một cách toàn diện, bao quát tất cả các khía cạnh có thể phát sinh rủi ro liên quan đến công nghệ thông tin và tài sản thông tin.

**Các bước cần thiết để đạt chứng nhận ISO/IEC 27001 bao gồm:**

* Xác định phạm vi của ISMS: Làm rõ phạm vi áp dụng của hệ thống quản lý an toàn thông tin, xác định các đơn vị, quy trình hoặc hệ thống liên quan.
* Đảm bảo cam kết từ lãnh đạo và ngân sách: Sự ủng hộ và chỉ đạo từ cấp quản lý cao nhất là điều kiện tiên quyết cho sự thành công của dự án triển khai ISMS.
* Xác định các bên liên quan và các yêu cầu pháp lý, quy định và hợp đồng: Nhận diện các yêu cầu bắt buộc tổ chức phải tuân thủ liên quan đến bảo mật thông tin.
* Thực hiện đánh giá rủi ro: Phân tích các mối đe dọa, lỗ hổng, khả năng và hậu quả để xây dựng kế hoạch xử lý rủi ro thích hợp.
* Xem xét và triển khai các điều khiển bảo mật bắt buộc: Áp dụng các biện pháp kiểm soát được quy định trong Phụ lục A của tiêu chuẩn ISO/IEC 27001 nhằm giảm thiểu rủi ro ở mức chấp nhận được.
* Xây dựng năng lực quản lý nội bộ: Thành lập nhóm dự án, phân công trách nhiệm và phát triển năng lực nội bộ để duy trì và vận hành hệ thống ISMS.
* Phát triển hệ thống tài liệu phù hợp: Soạn thảo các chính sách, quy trình, hướng dẫn và tài liệu quản lý khác nhằm hỗ trợ vận hành và duy trì ISMS.
* Đào tạo và nâng cao nhận thức cho nhân viên: Triển khai các chương trình đào tạo, tuyên truyền về vai trò của bảo mật thông tin đối với tất cả nhân sự trong tổ chức.
* Thực hiện các báo cáo cần thiết: Bao gồm Tuyên bố về khả năng áp dụng (SoA) và Kế hoạch xử lý rủi ro (Risk Treatment Plan), là hai tài liệu bắt buộc trong quá trình chứng nhận.
* Thực hiện đo lường, giám sát, xem xét và đánh giá ISMS: Định kỳ kiểm tra hiệu lực của hệ thống thông qua đánh giá nội bộ và xem xét của lãnh đạo.
* Thực hiện các hành động khắc phục và phòng ngừa: Xử lý các điểm không phù hợp, nguyên nhân gốc rễ và liên tục cải tiến hệ thống.
  + 1. **Quy trình chứng nhận ISO 27001**

ISO/IEC 27001 là tiêu chuẩn quốc tế về Hệ thống Quản lý An toàn Thông tin (*Information Security Management System – ISMS*). Đây là tiêu chuẩn do Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Ủy ban Kỹ thuật Điện Quốc tế (IEC) phối hợp ban hành, nhằm giúp các tổ chức thiết lập, thực hiện, duy trì và không ngừng cải tiến hệ thống quản lý nhằm bảo vệ tài sản thông tin khỏi các mối đe dọa ngày càng tinh vi.

Tiêu chuẩn này có thể áp dụng cho mọi tổ chức, bất kể quy mô, lĩnh vực hay loại hình kinh doanh, từ các doanh nghiệp vừa và nhỏ, tập đoàn đa quốc gia đến các tổ chức chính phủ.



Các bước trong quy trình chứng nhận ISO/IEC 27001:2022

**Bước 1: Khảo sát và đánh giá hiện trạng**

* Đánh giá hệ thống quản lý hiện tại của tổ chức.
* So sánh với các yêu cầu của ISO/IEC 27001 để xác định khoảng cách (gap analysis).
* Xác định phạm vi áp dụng ISMS.

**Bước 2: Phân tích và đánh giá rủi ro**

* Xác định tài sản thông tin cần bảo vệ.
* Phân tích mối đe dọa, điểm yếu và rủi ro liên quan.
* Đánh giá mức độ rủi ro và mức chấp nhận rủi ro.
* Lập kế hoạch xử lý rủi ro phù hợp.

**Bước 3: Xây dựng và triển khai ISMS**

* Xây dựng các chính sách, thủ tục, quy trình và biện pháp kiểm soát an toàn thông tin.
* Đào tạo nhân sự, nâng cao nhận thức về an toàn thông tin trong toàn tổ chức.
* Triển khai các biện pháp kỹ thuật và tổ chức nhằm kiểm soát rủi ro.

**Bước 4: Đánh giá nội bộ và rà soát tài liệu**

* Tổ chức đánh giá nội bộ theo định kỳ để đảm bảo ISMS được thực hiện đúng quy định.
* Xác định các điểm không phù hợp và thực hiện hành động khắc phục.
* Cập nhật và hoàn thiện tài liệu hệ thống quản lý.

**Bước 5: Xem xét của lãnh đạo**

* Ban lãnh đạo tiến hành họp định kỳ để xem xét hiệu lực của hệ thống ISMS.
* Đưa ra các quyết định cải tiến hoặc thay đổi nếu cần thiết.

**Bước 6: Đăng ký chứng nhận với tổ chức đánh giá**

* Lựa chọn một tổ chức chứng nhận độc lập (bên thứ ba được công nhận).
* Tổ chức chứng nhận sẽ thực hiện:

**Đánh giá giai đoạn 1 (Stage 1)**: Xem xét tài liệu, phạm vi áp dụng và mức độ sẵn sàng.

**Đánh giá giai đoạn 2 (Stage 2)**: Đánh giá đầy đủ việc thực hiện ISMS tại hiện trường.

**Bước 7: Cấp chứng nhận và giám sát định kỳ**

* Nếu đạt yêu cầu, tổ chức được cấp chứng nhận ISO/IEC 27001 có hiệu lực 3 năm.
* Trong thời gian này, tổ chức chứng nhận sẽ thực hiện các đợt đánh giá giám sát định kỳ (thường hàng năm) để đảm bảo hệ thống được duy trì hiệu quả.

**Bước 8: Tái chứng nhận**

* Sau 3 năm, tổ chức cần thực hiện đánh giá tái chứng nhận để duy trì hiệu lực của chứng chỉ ISO/IEC 27001.

**Lưu ý trong quá trình thực hiện**

* Cần có sự **cam kết mạnh mẽ từ lãnh đạo cấp cao**.
* Đội ngũ nhân sự cần được **đào tạo và nâng cao nhận thức bảo mật thông tin**.
* Việc triển khai ISMS không chỉ là hoạt động kỹ thuật mà còn liên quan đến **quản trị tổ chức và văn hóa doanh nghiệp**.
* Nên sử dụng **các công cụ hỗ trợ đánh giá rủi ro và kiểm soát bảo mật** để tối ưu hiệu quả.

 **Mẫu giấy chứng nhận ISO 27001:2022 - Tiếng Việt**

 **Mẫu giấy chứng nhận ISO 27001:2022 - Tiếng Anh**

1. **Cấu trúc của Tiêu chuẩn**

ISO/IEC 27001 được chia thành 11 phần gồm 10 Điều khoản và 01 Phụ lục A. Bắt đầu từ Điều 1 đến Điều 3 là phần giới thiệu, từ Điều 4 đến Điều 10 là các yêu cầu bắt buộc của ISO phải được thực hiện trong một tổ chức đạt được chứng nhận tiêu chuẩn ISO 27001. Ngoài ra, Phụ lục A của bộ tài liệu bao gồm các biện pháp kiểm soát về khả năng áp dụng của tổ chức, doanh nghiệp.



Cụ thể cấu trúc của Tiêu chuẩn ISO 27001:2022 bao gồm:

Mục giới thiệu:

Mục giới thiệu nêu lên mục đích của ISO 27001, lợi ích của ISO 27001 và giới thiệu về khả năng tương thích của ISO 27001 với các tiêu chuẩn quản lý khác.

Mục giới thiệu bao gồm:

* Điều khoản 1: Phạm vi ( đối tượng và phạm vi áp dụng của tiêu chuẩn)
* Điều khoản 2: Tham chiếu tiêu chuẩn (các thuật ngữ và định nghĩa mới được đưa ra)
* Điều khoản 3: Điều khoản và định nghĩa (giải thích về từ ngữ, định nghĩa và các nội dung liên quan tới thuật ngữ)

Các điều khoản bắt buộc (đều là các phần của giai đoạn Kế hoạch trong chu trình PDCA):

Điều khoản 4: Bối cảnh của tổ chức

Doanh nghiệp cần xác định các yêu cầu để hiểu các vấn đề bên ngoài và bên trong, các bên quan tâm và các yêu cầu của họ.  Sau đó từ việc phân tích này, Doanh nghiệp xác định phạm vi của Hệ thống An toàn Thông tin.

Điều khoản 5: Lãnh đạo

Doanh nghiệp cần xác định trách nhiệm quản lý của lãnh đạo, đặt vai trò và cũng như nội dung của chính sách bảo mật thông tin từ lãnh đạo cao nhất.

Điều khoản 6: Lập kế hoạch

Doanh nghiệp cần xác định các yêu cầu đánh giá rủi ro, xử lý rủi ro, tuyên bố về khả năng áp dụng, kế hoạch xử lý rủi ro và đặt ra các mục tiêu bảo mật thông tin.

Điều khoản 7: Hỗ trợ

Điều khoản quy định Doanh nghiệp cần phải xác định các yêu cầu về tính sẵn có của nguồn lực, năng lực nhận sự, nhận thức, trao đổi thông tin và kiểm soát tài liệu và hồ sơ.

Điều khoản 8: Hoạt động

Doanh nghiệp xác định việc thực hiện đánh giá và xử lý rủi ro, đồng thời kiểm soát và thực hiện các quy trình cần thiết để đạt được các mục tiêu bảo mật thông tin.

Điều khoản 9: Đánh giá hiệu suất

Doanh nghiệp cần xác định các yêu cầu để theo dõi, đo lường, phân tích, đánh giá, kiểm toán nội bộ và xem xét quản lý.

Mục 10: Cải tiến

Doanh nghiệp cần xay dựng các yêu cầu cho kiểm soát sự không phù hợp, thực hiện khắc phục, hành động phòng ngừa và cải tiến liên tục.

Phụ lục A:

Phụ lục này cung cấp một danh mục gồm 114 biện pháp bảo vệ được đặt trong 14 phần (phần A.5 đến A.18).

* 1. **Phạm vi**

Tài liệu này chỉ định rõ các yêu cầu đối với hoạt động thiết lập, áp dụng, duy trì và cải tiến liên tục một Hệ thống quản lý An toàn thông tin trong bối cảnh của tổ chức. Tài liệu này cũng bao gồm các yêu cầu cho hoạt động đánh giá và xử lý các rủi ro an toàn thông tin đáp ứng nhu cầu của tổ chức.

Các yêu cầu trình bày trong tài liệu này mang tính tổng quát và nhằm áp dụng cho tất cả các tổ chức, bất kể loại hình, qui mô, tính chất. Việc loại trừ bất kỳ yêu cầu nào trong điều 4 đến 10 đều không được chấp nhận khi tổ chức tuyên bố phù hợp với tài liệu này.

* 1. **Tham chiếu tiêu chuẩn**

Các tài liệu dưới đây, được đề cập đến trong văn bản theo cách mà một số hoặc tất cả nội dung của chúng tạo thành các yêu cầu của văn bản này. Với các trích dẫn ghi ngày tháng, chỉ có các trích dẫn được nêu mới áp dụng. Các trích dẫn không ghi ngày tháng, bản mới nhất của tài liệu trích dẫn (bao gồm cả bổ sung) được áp dụng.

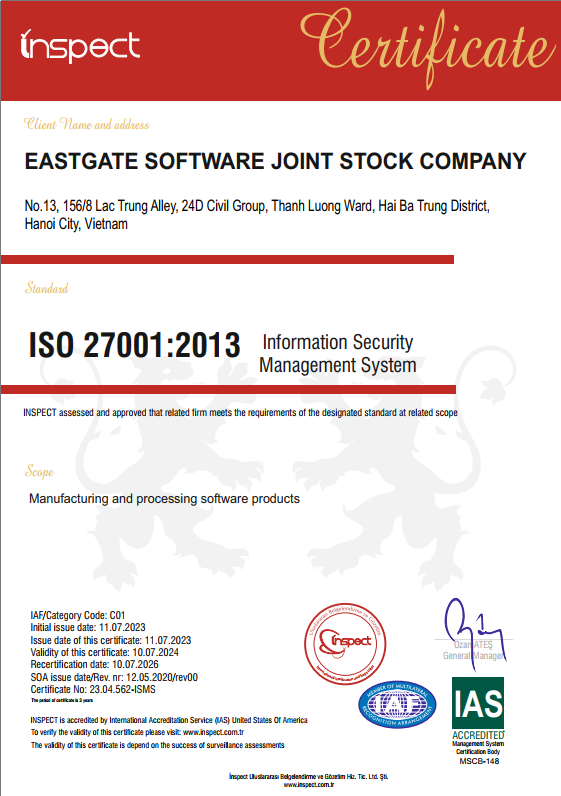
ISO/IEC 27000, Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Tổng quan và Từ vựng

* 1. **Thuật ngữ và định nghĩa**

Tài liệu này sử dụng các thuật ngữ và định nghĩa của ISO/IEC 27000

ISO và IEC duy trì cơ sở dữ liệu thuật ngữ để sử dụng trong hoạt động tiêu chuẩn hóa tại các địa chỉ sau:

* Nền tảng ISO Online: có tại https://www.iso.org/obp
* IEC Electropedia: có tại <https://www.electropedia.org/>



Mẫu giấy chứng nhận ISO 27001 quốc tế

* 1. **Bối cảnh của tổ chức**
     1. **Hiểu tổ chức và bối cảnh của tổ chức**

Tổ chức phải nhận diện những vấn đề đang tồn tại bên trong và bên ngoài mà có thể ảnh hưởng tới việc bảo vệ thông tin.

Việc xác định này giúp tổ chức "biết mình biết ta", từ đó xây ISMS sát với thực tế thay vì làm theo lý thuyết suông.

Một số vấn đề thường gặp như:

* Vấn đề nội bộ: Thiếu nhân sự IT, có hệ thống cũ kỹ, chưa có quy trình xử lý sự cố.
* Vấn đề bên ngoài: Bị cạnh tranh khốc liệt, chịu áp lực tuân thủ luật pháp (như Nghị định 53/2022 tại VN), hoặc nguy cơ từ hacker APT.
  + 1. **Hiểu nhu cầu và mong đợi của các bên quan tâm**

Tổ chức phải xác định ai là người bị ảnh hưởng hoặc có ảnh hưởng đến hệ thống an toàn thông tin - gọi là bên quan tâm (interested parties).

Một số “bên quan tâm” và nhu cầu/mong đợi (yêu cầu) điển hình:

* Khách hàng: Dữ liệu cá nhân không bị rò rỉ
* Nhân viên: Hệ thống làm việc ổn định
* Cơ quan nhà nước: Tuân thủ pháp luật, bảo vệ dữ liệu
* Đối tác: An toàn khi kết nối với hệ thống

Từ đó tổ chức cần xác định yêu cầu nào sẽ được đưa vào ISMS.

* + 1. **Xác định phạm vi của ISMS**

Tổ chức phải xác định rõ ISMS sẽ được áp dụng ở đâu, cho bộ phận nào, hoạt động nào, tại cơ sở nào…

Ví dụ: "ISMS được áp dụng tại phòng CNTT, bao gồm các hệ thống email, máy chủ nội bộ và cổng kết nối VPN, nhưng không áp dụng cho phòng kế toán vì dùng hệ thống độc lập."

Phạm vi này phải được ghi thành văn bản rõ ràng và sẽ dùng để xác định vùng cần bảo vệ, vùng cần đánh giá rủi ro.

* + 1. **Thiết lập hệ thống quản lý an toàn thông tin**

Sau khi xác định các mục ở trên, giờ tổ chức phải bắt tay vào xây dựng ISMS thực tế bao gồm:

* Các quy trình
* Các biện pháp bảo vệ
* Cách các phần này liên kết với nhau
* Và cam kết cải tiến liên tục theo chu trình PDCA (Plan – Do – Check – Act)
  1. **Sự lãnh đạo**

Mục tiêu: Lãnh đạo cấp cao phải dẫn dắt, cam kết, và gắn trách nhiệm rõ ràng cho việc triển khai ISMS.

* + 1. **Sự lãnh đạo và sự cam kết**

1. Lãnh đạo cao nhất phải thể hiện rằng họ không chỉ "gật đầu" mà thực sự tham gia, bằng cách:
2. Đặt ra chính sách và mục tiêu an toàn thông tin gắn với chiến lược công ty
3. Tích hợp ISMS vào các hoạt động, quy trình trong doanh nghiệp (không làm rời rạc)
4. Cung cấp đủ nguồn lực (nhân lực, tiền, công cụ,...)
5. Nói cho toàn tổ chức hiểu rõ tầm quan trọng của ISMS
6. Đảm bảo hệ thống đạt kết quả mong muốn (ví dụ: không bị rò rỉ dữ liệu)
7. Hỗ trợ nhân sự triển khai ISMS
8. Khuyến khích cải tiến liên tục
9. Trao quyền và hỗ trợ cho các quản lý cấp dưới về ISMS

Ví dụ thực tế: CEO tổ chức không chỉ ký văn bản, mà còn tham gia duyệt chính sách ATTT, cấp ngân sách mua firewall, duyệt kế hoạch đào tạo nhân sự IT2` và yêu cầu bộ phận báo cáo tiến độ triển khai ISMS.

* + 1. **Chính sách an toàn thông tin**

Lãnh đạo cấp cao phải ban hành chính sách ATTT rõ ràng và chính sách đó cần:

1. Phù hợp với hoạt động của công ty
2. Là nền tảng để đặt ra mục tiêu ATTT cụ thể
3. Cam kết tuân thủ pháp luật, quy định liên quan
4. Cam kết liên tục cải tiến ISMS

Và chính sách an toàn thông tin phải:

1. Phải có văn bản rõ ràng
2. Phải được phổ biến cho toàn tổ chức
3. Phải cung cấp cho các bên liên quan khi cần thiết
   * 1. **Vai trò, trách nhiệm và quyền hạn**

Lãnh đạo cấp cao cần:

* Phân rõ trách nhiệm cho từng vai trò trong tổ chức về ATTT
* Đảm bảo có người chịu trách nhiệm chính cho việc duy trì, cải tiến và báo cáo tình trạng ISMS
  1. **Hoạch định**
     1. **Hành động để giải quyết rủi ro và các cơ hội cải tiến**

1. **Khái quát**

Tổ chức cần:

Xác định rủi ro và cơ hội để:

* + Đảm bảo đạt được kết quả mong muốn của hệ thống ISMS.
  + Giảm thiểu tác động không mong muốn.
  + Cải tiến liên tục hệ thống.

Lập kế hoạch hành động để:

* + Giải quyết rủi ro/cơ hội.
  + Triển khai vào quá trình của hệ thống ISMS.
  + Đánh giá hiệu quả các hành động này.

1. **Đánh giá rủi ro an toàn thông tin**

Tổ chức cần có quy trình đánh giá rủi ro bao gồm:

Tiêu chí đánh giá rủi ro:

* + Tiêu chí chấp nhận rủi ro.
  + Tiêu chí để thực hiện đánh giá.

Đảm bảo tính nhất quán, hợp lệ và có thể so sánh của đánh giá.

Xác định rủi ro:

* + Theo các thuộc tính: bảo mật, toàn vẹn, sẵn sàng.
  + Xác định chủ sở hữu rủi ro.

Phân tích rủi ro:

* + Đánh giá hậu quả và khả năng xảy ra.
  + Xác định mức độ rủi ro.

Ước lượng rủi ro:

* + So sánh với tiêu chí.
  + Ưu tiên xử lý.

Lưu giữ hồ sơ đánh giá rủi ro.

1. **Xử lý rủi ro an toàn thông tin**

Tổ chức cần có quy trình xử lý:

* Lựa chọn phương án xử lý phù hợp kết quả đánh giá.
* Xác định các biện pháp kiểm soát cần thiết.
* So sánh với Phụ lục A để đảm bảo không bỏ sót kiểm soát quan trọng.
* Tạo Tuyên bố áp dụng (SoA): Danh sách các kiểm soát được áp dụng và lý do loại trừ.
* Lập kế hoạch xử lý rủi ro và
* Xin phê duyệt của chủ sở hữu rủi ro với các rủi ro còn lại.
  + 1. **Mục tiêu an toàn thông tin và hoạch định thực hiện**

Tổ chức cần:

Thiết lập mục tiêu an toàn thông tin tại các cấp/bộ phận phù hợp.

Mục tiêu phải:

* + Phù hợp với chính sách.
  + Có thể đo lường (nếu có thể).
  + Dựa trên yêu cầu, kết quả đánh giá và xử lý rủi ro.
  + Được theo dõi, truyền đạt, cập nhật và lập văn bản.

Kế hoạch để đạt được mục tiêu phải xác định rõ:

* + Việc cần làm.
  + Nguồn lực.
  + Người phụ trách.
  + Thời hạn hoàn thành.
  + Cách đo lường kết quả.
    1. **Hoạch định các thay đổi**

Khi tổ chức xác định sự cần thiết phải thay đổi đối với hệ thống quản lý an toàn thông tin, thì các thay đổi này phải được thực hiện một cách có kế hoạch.

* 1. **Hỗ trợ**
     1. **Nguồn lực**

Tổ chức phải xác định và cung cấp các nguồn lực cần thiết cho việc thiết lập, áp dụng, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin.

* + 1. **Năng lực**

Tổ chức phải:

* Xác định năng lực cần thiết của (những) người đang làm công việc mà dưới sự quản lý của họ có ảnh hưởng đến hoạt động an toàn thông tin;
* Đảm bảo rằng những người đó có đủ năng lực dựa trên cơ sở được giáo dục, đào tạo hoặc kinh nghiệm;
* Khi thích hợp, tiến hành thực hiện các hành động bổ sung nếu cần (ví dụ: đào tạo, thuê ngoài...) và đánh giá hiệu lực của các hành động đã thực hiện;
* Lưu giữ thông tin được lập văn bản thích hợp như bằng chứng về năng lực.

CHÚ THÍCH: Áp dụng các hành động có thể bao gồm, ví dụ: cung cấp các khóa đào tạo, các cố vấn, hoặc phân công lại vai trò của người lao động hiện hành; hoặc tuyển dụng hoặc ký hợp đồng với người đủ năng lực.

* + 1. **Nhận thức**

Người làm công việc dưới sự quản lý của tổ chức phải có nhận thức về:

* Chính sách an toàn thông tin;
* Việc đóng góp của họ vào hiệu lực của hệ thống quản lý an toàn thông tin, bao gồm cả các lợi ích của sự cải tiến hoạt động thực hiện an toàn thông tin;
* Những hệ quả của việc không thực hiện phù hợp với các yêu cầu của hệ thống quản lý an toàn thông tin.
  + 1. **Trao đổi thông tin**

Tổ chức phải xác định nhu cầu trao đổi thông tin nội bộ và bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin bao gồm:

* Trao đổi cái gì?
* Khi nào?
* Với ai?
* Bằng cách nào?
  + 1. **Thông tin được lập văn bản**

**Khái quát:**

Tổ chức phải duy trì các tài liệu:

* Được yêu cầu theo tiêu chuẩn;
* Tài liệu nội bộ cần thiết để vận hành hiệu quả ISMS.

CHÚ THÍCH: Mức độ thông tin được lập văn bản cho một hệ thống quản lý an toàn thông tin có thể khác nhau giữa các tổ chức phụ thuộc vào:

1) quy mô của tổ chức và loại hình hoạt động, quy trình,

sản phẩm và dịch vụ của tổ chức;

2) sự phức tạp và sự tương tác của các quá trình; và

3) năng lực của con người.

**Khởi tạo và cập nhật:**

Phải đảm bảo:

* Định danh và mô tả (ví dụ như tiêu đề, ngày tháng, tác giả, hoặc mã số tài liệu……) một cách rõ ràng;
* Định dạng (ví dụ như ngôn ngữ, phiên bản phần mềm, đồ họa) và phương tiện (ví dụ như giấy, điện tử);
* Được xem xét và phê duyệt cho thích hợp và thỏa đáng.

**Quản lý thông tin Thông tin phải được kiểm soát để đảm bảo:**

* Luôn sẵn sàng khi cần;
* Được bảo vệ khỏi truy cập/truy xuất/trình sửa trái phép;
* Có các quy định cụ thể về phân phối, lưu trữ, kiểm soát phiên bản và hủy bỏ.

CHÚ THÍCH: Thuật ngữ Truy cập bao hàm ý nghĩa một quyết định liên quan đến việc cho phép chỉ xem thông tin được lập văn bản, hoặc sự cho phép và thẩm quyền để xem và thay đổi thông tin được lập văn bản,….

* 1. **Điều hành**
     1. **Hoạch định và kiểm soát hoạt động**

Tổ chức phải lập kế hoạch, thực hiện và kiểm soát các quy trình cần thiết để đáp ứng yêu cầu an toàn thông tin, và triển khai các hoạt động đã xác định trong Điều 1.5, thông qua:

* thiết lập các tiêu chí cho các quá trình;
* thực hiện kiểm soát các quá trình phù hợp với các tiêu chí.

Thông tin dạng văn bản sẽ sẵn có ở mức độ cần thiết để đảm bảo tin cậy rằng các quá trình đã được tiến hành theo kế hoạch.

Tổ chức phải kiểm soát các thay đổi kế hoạch và xem xét các hậu quả của sự thay đổi ngoài ý muốn, có hành động để giảm thiểu bất kỳ tác dụng phụ nào, khi cần thiết.

Tổ chức phải đảm bảo rằng các quá trình, sản phẩm hoặc dịch vụ được cung cấp bởi bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin được kiểm soát.

* + 1. **Đánh giá rủi ro an toàn thông tin**

Tổ chức phải:

* Tiến hành đánh giá rủi ro định kỳ hoặc khi có thay đổi lớn;
* Tuân theo tiêu chí được đề cập trong 1.5.2 Mục tiêu an toàn thông tin và hoạch định để đạt được mục tiêu) (ví dụ: xác suất, tác động, mức độ rủi ro);
* Lưu giữ tài liệu kết quả đánh giá rủi ro (file, báo cáo…).
  + 1. **Xử lý rủi ro an toàn thông tin**

Tổ chức cần:

* Triển khai kế hoạch xử lý rủi ro đã xây dựng (ví dụ: giảm thiểu, tránh, chấp nhận, chuyển giao);
* Lưu giữ tài liệu kết quả xử lý rủi ro (như báo cáo xử lý, bằng chứng triển khai biện pháp bảo vệ...).

**Ghi chú dành cho triển khai thực tế**:

* Phần này cực kỳ quan trọng khi thực hiện chứng nhận ISO 27001, vì nó liên quan trực tiếp đến risk assessment và risk treatment.
* Có thể kết hợp với công cụ như OCTAVE, ISO 27005, hoặc bảng Excel quản lý rủi ro với cột mô tả – xác suất – tác động – phương án xử lý.
  1. **Đánh giá hiệu quả**
     1. **Giám sát, đo lường, phân tích và đánh giá**

Tổ chức phải:

Đánh giá sự thực thi và tính hiệu lực của ISMS (Hệ thống Quản lý ATTT);

Xác định:

* + Những gì cần phải được giám sát và đo lường, bao gồm các quá trình và các biện pháp kiểm soát an toàn thông tin;
  + Các phương pháp giám sát, đo lường, phân tích và đánh giá, nếu có, để đảm bảo kết quả hợp lệ; Các phương pháp được lựa chọn cần tạo ra kết quả có thể so sánh được và có thể tái sử dụng, được coi là hợp lệ.
  + Khi nào hoạt động giám sát và đo lường được thực hiện;
  + Ai phải thực hiện giám sát và đo lường
  + Khi nào các kết quả từ giám sát và đo lường được phân tích và đánh giá;
  + Ai phải phân tích và đánh giá các kết quả này.

Thông tin dạng văn bản phải sẵn có làm bằng chứng về kết quả giám sát và đo lường.

Tổ chức phải đánh giá việc thực hiện an toàn thông tin và tính hiệu lực của hệ thống quản lý an toàn thông tin.

* + 1. **Đánh giá nội bộ**

Tổ chức phải lập kế hoạch, thiết lập, triển khai và duy trì (các) chương trình đánh giá, bao gồm tần suất, phương pháp, trách nhiệm, yêu cầu lập kế hoạch và báo cáo.

Chương trình đánh giá có tính đến tầm quan trọng của cá quá trình có liên quan và kết quả các cuộc đánh giá trước đó;

Tổ chức phải:

* Xác định các tiêu chí đánh giá và phạm vi cho từng cuộc đánh giá;
* Lựa chọn đánh giá viên và thực hiện việc đánh giá đảm bảo tính khách quan và công bằng của quá trình đánh giá;
* Đảm bảo rằng các kết quả của cuộc đánh giá được báo cáo đến các cấp quản lý có liên quan;

Thông tin được lập văn bản phải sẵn có làm bằng chứng về việc thực hiện (các) chương trình đánh giá và các kết quả đánh giá.

* + 1. **Xem xét của lãnh đạo**

**Khái quát**

Lãnh đạo cao nhất phải xem xét định kỳ theo kế hoạch hệ thống ISMS của tổ chức để đảm bảo nó luôn phù hợp, thoả đáng và có hiệu lực.

**Đầu vào xem xét của lãnh đạo**

1. Việc xem xét của lãnh đạo phải bao gồm sự xem xét:
2. Tình trạng của các hành động từ lần xem xét lãnh đạo trước đó;
3. Các thay đổi trong các vấn đề bên ngoài và nội bộ có liên quan đến hệ thống quản lý an toàn thông tin;
4. Những thay đổi về nhu cầu và mong đợi của các bên quan tâm có liên quan đến hệ thống quản lý an toàn thông tin;
5. Phản hồi về việc thực hiện an toàn thông tin, bao gồm:
6. Các sự không phù hợp và các hành động khắc phục;
7. Các kết quả giám sát và đo lường;
8. Các kết quả đánh giá;
9. Sự đáp ứng các mục tiêu an toàn thông tin;
10. Thông tin phản hồi từ các bên quan tâm;
11. Kết quả đánh giá rủi ro và tình trạng của kế hoạch xử lý rủi ro;
12. Các cơ hội cải tiến liên tục.

**Kết quả xem xét của lãnh đạo**

Kết quả xem xét của lãnh đạo phải bao gồm những quyết định liên quan đến các cơ hội cải tiến liên tục và bất cứ nhu cầu cần thiết nào cho các thay đổi đối với hệ thống quản lý an toàn thông tin.

Thông tin được lập văn bản phải sẵn có làm bằng chứng về kết quả của các cuộc xem xét của lãnh đạo.

* 1. **Cải tiến**
     1. **Cải tiến liên tục**

Tổ chức phải liên tục cải tiến nâng cao tính thích hợp, đầy đủ và hiệu lực của hệ thống quản lý an toàn thông tin.

* + 1. **Sự không phù hợp và hành động khắc phục**

Khi xảy ra sự không phù hợp, tổ chức phải:

1. Phản ứng với sự không phù hợp, và có thể áp dụng:
2. Có hành động để kiểm soát và sửa chữa nó; và
3. Giải quyết các hậu quả;
4. Đánh giá sự cần thiết phải hành động để loại bỏ nguyên nhân của sự không phù hợp, để nó không tái xuất hiện hay xảy ra ở những nơi khác, bằng cách:
5. Xem xét sự không phù hợp;
6. Xác định nguyên nhân của sự không phù hợp; và
7. Xác định nếu có sự không phù hợp tương tự tồn tại, hoặc có khả năng có thể xảy ra;
8. Thực hiện bất kỳ hành động cần thiết nào;
9. Xem xét hiệu lực của bất kỳ hành động khắc phục đã thực hiện;
10. Thay đổi hệ thống quản lý an toàn thông tin, nếu cần thiết.
    1. **Phụ lục A (quy định)**

Các biện pháp kiểm soát an toàn thông tin tham khảo Các biện pháp kiểm soát an toàn thông tin được liệt kê trong bảng A.1 bắt nguồn trực tiếp và có liên kết với các mục từ mục 5 đến 8 được liệt kê trong ISO/IEC27002:2022 và phải được sử dụng trong bối cảnh của điều khoản **2.6.1. Hành động để giải quyết rủi ro và các cơ hội cải tiến - c) Xử lý rủi ro an toàn thông tin.**

**Bảng A.1- Các biện pháp kiểm soát an toàn thông tin**

|  |  |  |  |
| --- | --- | --- | --- |
| **A.5 Organizational controls *– Các biện pháp kiểm soát về tổ chức*** | | | |
|  | A.5.1 | Policies for information security | Chính sách an toàn thông tin |
|  | A.5.2 | Information security roles and responsibilities | Vai trò và trách nhiệm an toàn thông tin |
|  | A.5.3 | Segregation of duties | Phân tách nhiệm vụ |
|  | A.5.4 | Management responsibilities | Trách nhiệm của lãnh đạo |
|  | A.5.5 | Contact with authorities | Thiết lập và duy trì liên lạc với các cơ quan chức năng |
|  | A.5.6 | Contact with special interest groups | Liên lạc thường xuyên với các nhóm chuyên gia |
|  | A.5.7 | Threat intelligence | Cập nhật thông tin tình báo về các mối đe dọa |
|  | A.5.8 | Information security in project management | An toàn thông tin trong quản lý dự án |
|  | A.5.9 | Inventory of information and other associated assets | Kiểm kê thông tin và các tài sản liên quan khác |
|  | A.5.10 | Acceptable use of information and other associated assets | Việc sử dụng thông tin và các tài sản liên quan khác được chấp nhận |
|  | A.5.11 | Return of assets | Hoàn trả tài sản |
|  | A.5.12 | Classification of information | Phân loại thông tin |
|  | A.5.13 | Labelling of information | Ghi nhãn thông tin |
|  | A.5.14 | Information transfer | Chuyển giao thông tin |
|  | A.5.15 | Access control | Kiểm soát truy cập |
|  | A.5.16 | Identity management | Quản lý danh tính |
|  | A.5.17 | Authentication information | Thông tin xác thực |
|  | A.5.18 | Access rights | Quyền truy cập |

|  |  |  |  |
| --- | --- | --- | --- |
|  | A.5.19 | Information security in supplier relationships | An toàn thông tin trong các mối quan hệ với nhà cung cấp |
|  | A.5.20 | Addressing information security within supplier agreements | Giải quyết vấn đề an toàn thông tin trong các thỏa thuận với nhà cung cấp |
|  | A.5.21 | Managing information security in the ICT supply chain | Quản lý an toàn thông tin trong chuỗi cung ứng CNTT- TT |
|  | A.5.22 | Monitoring, review and change management of supplier services | Giám sát, xem xét và quản lý thay đổi các dịch vụ của nhà cung cấp |
|  | A.5.23 | Information security for use of cloud services | An toàn thông tin khi sử dụng các dịch vụ đám mây |
|  | A.5.24 | Information security incident management planning and preparation | Lập kế hoạch và chuẩn bị quản lý sự cố an toàn thông tin |
|  | A.5.25 | Assessment and decision on information security events | Đánh giá và quyết định các sự kiện an toàn thông tin |
|  | A.5.26 | Response to information security incidents | Ứng phó sự cố an toàn thông tin |
|  | A.5.27 | Learning from information security incidents | Rút kinh nghiệm từ các sự cố an toàn thông tin |
|  | A.5.28 | Collection of evidence | Thu thập bằng chứng |
|  | A.5.29 | Information security during disruption | An toàn thông tin trong thời gian gián đoạn |
|  | A.5.30 | ICT readiness for business continuity | Sẵn sàng về CNTT-TT cho hoạt động kinh doanh liên tục |
|  | A.5.31 | Legal, statutory, regulatory and contractual requirements | Các yêu cầu pháp lý, luật định, quy định và hợp đồng |
|  | A.5.32 | Intellectual property rights | Quyền sở hữu trí tuệ |
|  | A.5.33 | Protection of records | Bảo vệ hồ sơ |
|  | A.5.34 | Privacy and protection of PII | Quyền riêng tư và bảo vệ thông tin định danh cá nhân |
|  | A.5.35 | Independent review of information security | Xem xét độc lập về an toàn thông tin |
|  | A.5.36 | Compliance with policies, rules and standards for information security | Tuân thủ các chính sách, quy tắc và tiêu chuẩn về an toàn thông tin |
|  | A.5.37 | Documented operating procedures | Quy trình vận hành được lập thành văn bản |

|  |  |  |  |
| --- | --- | --- | --- |
| **A.6 People controls – *Các biện pháp kiểm soát về con người*** | | | |
|  | A.6.1 | Screening | Sàng lọc |
|  | A.6.2 | Terms and conditions of employment | Điều khoản và điều kiện làm việc |
|  | A.6.3 | Information security awareness, education and training | Nhận thức, giáo dục và đào tạo về an toàn thông tin |
|  | A.6.4 | Disciplinary process | Quy trình xử lý kỷ luật |
|  | A.6.5 | Responsibilities after termination or change of employment | Trách nhiệm sau khi thôi việc hoặc thay đổi công việc |
|  | A.6.6 | Confidentiality or non-disclosure agreements | Thỏa thuận bảo mật hoặc không tiết lộ thông tin |
|  | A.6.7 | Remote working | Làm việc từ xa |
|  | A.6.8 | Information security event reporting | Báo cáo sự kiện an toàn thông tin |
| **A.7 Physical controls – *Các biện pháp kiểm soát về vật lý*** | | | |
|  | A.7.1 | Physical security perimeters | Các vành đai an ninh vật lý |
|  | A.7.2 | Physical entry | Cổng ra vào vật lý |
|  | A.7.3 | Securing offices, rooms and facilities | Bảo vệ văn phòng, phòng và cơ sở vật chất |
|  | A.7.4 | Physical security monitoring | Giám sát an ninh vật lý |
|  | A.7.5 | Protecting against physical and environmental threats | Bảo vệ chống lại các mối đe dọa vật lý và môi trường |
|  | A.7.6 | Working in secure areas | Làm việc trong các khu vực an toàn |
|  | A.7.7 | Clear desk and clear screen | Bàn sạch và màn hình sạch |
|  | A.7.8 | Equipment siting and protection | Bố trí và bảo vệ thiết bị |
|  | A.7.9 | Security of assets off-premises | An toàn tài sản bên ngoài trụ sở |
|  | A.7.10 | Storage media | Phương tiện lưu trữ |
|  | A.7.11 | Supporting utilities | Các tiện ích hỗ trợ |
|  | A.7.12 | Cabling security | An toàn dây cáp |
|  | A.7.13 | Equipment maintenance | Bảo trì thiết bị |
|  | A.7.14 | Secure disposal or re-use of equipment | Xử lý hoặc tái sử dụng thiết bị an toàn |

|  |  |  |  |
| --- | --- | --- | --- |
| **A.8 Technological controls – *Các biện pháp kiểm soát về kỹ thuật*** | | | |
|  | A.8.1 | User endpoint devices | Thiết bị đầu cuối của người dùng |
|  | A.8.2 | Privileged access rights | Quyền truy cập đặc quyền |
|  | A.8.3 | Information access restriction | Hạn chế truy cập thông tin |
|  | A.8.4 | Access to source code | Truy cập mã nguồn |
|  | A.8.5 | Secure authentication | Xác thực an toàn |
|  | A.8.6 | Capacity management | Quản lý năng lực |
|  | A.8.7 | Protection against malware | Bảo vệ chống lại phần mềm độc hại |
|  | A.8.8 | Management of technical vulnerabilities | Quản lý các lỗ hổng kỹ thuật |
|  | A.8.9 | Configuration management | Quản lý cấu hình |
|  | A.8.10 | Information deletion | Xóa thông tin |
|  | A.8.11 | Data masking | Che dấu dữ liệu |
|  | A.8.12 | Data leakage prevention | Ngăn chặn rò rỉ dữ liệu |
|  | A.8.13 | Information backup | Sao lưu thông tin |
|  | A.8.14 | Redundancy of information processing facilities | Dự phòng các phương tiện xử lý thông tin |
|  | A.8.15 | Logging | Ghi nhật ký |
|  | A.8.16 | Monitoring activities | Các hoạt động giám sát |
|  | A.8.17 | Clock synchronization | Đồng bộ thời gian |
|  | A.8.18 | Use of privileged utility programs | Sử dụng các chương trình tiện ích đặc quyền |
|  | A.8.19 | Installation of software on operational systems | Cài đặt phần mềm trên các hệ điều hành |
|  | A.8.20 | Networks security | An toàn mạng |
|  | A.8.21 | Security of network services | An toàn các dịch vụ mạng |
|  | A.8.22 | Segregation of networks | Phân tách mạng |
|  | A.8.23 | Web filtering | Lọc web |
|  | A.8.24 | Use of cryptography | Sử dụng mật mã |
|  | A.8.25 | Secure development life cycle | Vòng đời phát triển an toàn |
|  | A.8.26 | Application security requirements | Yêu cầu an toàn ứng dụng |
|  | A.8.27 | Secure system architecture and engineering principles | Kiến trúc hệ thống an toàn và các nguyên tắc kỹ thuật |

|  |  |  |  |
| --- | --- | --- | --- |
|  | A.8.28 | Secure coding | Mã hóa an toàn |
|  | A.8.29 | Security testing in development and acceptance | Kiểm tra bảo mật trong quá trình phát triển và chấp nhận |
|  | A.8.30 | Outsourced development | Phát triển thuê ngoài |
|  | A.8.31 | Separationofdevelopment,testandproductionenvironments | Phân tách môi trường phát triển, kiểm thử và sản xuất |
|  | A.8.32 | Change management | Quản lý thay đổi |
|  | A.8.33 | Test information | Thông tin kiểm tra |
|  | A.8.34 | Protection of information systems during audit testing | Bảo vệ hệ thống thông tin trong quá trình kiểm tra đánh giá |

*\*Nội dung chi tiết các biện pháp kiểm soát và các hướng dẫn thực hiện kiểm soát, xin tham khảo bản dịch Tiếng Việt của ISO/IEC 27002:2022 đi kèm bản dịch này*.

1. **Hiểu cấu trúc tiêu chuẩn ISO/IEC 27001:2022**

ISO 27001 bản mới gồm 2 phần chính:

**Main Clauses**: Điều khoản tổng quát (Clause 4-10) về yêu cầu xây dựng ISMS (Information Security Management System).

**Annex A**: 93 control chia thành 4 nhóm chủ đề lớn:

|  |  |  |
| --- | --- | --- |
| **Nhóm chủ đề** | **Nội dung** | **Số lượng controls** |
| **A.5 Organizational Controls** | Các chính sách, phân công trách nhiệm, quản lý rủi ro, đào tạo nhận thức | 37 controls |
| **A.6 People Controls** | Bảo vệ nhân sự, phân quyền truy cập, đào tạo chuyên sâu | 8 controls |
| **A.7 Physical Controls** | Bảo vệ vật lý như data center, access control vật lý | 14 controls |
| **A.8 Technological Controls** | Bảo vệ hệ thống IT: SIEM, Endpoint Security, Patch Management, Encryption... | 34 controls |

Từ đó có thể rút ra quy chuẩn về an toàn thông tin cho tổ chức thành 4 phần chính và các giải pháp cho từng phần

|  |  |  |  |
| --- | --- | --- | --- |
| **Nhóm chủ đề** | **Tương ứng ISO** | **Nội dung** | **Ví dụ giải pháp** |
| **Con người (People)** | A.6 | Đào tạo, kiểm soát truy cập người dùng, xác thực mạnh | Đào tạo, kiểm soát truy cập người dùng, xác thực mạnh |
| **Ứng dụng (Application)** | A.8 | An toàn phần mềm, kiểm soát ứng dụng, secure coding | WAF, DAST, SAST |
| **Kiến trúc hệ thống (Infrastructure)** | A.5, A.7, A.8 | Thiết kế hệ thống an toàn, phân vùng mạng, giám sát, backup | SIEM, IDS/IPS, Zero Trust Network |
| **Dữ liệu và Tài sản (Data/Asset)** | A.5, A.8 | Bảo vệ dữ liệu, phân loại tài sản, mã hóa, quản lý backup | DLP, Encryption, Data Classification |

1. **Mối đe dọa APT (Advanced Persistent Threat) và liên hệ với ISO/IEC 27001**

“Trong thời đại số hóa phát triển mạnh mẽ, không gian mạng trở thành đấu trường căng thẳng với hàng loạt mối đe dọa an ninh mạng ngày càng tinh vi. Năm 2024 và đầu năm 2025 đánh dấu sự bùng nổ của các cuộc tấn công mạng quy mô lớn, gây ảnh hưởng nghiêm trọng đến doanh nghiệp, tổ chức và cả cá nhân. Sự gia tăng của trí tuệ nhân tạo (AI), sự mở rộng của Internet vạn vật (IoT) và các lỗ hổng bảo mật trong hệ thống đám mây đã khiến các tổ chức trở thành mục tiêu dễ dàng của tội phạm mạng.Theo các chuyên gia, tội phạm mạng không chỉ nhắm vào tài sản tài chính mà còn khai thác thông tin cá nhân, dữ liệu doanh nghiệp và cả cơ sở hạ tầng trọng yếu. Trước tình hình này, việc nâng cao nhận thức và triển khai các biện pháp bảo vệ mạnh mẽ là điều tất yếu để đảm bảo an toàn thông tin trong kỷ nguyên số.” (Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT, 2025)

* 1. **Tổng quan về APT**

Advanced Persistent Threat (APT) đại diện cho một hình thức tấn công mạng phức tạp và tinh vi được thực hiện bởi các đối tượng có kỹ năng chuyên sâu và nguồn lực dồi dào. Không như các cuộc tấn công thông thường, APT được đặc trưng bởi tính chất bền bỉ, mục tiêu rõ ràng và chiến lược dài hạn. Các cuộc tấn công này thường được thiết kế và thực hiện bởi các nhóm được tài trợ bởi quốc gia, tổ chức tội phạm có tổ chức hoặc đối thủ cạnh tranh có tiềm lực tài chính mạnh.

Đối tượng mục tiêu của APT thường là các tổ chức có giá trị cao như cơ quan chính phủ, tập đoàn đa quốc gia, cơ sở hạ tầng quan trọng, tổ chức quốc phòng, hoặc các tổ chức nắm giữ dữ liệu nhạy cảm và tài sản trí tuệ có giá trị. APT không chỉ đơn thuần nhằm vào việc thỏa mãn các mục tiêu tài chính ngắn hạn mà còn hướng đến các lợi ích chiến lược lâu dài như thu thập thông tin tình báo, gián điệp công nghiệp, giành lợi thế cạnh tranh, hoặc thậm chí là phá hoại cơ sở hạ tầng quan trọng.

Điểm đặc biệt của các cuộc tấn công APT là khả năng duy trì sự hiện diện không bị phát hiện trong hệ thống mục tiêu trong thời gian dài, đôi khi kéo dài nhiều năm. Trong suốt thời gian này, đối tượng tấn công liên tục điều chỉnh chiến thuật, kỹ thuật và quy trình để đối phó với các biện pháp bảo mật mới và tiếp tục khai thác hệ thống mục tiêu.

* 1. **Đặc điểm chính của APT**

Các cuộc tấn công APT có những đặc điểm riêng biệt, phân biệt chúng với các mối đe dọa an ninh mạng thông thường. Việc hiểu rõ những đặc điểm này là cần thiết để xây dựng các chiến lược phòng thủ hiệu quả.

**Tính phức tạp và tinh vi cao** là một trong những đặc điểm nổi bật nhất của APT. Các đối tượng tấn công thường sử dụng kết hợp nhiều kỹ thuật tấn công tiên tiến, bao gồm cả việc khai thác các lỗ hổng zero-day chưa được biết đến, các kỹ thuật kỹ thuật xã hội phức tạp, và malware tùy chỉnh được thiết kế đặc biệt để vượt qua các hệ thống phòng thủ cụ thể. Các công cụ và phương pháp này thường được phát triển riêng cho từng chiến dịch tấn công, làm cho chúng khó bị phát hiện bởi các giải pháp bảo mật dựa trên dấu hiệu (signature-based) truyền thống.

**Mục tiêu rõ ràng và nghiên cứu kỹ lưỡng** là đặc điểm thứ hai của APT. Trước khi tiến hành tấn công, đối tượng APT thường dành thời gian đáng kể để nghiên cứu về mục tiêu, bao gồm cấu trúc tổ chức, cơ sở hạ tầng CNTT, các quy trình bảo mật, và thậm chí là thông tin cá nhân của nhân viên chủ chốt. Điều này cho phép họ thiết kế các cuộc tấn công được điều chỉnh riêng để tăng tối đa khả năng thành công và giảm thiểu nguy cơ bị phát hiện.

**Thời gian kéo dài và kiên trì** là đặc điểm thứ ba đáng chú ý của APT. Khác với các cuộc tấn công thông thường nhằm mục đích thu lợi nhanh chóng, các chiến dịch APT thường kéo dài trong nhiều tháng hoặc thậm chí nhiều năm. Trong thời gian này, đối tượng tấn công duy trì sự hiện diện liên tục trong hệ thống mục tiêu, liên tục thu thập dữ liệu và điều chỉnh chiến thuật để đạt được mục tiêu lâu dài của họ.

**Khả năng thích ứng cao** là một trong những lý do chính giúp APT duy trì hiệu quả trong thời gian dài. Đối tượng tấn công thường xuyên thay đổi công cụ, kỹ thuật và quy trình (TTPs) của họ để tránh bị phát hiện và đối phó với các biện pháp phòng thủ mới được triển khai. Khi phát hiện ra một lỗ hổng bị vá hoặc một kỹ thuật không còn hiệu quả, họ nhanh chóng chuyển sang các phương pháp thay thế để duy trì quyền truy cập vào hệ thống mục tiêu.

**Nguồn lực dồi dào và tổ chức chuyên nghiệp** là đặc điểm quan trọng khác của APT. Các nhóm APT thường có cấu trúc tổ chức chặt chẽ, với các thành viên chuyên về các lĩnh vực khác nhau như nghiên cứu lỗ hổng, phát triển malware, kỹ thuật xã hội, và phân tích tình báo. Họ thường được tài trợ bởi các quốc gia, tổ chức tội phạm quy mô lớn, hoặc các đối thủ cạnh tranh, cung cấp cho họ nguồn lực cần thiết để duy trì các chiến dịch tấn công phức tạp và dài hạn.

**Khả năng che giấu và xóa dấu vết** là đặc điểm cuối cùng nhưng quan trọng không kém của APT. Các đối tượng tấn công triển khai các kỹ thuật ẩn mình tinh vi để tránh bị phát hiện, bao gồm việc mã hóa liên lạc, sử dụng các kênh liên lạc bí mật, và thường xuyên xóa dấu vết của hoạt động của họ trong hệ thống mục tiêu. Điều này làm cho việc phát hiện và điều tra các cuộc tấn công APT trở nên đặc biệt khó khăn, thậm chí đối với các tổ chức có đội ngũ bảo mật mạnh mẽ.

* 1. **Vòng đời của APT**

Vòng đời của một cuộc tấn công APT thường tuân theo một quy trình có cấu trúc và phân chia thành nhiều giai đoạn riêng biệt, mỗi giai đoạn đều có mục tiêu và phương pháp thực hiện cụ thể. Việc hiểu rõ vòng đời này giúp các tổ chức nhận biết và phát hiện các cuộc tấn công APT ở các giai đoạn khác nhau, từ đó phát triển các chiến lược phòng thủ phù hợp.

**Giai đoạn trinh sát và thu thập thông tin** là bước đầu tiên và nền tảng của mọi cuộc tấn công APT thành công. Trong giai đoạn này, đối tượng tấn công tập trung vào việc thu thập thông tin chi tiết về tổ chức mục tiêu, bao gồm cấu trúc tổ chức, hệ thống CNTT, công nghệ đang sử dụng, các biện pháp bảo mật hiện có, và thông tin về nhân viên chủ chốt. Quá trình này có thể kéo dài nhiều tuần hoặc thậm chí nhiều tháng và thường sử dụng kết hợp nhiều phương pháp thu thập thông tin như OSINT (Open Source Intelligence), kỹ thuật xã hội, và quét lỗ hổng từ xa. Thông tin thu thập được trong giai đoạn này sẽ được sử dụng để lập kế hoạch chi tiết cho các giai đoạn tiếp theo, xác định các điểm yếu tiềm năng và phát triển các chiến thuật xâm nhập phù hợp.

**Giai đoạn xâm nhập ban đầu** là bước tiếp theo, trong đó đối tượng tấn công thiết lập điểm truy cập ban đầu vào hệ thống của tổ chức mục tiêu. Dựa trên thông tin thu thập được trong giai đoạn trinh sát, đối tượng tấn công lựa chọn phương pháp xâm nhập có khả năng thành công cao nhất. Các phương pháp phổ biến bao gồm spear phishing (email lừa đảo có mục tiêu cụ thể), khai thác các lỗ hổng trong các ứng dụng web hoặc dịch vụ mạng hướng ra bên ngoài, tấn công chuỗi cung ứng thông qua các nhà cung cấp bên thứ ba, hoặc thậm chí là tấn công vật lý thông qua thiết bị USB độc hại. Mục tiêu của giai đoạn này là thiết lập một điểm tựa ban đầu trong hệ thống mục tiêu, từ đó có thể mở rộng phạm vi kiểm soát trong các giai đoạn tiếp theo.

**Giai đoạn thiết lập bệ đỡ** diễn ra ngay sau khi xâm nhập thành công. Trong giai đoạn này, đối tượng tấn công tập trung vào việc củng cố vị trí của họ trong hệ thống mục tiêu bằng cách cài đặt các công cụ để đảm bảo họ có thể duy trì quyền truy cập lâu dài. Điều này thường bao gồm việc cài đặt backdoor, rootkit, hoặc các công cụ RAT (Remote Access Trojan) cho phép họ kiểm soát hệ thống từ xa. Các công cụ này thường được ngụy trang dưới dạng phần mềm hợp pháp hoặc được ẩn sâu trong hệ thống để tránh bị phát hiện. Đối tượng tấn công cũng thường thiết lập các kênh liên lạc bí mật với máy chủ điều khiển và kiểm soát (C2) bên ngoài, cho phép họ gửi lệnh và nhận dữ liệu từ hệ thống bị xâm nhập.

**Giai đoạn mở rộng kiểm soát** là giai đoạn trọng tâm của cuộc tấn công, trong đó đối tượng APT tập trung vào việc di chuyển ngang (lateral movement) trong mạng mục tiêu để mở rộng quyền kiểm soát của họ. Bằng cách khai thác các lỗ hổng nội bộ, đánh cắp thông tin xác thực, hoặc sử dụng các kỹ thuật leo thang đặc quyền, đối tượng tấn công dần dần giành quyền truy cập vào các hệ thống quan trọng hơn trong mạng. Họ thường di chuyển một cách thận trọng và từ từ, tránh gây ra các hoạt động bất thường có thể kích hoạt cảnh báo bảo mật. Mục tiêu cuối cùng của giai đoạn này là giành quyền kiểm soát đối với các hệ thống quan trọng và có giá trị nhất trong mạng mục tiêu.

**Giai đoạn thu thập thông tin nội bộ** diễn ra sau khi đối tượng tấn công đã mở rộng phạm vi kiểm soát của họ trong mạng mục tiêu. Trong giai đoạn này, họ tập trung vào việc xác định vị trí và tiếp cận dữ liệu có giá trị trong hệ thống. Điều này có thể bao gồm thông tin tài chính, dữ liệu khách hàng, tài sản trí tuệ, thông tin chiến lược, hoặc bất kỳ dữ liệu nào khác phù hợp với mục tiêu của cuộc tấn công. Đối tượng tấn công thường sử dụng các công cụ tìm kiếm dữ liệu tự động hoặc thực hiện các hoạt động do thám có mục tiêu để xác định vị trí của thông tin có giá trị.

**Giai đoạn chiếm đoạt dữ liệu** là giai đoạn mà đối tượng tấn công thực hiện mục tiêu chính của họ: khai thác và trích xuất dữ liệu có giá trị từ hệ thống mục tiêu. Dữ liệu bị đánh cắp thường được mã hóa, nén, hoặc ngụy trang dưới dạng lưu lượng mạng bình thường để tránh bị phát hiện bởi các hệ thống giám sát mạng. Đối tượng tấn công có thể sử dụng các kỹ thuật như DNS tunneling, steganography, hoặc liên lạc qua các kênh mạng hợp pháp để truyền dữ liệu ra khỏi tổ chức mục tiêu. Trong một số trường hợp, đặc biệt là khi mục tiêu là phá hoại, giai đoạn này có thể bao gồm việc sửa đổi hoặc phá hủy dữ liệu quan trọng thay vì chiếm đoạt nó.

**Giai đoạn duy trì hiện diện** là giai đoạn cuối cùng của vòng đời APT, nhưng không kém phần quan trọng. Sau khi đã đạt được mục tiêu ban đầu, đối tượng tấn công thường muốn duy trì quyền truy cập vào hệ thống mục tiêu để sử dụng trong tương lai. Họ có thể cài đặt các backdoor bổ sung, tạo tài khoản người dùng ẩn, hoặc thiết lập các cơ chế kiên trì khác để đảm bảo họ có thể quay lại hệ thống mục tiêu bất cứ khi nào cần thiết. Đối tượng tấn công cũng thường xuyên xóa dấu vết của hoạt động của họ, làm sạch các log hệ thống, và loại bỏ bất kỳ dấu hiệu nào của sự xâm nhập để tránh bị phát hiện trong các cuộc điều tra an ninh.

* 1. **Quy trình tấn công**

**Các giai đoạn tấn công APT**

**- Giai đoạn 1: Xâm nhập ban đầu**

Các tổ chức thường bị xâm nhập thông qua nhiều vector tấn công khác nhau như ứng dụng web, tài nguyên mạng hoặc thông qua yếu tố con người. Khi bắt đầu cuộc tấn công, đối tượng APT thường triển khai các tệp tin độc hại thông qua việc khai thác các lỗ hổng trong ứng dụng web, dịch vụ mạng, hoặc sử dụng kỹ thuật kỹ thuật xã hội tinh vi như spear phishing. Các email lừa đảo này thường được cá nhân hóa cao độ, chứa tệp đính kèm độc hại hoặc liên kết dẫn đến trang web độc hại đã được thiết kế đặc biệt để khai thác lỗ hổng trình duyệt hoặc lừa đảo thông tin đăng nhập.

Trong nhiều trường hợp, đối tượng tấn công có thể đồng thời thực hiện các cuộc tấn công DDoS (Distributed Denial of Service) như một chiến thuật đánh lạc hướng. Điều này tạo ra sự hỗn loạn và buộc đội ngũ an ninh phải tập trung vào việc khôi phục các dịch vụ bị gián đoạn, từ đó làm giảm khả năng phát hiện hoạt động xâm nhập thực sự đang diễn ra ở nơi khác trong mạng.

Ngay sau khi thiết lập được quyền truy cập ban đầu, đối tượng APT nhanh chóng cài đặt phần mềm độc hại hoặc backdoor shell cho phép duy trì quyền truy cập liên tục vào mạng và điều khiển các hoạt động tấn công từ xa. Các backdoor này thường được ngụy trang dưới dạng phần mềm hợp pháp, được thiết kế để tránh bị phát hiện bởi các giải pháp bảo mật truyền thống và thường sử dụng các kênh liên lạc mã hóa để giao tiếp với máy chủ điều khiển và kiểm soát (C&C).

**- Giai đoạn 2: Mở rộng phạm vi**

Sau khi thiết lập được điểm tựa vững chắc trong hệ thống mạng mục tiêu, đối tượng APT chuyển sang giai đoạn mở rộng quyền kiểm soát trong toàn bộ cơ sở hạ tầng CNTT của tổ chức. Đây là quá trình di chuyển ngang (lateral movement) và leo thang đặc quyền (privilege escalation) để đạt được quyền truy cập sâu hơn vào các hệ thống quan trọng.

Trong giai đoạn này, kẻ tấn công thực hiện rà quét các hệ thống khác trong mạng, thu thập thông tin xác thực của người dùng thông qua các công cụ như mimikatz hoặc quá trình khai thác bộ nhớ, đồng thời phát tán các mã độc bổ sung để thiết lập nhiều điểm truy cập vào các kho dữ liệu nhạy cảm. Bằng cách này, đối tượng APT có thể tiếp cận và thu thập các thông tin kinh doanh có giá trị, bao gồm thông tin về dòng sản phẩm, dữ liệu nhân viên, chiến lược kinh doanh và hồ sơ tài chính.

Tùy thuộc vào động cơ và mục tiêu cuối cùng, dữ liệu thu thập được có thể được chuyển giao cho đối thủ cạnh tranh, bị sửa đổi hoặc phá hủy để gây thiệt hại cho hoạt động kinh doanh, hoặc được sử dụng để thiết lập quyền kiểm soát toàn diện đối với cơ sở hạ tầng của tổ chức. Trong trường hợp động cơ là phá hoại, giai đoạn này được sử dụng để nắm quyền kiểm soát các chức năng quan trọng và điều khiển chúng theo một trình tự được lập trình sẵn nhằm tối đa hóa thiệt hại. Ví dụ, đối tượng APT có thể xóa toàn bộ cơ sở dữ liệu quan trọng, phá hủy các bản sao lưu, và làm tê liệt hệ thống mạng để kéo dài thời gian khôi phục.

**- Giai đoạn 3: Khai thác thông tin**

Trong suốt quá trình thực hiện cuộc tấn công APT, thông tin bị đánh cắp thường được tập hợp và lưu trữ tạm thời tại một vị trí an toàn bên trong hệ thống mạng đã bị xâm nhập. Khi đã thu thập đủ dữ liệu theo mục tiêu đã định, đối tượng APT sẽ thực hiện quá trình trích xuất dữ liệu một cách tinh vi và khó phát hiện.

Để tăng khả năng thành công trong giai đoạn này, các đối tượng APT thường triển khai các chiến thuật đa dạng nhằm tạo ra nhiễu loạn trong hệ thống giám sát an ninh mạng, từ đó đánh lạc hướng đội ngũ bảo mật của tổ chức. Những chiến thuật này có thể bao gồm các cuộc tấn công DDoS có chủ đích, khai thác các lỗ hổng trong hệ thống tường lửa hoặc proxy, hoặc tạo ra các sự cố hệ thống giả để thu hút sự chú ý. Trong khi đội ngũ an ninh bận rộn ứng phó với các vấn đề này, dữ liệu quan trọng được truyền ra ngoài thông qua các kênh bị che giấu, sử dụng các kỹ thuật ẩn dấu dữ liệu (data obfuscation), mã hóa hoặc giả mạo lưu lượng mạng hợp pháp để tránh bị phát hiện bởi các hệ thống phát hiện và phòng chống xâm nhập.

**- Giai đoạn 4: Duy trì hiện diện**

Một đặc điểm quan trọng của các cuộc tấn công APT là tính bền vững và khả năng duy trì sự hiện diện lâu dài trong hệ thống mục tiêu. Sau khi hoàn thành mục tiêu ban đầu, đối tượng APT thường không rút lui hoàn toàn mà thiết lập các cơ chế để duy trì quyền truy cập vào mạng mục tiêu trong tương lai.

Để đạt được điều này, đối tượng APT triển khai nhiều backdoor dự phòng và các cơ chế kiên trì (persistence mechanisms) tinh vi trong hệ thống. Các cơ chế này có thể bao gồm việc sửa đổi registry Windows, tạo các scheduled tasks ẩn, cài đặt malware vào firmware hoặc BIOS của thiết bị, hoặc tận dụng các dịch vụ hệ thống hợp pháp để tự động khởi động lại malware sau khi khởi động lại hệ thống.

Đối tượng APT cũng thường xuyên cập nhật và thay đổi công cụ, kỹ thuật và quy trình (TTPs) để thích ứng với các biện pháp phòng thủ mới được triển khai. Điều này tạo ra một cuộc chiến liên tục giữa đối tượng tấn công và đội ngũ phòng thủ, trong đó đối tượng APT liên tục tìm kiếm các lỗ hổng mới và điều chỉnh chiến thuật để duy trì quyền truy cập vào hệ thống mục tiêu trong thời gian dài, có thể kéo dài từ nhiều tháng đến nhiều năm.

* 1. **Hậu quả của các cuộc tấn công**

Các cuộc tấn công APT có thể gây ra hậu quả nghiêm trọng và đa chiều cho tổ chức bị nhắm mục tiêu. Những tác động này không chỉ giới hạn ở mất mát tài chính ngắn hạn mà còn có thể ảnh hưởng sâu sắc đến hoạt động dài hạn, danh tiếng và khả năng cạnh tranh của tổ chức.

**Thiệt hại tài chính trực tiếp** là hậu quả dễ nhận thấy nhất của các cuộc tấn công APT thành công. Chi phí điều tra và khắc phục sự cố thường rất lớn, đặc biệt khi xét đến tính chất phức tạp và phạm vi rộng của các cuộc tấn công APT. Tổ chức phải đầu tư vào các dịch vụ điều tra pháp y số chuyên nghiệp, thuê các chuyên gia bảo mật để phân tích phạm vi xâm nhập, và triển khai các biện pháp khắc phục toàn diện trên toàn bộ cơ sở hạ tầng CNTT. Ngoài ra, các cuộc tấn công APT thường gây ra gián đoạn hoạt động kinh doanh đáng kể, dẫn đến mất doanh thu trong thời gian hệ thống bị ảnh hưởng. Trong nhiều trường hợp, tổ chức còn phải đối mặt với các khoản phạt pháp lý đáng kể do vi phạm các quy định về bảo vệ dữ liệu và quyền riêng tư, đặc biệt khi dữ liệu cá nhân của khách hàng bị xâm phạm.

**Thiệt hại về tài sản trí tuệ** có thể có tác động sâu sắc và lâu dài đến vị thế cạnh tranh của tổ chức. Khi bí quyết công nghệ, kết quả nghiên cứu phát triển, thiết kế sản phẩm, hoặc các thông tin độc quyền khác bị đánh cắp, tổ chức có thể mất đi lợi thế cạnh tranh quan trọng trên thị trường. Điều này đặc biệt nghiêm trọng trong các ngành công nghiệp sáng tạo hoặc công nghệ cao, nơi việc đi đầu về công nghệ là yếu tố quyết định thành công. Trong một số trường hợp, thông tin bị đánh cắp có thể được sử dụng để sao chép sản phẩm, đánh cắp thị phần, hoặc vô hiệu hóa các chiến lược kinh doanh của tổ chức bị tấn công.

**Thiệt hại về danh tiếng** thường là một trong những hậu quả nghiêm trọng nhất của các cuộc tấn công APT, đặc biệt khi thông tin về vụ việc được công bố rộng rãi. Tổ chức có thể phải đối mặt với sự mất niềm tin đáng kể từ khách hàng, đối tác kinh doanh, và các bên liên quan khác, dẫn đến mất khách hàng, hủy hợp đồng, hoặc gián đoạn trong các mối quan hệ kinh doanh quan trọng. Cổ đông và nhà đầu tư cũng có thể phản ứng tiêu cực, dẫn đến giảm giá cổ phiếu và mất giá trị thị trường. Ngoài ra, tổ chức còn gặp khó khăn trong việc thu hút và giữ chân nhân tài, đặc biệt là các chuyên gia CNTT và bảo mật, những người có thể lo ngại về môi trường làm việc không an toàn.

**Rủi ro pháp lý và quy định** ngày càng trở nên nghiêm trọng hơn khi các quy định về bảo vệ dữ liệu và an ninh mạng ngày càng chặt chẽ trên toàn cầu. Các cuộc tấn công APT dẫn đến vi phạm dữ liệu có thể khiến tổ chức phải đối mặt với các cuộc điều tra pháp lý, các khoản phạt hành chính đáng kể, và thậm chí là các vụ kiện tập thể từ các cá nhân bị ảnh hưởng. Các quy định như GDPR ở Châu Âu, CCPA ở California, và nhiều luật tương tự khác trên toàn cầu yêu cầu các tổ chức phải thông báo cho các cơ quan quản lý và cá nhân bị ảnh hưởng về các vụ vi phạm dữ liệu, đồng thời tuân thủ các tiêu chuẩn nghiêm ngặt về bảo vệ dữ liệu. Việc không tuân thủ các quy định này có thể dẫn đến các khoản phạt lên đến hàng triệu đô la.

**Rủi ro an ninh quốc gia** là mối quan tâm đặc biệt khi các cuộc tấn công APT nhắm vào các cơ quan chính phủ, tổ chức quốc phòng, hoặc cơ sở hạ tầng trọng yếu. Việc lộ thông tin mật liên quan đến quốc phòng hoặc an ninh quốc gia có thể gây ra những hậu quả nghiêm trọng cho an ninh quốc gia và lợi ích chiến lược của một quốc gia. Các cuộc tấn công nhắm vào cơ sở hạ tầng quan trọng như lưới điện, hệ thống cung cấp nước, hoặc mạng lưới giao thông có thể gây ra gián đoạn nghiêm trọng cho các dịch vụ thiết yếu, đe dọa đến sự an toàn và phúc lợi của người dân. Trong bối cảnh địa chính trị căng thẳng, các cuộc tấn công APT còn có thể góp phần làm leo thang căng thẳng giữa các quốc gia và thậm chí dẫn đến các cuộc xung đột ngoại giao hoặc kinh tế.

* 1. **Mối liên hệ giữa APT và tiêu chuẩn ISO/IEC 27001**

Tiêu chuẩn ISO/IEC 27001 cung cấp một khung quản lý an ninh thông tin toàn diện có thể được áp dụng để đối phó hiệu quả với các mối đe dọa APT. Mối liên hệ giữa APT và ISO/IEC 27001 thể hiện rõ qua việc tiêu chuẩn này giải quyết trực tiếp nhiều điểm yếu mà APT thường khai thác.

Tiêu chuẩn ISO/IEC 27001 với phương pháp tiếp cận dựa trên rủi ro yêu cầu tổ chức phải thực hiện đánh giá rủi ro an ninh thông tin một cách thường xuyên và có hệ thống. Quy trình này đặc biệt quan trọng trong việc xác định các mối đe dọa APT tiềm tàng, đánh giá điểm yếu có thể bị khai thác và đo lường tác động tiềm tàng đối với tổ chức. Thông qua việc áp dụng phương pháp đánh giá rủi ro được chuẩn hóa, tổ chức có thể xác định các tài sản thông tin quan trọng nhất—chính là những mục tiêu hàng đầu mà các nhóm APT thường nhắm đến.

Khi phân tích các yêu cầu của ISO/IEC 27001 trong bối cảnh phòng chống APT, chúng ta thấy rằng các biện pháp kiểm soát được đề xuất trong Phụ lục A của tiêu chuẩn giải quyết trực tiếp nhiều khía cạnh của vòng đời tấn công APT. Ví dụ, các biện pháp kiểm soát liên quan đến quản lý tài sản (A.8) giúp tổ chức hiểu rõ các tài sản cần được bảo vệ, trong khi các biện pháp kiểm soát truy cập (A.9) giúp giảm thiểu khả năng di chuyển ngang của kẻ tấn công trong môi trường nội bộ.

Đặc biệt, phiên bản ISO/IEC 27001:2022 đã tăng cường tập trung vào các khía cạnh quan trọng để phòng chống APT hiệu quả hơn. Tiêu chuẩn mới nhấn mạnh vào việc giám sát liên tục và phát hiện sự cố sớm—đây là yếu tố then chốt để ngăn chặn các cuộc tấn công APT phát triển qua các giai đoạn của chúng. Thêm vào đó, tiêu chuẩn đề cao tầm quan trọng của việc quản lý nhà cung cấp, nhằm giảm thiểu rủi ro bị tấn công thông qua chuỗi cung ứng—một vector tấn công ngày càng phổ biến được sử dụng bởi các nhóm APT tinh vi.

Việc áp dụng ISO/IEC 27001 cung cấp cho tổ chức một cấu trúc quản lý an ninh thông tin có khả năng thích ứng cao, cho phép họ phản ứng nhanh chóng với các chiến thuật tấn công ngày càng phát triển. Thông qua việc thực hiện các quy trình cải tiến liên tục như được quy định trong tiêu chuẩn, tổ chức có thể liên tục nâng cao khả năng phòng thủ của mình để đối phó với các kỹ thuật APT mới nổi.

Tuy nhiên, điều quan trọng cần lưu ý là việc tuân thủ ISO/IEC 27001 không đảm bảo khả năng miễn nhiễm hoàn toàn với các cuộc tấn công APT. Thay vào đó, tiêu chuẩn cung cấp một nền tảng vững chắc để xây dựng chiến lược phòng thủ nhiều lớp, tăng cường khả năng phát hiện sớm các hoạt động độc hại và cải thiện năng lực phản ứng khi sự cố xảy ra. Khi được tích hợp vào một chiến lược an ninh mạng toàn diện, ISO/IEC 27001 trở thành một công cụ quan trọng trong cuộc chiến chống lại các mối đe dọa APT ngày càng phức tạp.

1. **Các giải pháp phòng chống tấn công APT**

Để đối phó hiệu quả với mối đe dọa APT ngày càng gia tăng, tổ chức cần xây dựng và triển khai chiến lược phòng thủ toàn diện, áp dụng phương pháp phòng thủ theo chiều sâu (defense-in-depth) kết hợp với khả năng phát hiện và ứng phó nhanh chóng. Các giải pháp phòng chống APT hiệu quả bao gồm nhiều lớp bảo vệ, từ các biện pháp phòng ngừa đến phát hiện và ứng phó.

**Các biện pháp phòng ngừa** là lớp bảo vệ đầu tiên chống lại các cuộc tấn công APT. Đào tạo nhận thức an ninh mạng chuyên sâu cho nhân viên là một trong những biện pháp phòng ngừa hiệu quả nhất, giúp nhân viên nhận biết và tránh các chiến thuật kỹ thuật xã hội phổ biến như spear phishing. Chương trình đào tạo nên bao gồm các tình huống thực tế, mô phỏng các cuộc tấn công, và cập nhật thường xuyên về các chiến thuật tấn công mới nổi.

Bên cạnh đó, tổ chức cần triển khai các chính sách bảo mật mạnh mẽ và cập nhật thường xuyên, bao gồm chính sách quản lý mật khẩu, kiểm soát truy cập, quản lý bản vá, và sử dụng thiết bị cá nhân. Việc áp dụng nguyên tắc đặc quyền tối thiểu (principle of least privilege) giúp giảm thiểu phạm vi ảnh hưởng khi một tài khoản bị xâm phạm, trong khi phân đoạn mạng (network segmentation) ngăn chặn hoặc hạn chế khả năng di chuyển ngang của kẻ tấn công trong mạng.

Ngoài ra, tổ chức cũng nên áp dụng các biện pháp kỹ thuật như mã hóa dữ liệu nhạy cảm, triển khai hệ thống quản lý bản vá tự động, và sử dụng các giải pháp bảo mật như tường lửa thế hệ mới (NGFW), hệ thống phòng chống xâm nhập (IPS), và các giải pháp bảo mật điểm cuối tiên tiến.

**Các biện pháp phát hiện** là lớp bảo vệ thứ hai, giúp phát hiện các cuộc tấn công APT khi chúng đã vượt qua lớp phòng ngừa. Các tổ chức nên triển khai các hệ thống phát hiện xâm nhập (IDS) và phòng chống xâm nhập (IPS) tiên tiến có khả năng phát hiện các hành vi bất thường và dấu hiệu của các cuộc tấn công APT. Các giải pháp EDR (Endpoint Detection and Response) và XDR (Extended Detection and Response) cung cấp khả năng giám sát và phân tích hành vi của các thiết bị đầu cuối, phát hiện các dấu hiệu xâm nhập trên từng thiết bị.

Phân tích hành vi người dùng và hệ thống (UEBA) là một công nghệ quan trọng khác, sử dụng học máy và phân tích dữ liệu lớn để phát hiện các mẫu hành vi bất thường có thể chỉ ra sự hiện diện của kẻ tấn công. Theo dõi và phân tích liên tục các sự kiện bảo mật thông qua các giải pháp SIEM (Security Information and Event Management) giúp tổ chức phát hiện các mối đe dọa tiềm ẩn bằng cách tổng hợp và phân tích dữ liệu từ nhiều nguồn khác nhau.

Ngoài ra, các tổ chức nên triển khai các hoạt động threat hunting chủ động, trong đó các chuyên gia an ninh mạng chủ động tìm kiếm dấu hiệu xâm nhập trong mạng mà có thể không được phát hiện bởi các hệ thống tự động.

**Các biện pháp ứng phó** là lớp bảo vệ thứ ba, được kích hoạt khi một cuộc tấn công APT đã được phát hiện. Để ứng phó hiệu quả, tổ chức cần phát triển kế hoạch ứng phó sự cố chi tiết, xác định rõ vai trò và trách nhiệm của từng cá nhân, quy trình thông báo, và các bước ứng phó cụ thể cho từng loại sự cố. Thành lập đội ứng cứu sự cố

* 1. **Triển khai Honeypot để bẫy và giám sát hành vi APT**

**Mục đích:**

Honeypot là một cái "bẫy" giả vờ đóng vai một dịch vụ thật (như SSH, Web Server, GitLab, Mail...) nhưng mục tiêu là để dụ hacker tấn công vào.  
→ Khi hacker tưởng là dịch vụ thật và cố gắng khai thác, mình sẽ ghi lại mọi hành động của họ: brute-force password, exploit lỗ hổng, upload file độc hại, chiếm quyền...

**Dữ liệu mình thu được** sẽ giúp:

* Phát hiện ai đang tấn công mình (IP, kỹ thuật, công cụ, lệnh...).
* Biết chúng đang tìm kiếm cái gì (repo GitLab, file nhạy cảm, cổng backdoor...).
* Có bằng chứng (log) để phản ứng hoặc phân tích sâu hơn (threat hunting).

**Giải pháp triển khai:**

* + Dùng T-Pot CE (community edition) hoặc Cowrie để dựng một máy honeypot riêng biệt.
  + Đặt honeypot trong vùng DMZ của OPNsense hoặc tạo VLAN riêng.
  + OPNsense cấu hình port forwarding hoặc NAT policy để đưa lưu lượng từ internet hoặc mạng LAN lạ vào honeypot.

**Lợi ích:**

Phát hiện sớm hành vi bất thường mà IDS hoặc endpoint chưa thấy.

Honeypot không chứa dữ liệu thật → không sợ bị thiệt hại nếu bị chiếm.

* 1. **Tăng cường bảo vệ điểm cuối bằng EDR (Endpoint Detection and Response)**

**Mục đích:**

Phát hiện và theo dõi hành vi bất thường ở cấp độ máy trạm, máy chủ, và container.

Ngăn chặn giai đoạn implant malware trong chuỗi tấn công APT.

**Giải pháp triển khai:**

**a) Wazuh**

Cài Wazuh Agent trên các máy chủ và endpoint quan trọng (như máy chạy GitLab).

Triển khai Wazuh Server riêng hoặc tích hợp vào SIEM nếu có sẵn.

Cấu hình gửi alert từ Wazuh về hệ thống Grafana thông qua Wazuh API + Prometheus Exporter hoặc syslog.

Tích hợp vào OPNsense nếu bật chức năng syslog receiver (giám sát alert tập trung).

**b) Falco**

Cài Falco trên các server Linux, đặc biệt là server có chạy container (Docker, Kubernetes).

Falco sẽ giám sát hành vi runtime như: khởi chạy process bất thường, truy cập file nhạy cảm, hoặc mở kết nối mạng lạ.

Log cảnh báo Falco có thể đưa vào Grafana qua Falco Exporter hoặc qua syslog → Grafana hiển thị dashboard cảnh báo real-time.

Falco cực kỳ nhẹ, phù hợp bảo vệ GitLab server mà không làm nặng hệ thống.

Gợi ý triển khai cụ thể:

Nếu hệ thống của bạn đã có Grafana và OPNsense, nên:

* Wazuh chuyên phân tích log sâu, timeline tấn công.
* Falco chuyên phát hiện hành vi runtime bất thường real-time.

Cả 2 gửi alert về OPNsense và Grafana để tập trung giám sát toàn bộ mạng lưới và server.

Liên hệ với ISO/IEC 27001:2022

Theo ISO/IEC 27001:2022, các biện pháp kiểm soát an ninh thông tin liên quan gồm:

A.8.16 Monitoring activities (Theo dõi hoạt động): Yêu cầu theo dõi việc truy cập và hành vi trong hệ thống thông tin để phát hiện các hành vi trái phép hoặc bất thường. Việc triển khai EDR (như Wazuh, Falco) giúp đáp ứng yêu cầu này bằng cách liên tục giám sát và phát hiện các sự kiện nghi ngờ.

A.5.23 Information security for use of cloud services (An toàn thông tin cho các dịch vụ đám mây): Falco giám sát container và môi trường cloud runtime giúp kiểm soát rủi ro trong môi trường cloud hoặc hybrid cloud.

A.5.7 Threat intelligence (Tình báo mối đe dọa): Phân tích hành vi từ EDR góp phần xây dựng cơ sở dữ liệu về các mối đe dọa, phục vụ cảnh báo sớm cho tổ chức.

Triển khai các giải pháp EDR như Wazuh và Falco không chỉ tăng cường khả năng bảo vệ thực tế trước APT mà còn hỗ trợ tổ chức tuân thủ các yêu cầu giám sát, phát hiện, phân tích mối đe dọa theo tiêu chuẩn ISO/IEC 27001:2022.

* 1. **Kết hợp IDS/IPS OPNsense với Threat Hunting**

**Mục đích:** Không chỉ chờ cảnh báo, mà chủ động săn lùng APT dựa trên IOC, hành vi traffic bất thường và mối đe dọa tiềm ẩn.

**Giải pháp triển khai:**

**a) Cập nhật và mở rộng Suricata RuleSet**

OPNsense đã tích hợp Suricata (IDS/IPS).

Thực hiện cập nhật thêm ruleset chuyên về threat hunting:

* ET Pro Ruleset (Emerging Threats Professional) – phát hiện mối đe dọa APT phức tạp.
* Custom rules tự viết dựa trên: IOC thu thập từ honeypot (như Cowrie, Dionaea...); Threat intelligence feeds.

**b) Tự động hóa phản ứng nhanh**

Khi honeypot phát hiện IP/mẫu tấn công lạ:

* Tự động tạo rule Suricata chặn IP hoặc pattern tương ứng.
* Có thể bổ sung blocklist trực tiếp vào Firewall Alias của OPNsense.

**c) Phân tích sâu traffic khả nghi bằng Zeek**

Nếu cần mức độ chi tiết cao hơn:

* Tích hợp thêm Zeek (Bro) làm network traffic analyzer.
* Zeek giúp phân tích file download, HTTP request/response, DNS query... để tìm hành vi APT ẩn.

Liên hệ với ISO/IEC 27001:2022

A.8.7 Threat intelligence: (Yêu cầu phải thu thập, phân tích và xử lý thông tin về mối đe dọa để bảo vệ tổ chức.)

A.8.16 Monitoring activities: (Theo dõi liên tục để phát hiện hoạt động bất thường.)

A.5.25 Management of technical vulnerabilities: (Quản lý lỗ hổng kỹ thuật thông qua giám sát và cập nhật liên tục.)

Việc triển khai Threat Hunting theo mô hình này hỗ trợ tổ chức phát hiện, phản ứng sớm với các tấn công APT, và tuân thủ các yêu cầu bắt buộc trong tiêu chuẩn ISO/IEC 27001:2022.

* 1. **Đào tạo nhận thức và xây dựng quy trình ứng phó sự cố**

Trong bối cảnh các cuộc tấn công APT ngày càng tinh vi và nhắm vào yếu tố con người, việc chỉ đầu tư vào công nghệ phòng thủ là chưa đủ. Một thành phần then chốt để bảo vệ tổ chức chính là nâng cao nhận thức an ninh cho nhân sự và xây dựng quy trình ứng phó sự cố (Incident Response Plan – IRP) bài bản.

Mục tiêu của đào tạo nhận thức an ninh là giảm thiểu nguy cơ thành công của các hình thức tấn công như spear phishing, đánh cắp thông tin đăng nhập (credential theft) hoặc các thủ đoạn lừa đảo xã hội khác. Các chương trình đào tạo cần tập trung vào việc giúp nhân viên nhận biết các dấu hiệu đáng ngờ từ email, file đính kèm, liên kết lạ hoặc những hành vi bất thường trong môi trường làm việc hàng ngày. Đào tạo không chỉ mang tính lý thuyết mà nên đi kèm các buổi diễn tập giả lập tình huống tấn công (phishing simulation) nhằm củng cố kỹ năng nhận diện thực tế.

Bên cạnh đó, việc xây dựng và thực thi một kế hoạch ứng phó sự cố (IRP) rõ ràng là yêu cầu bắt buộc để tổ chức có thể phản ứng kịp thời khi APT xâm nhập. Kế hoạch cần quy định rõ vai trò, trách nhiệm của từng bộ phận, các kịch bản xử lý theo cấp độ sự cố, và quy trình thông báo nội bộ cũng như với các cơ quan chức năng khi cần thiết.

Về mặt kỹ thuật, hệ thống mạng cần hỗ trợ các hành động phản ứng nhanh như: chặn ngay lập tức các IP hoặc domain nghi vấn tại lớp firewall, cô lập các thiết bị nghi nhiễm thông qua phân đoạn mạng VLAN hoặc áp dụng captive portal để kiểm soát truy cập tạm thời. Các nền tảng firewall thế hệ mới như OPNsense, pfSense hoặc FortiGate có thể đóng vai trò trung tâm kiểm soát trong quá trình này, giúp nhanh chóng thực hiện các biện pháp khoanh vùng, ngăn chặn lây lan sự cố trên diện rộng.

Ngoài ra, việc tổ chức diễn tập ứng phó sự cố định kỳ (tabletop exercise, live incident drill) cũng là một yếu tố quan trọng để đảm bảo kế hoạch IRP không chỉ tồn tại trên lý thuyết mà thực sự khả thi khi sự cố xảy ra.

Tất cả các hoạt động đào tạo và quy trình ứng phó sự cố này đều đáp ứng các yêu cầu của tiêu chuẩn ISO/IEC 27001:2022, đặc biệt là các điều khoản liên quan đến "Information Security Awareness, Education and Training" (A.6.3) và "Information Security Incident Management" (A.5.24, A.5.25, A.5.26). Điều này không chỉ giúp tổ chức tăng cường khả năng tự vệ trước APT mà còn hỗ trợ đạt được sự tuân thủ quốc tế về an toàn thông tin.

# TÀI LIỆU THAM KHẢO

Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT. (2025, 4 26). Retrieved from https://www.hpt.vn/tin-tuc/thach-thuc-an-ninh-mang-cua-doanh-nghiep-trong-ky-nguyen-so-2025/12648

Management of enterprise cyber security: A review of ISO/IEC 27001: 2022 https://ieeexplore.ieee.org/abstract/document/10051114/

Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013 https://www.journal.fkpt.org/index.php/BIT/article/view/421

ISO/IEC 27001: 2022: An introduction to information security and the ISMS standard https://www.torrossa.com/gs/resourceProxy?an=5751061&publisher=FZO328

Chứng nhận ISO 27001 Hệ thống quản lý an toàn thông tin

https://chungnhanquocgia.com/iso-27001

# PHỤ LỤC