# Bài: 1.7 Giới thiệu về Ethical Hacking - Bảo mật vật lý & Quản lý sự cố

*Xem bài học trên website để ủng hộ Kteam: 1.7 Giới thiệu về Ethical Hacking - Bảo mật vật lý & Quản lý sự cố*

*Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!*

## Physical Security (Bảo mật vật lý)

**Physical Security (Bảo mật vật lý)** luôn luôn được ưu tiên sử dụng trong bảo mật bất kỳ thứ gì. Trong bảo mật thông tin, **physical security** cũng được coi là lớp bảo vệ đầu tiên vô cùng quan trọng. **Physical security** bao gồm bảo vệ khỏi các cuộc tấn công xâm nhập do con người thực hiện như trộm cắp, đánh đập, đột nhập trái phép cũng như các yếu tố tự nhiên như mưa, bụi, mất điện, lửa,...

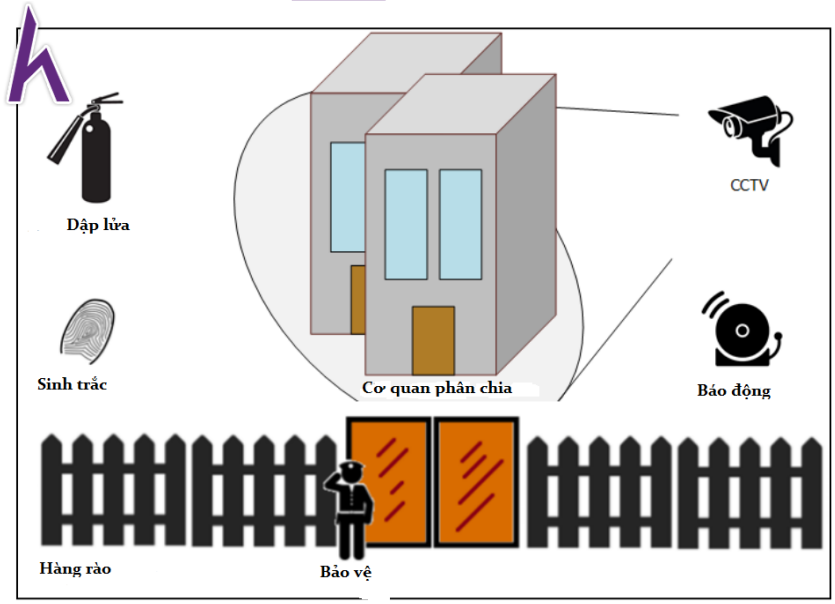


*Figure 1-12 Physical Security*

Bảo mật vật lí phải đảm bảo ngăn chặn việc trộm cắp, giả mạo, làm hư hỏng, ăn trộm và nhiều kiểu tấn công vật lí khác. Hệ thống hàng rào, bảo vệ, CCTV camera, hệ thống phát hiện đột nhập, chuông báo động trộm, làm cản trở để bảo vệ những thứ đáng giá.

Những tài liệu quan trọng không nên được đặt ở những khu vực không an toàn ngay cả khi đang ở trong tổ chức hoặc đã được khóa lại, chỉ nên ở trong quyền kiểm soát của người được ủy quyền.

Khu vực vận hành phải được cách li để bảo vệ. Việc giám sát nghe trộm, thiết bị máy tính, hệ thống chống cháy cũng nên được đảm bảo diễn ra liên tục và thường xuyên.

---

## Incident Management (Quản lý sự cố)

**Incident Management (Quản lý sự cố)** là cách thức, quá trình điều chỉnh, xử lý khi có sự cố xảy ra. Sự cố có thể là bất cứ sự chống đối rõ ràng nào đối với các điều kiện, điều lệ, .... Tương tự, trong an toàn thông tin, việc phản hồi sự cố những việc được thực hiện nhằm phản ứng lại các trường hợp, các mối đe dọa hoặc các cuộc tấn công và tiến tới loại bỏ ( khi hệ thống đã an toàn, ổn định, thực hiện các chức năng)

**Quản lí ứng cứu sự cố** xác định vai trò, trách nhiệm của những **pentester**, người dùng hoặc nhân viên của tổ chức. Thêm vào đó, quản lí ứng cứu sự cố định rõ những gì cần làm khi hệ thống đang đối mặt với các mối đe dọa đến tính nguyên vẹn, tính bảo mật, tính xác thực và tính sẵn sàng của nó tùy theo mức độ nguy hiểm.

Ban đầu, cần nhớ khi một hê thống đang chống chọi với các mối nguy hiểm, điều cần thiết là sự sửa chữa tinh vi, phức tạp đến từ các chuyên gia. Trong quá trình ứng cứu sự cố, chuyên gia sẽ thu thập bằng chứng, thông tin và dấu vết hữu ích cho việc bảo vệ trong tương lai, theo dấu kẻ tấn công, tìm kiếm lỗ hổng cùng điểm yếu trong hệ thống.

Quy trình quản lý sự cố:

1. Chuẩn bị cho ứng cứu sự cố
2. Dò tìm và phân tích ứng cứu sự cố
3. Phân loại sự cố và sắp xếp giải quyết theo mức độ ưu tiên
4. Thông báo và công bố
5. Chính sách ngăn chặn
6. điều tra giám định sự cố
7. Loại bỏ và sửa chữa
8. Các hoạt động sau sự cố.

## Trách nhiệm của đội ngũ ứng cứu sự cố

**Đội ngũ ứng cứu** sự cố bao gồm những thành viên có ý thức sâu sắc về việc đối mặt với sự cố. Đội ngũ ứng cứu này là tập hợp của những chuyên gia được đào tạo chính thức trong việc thu thập thông tin và bảo vệ chứng cứ của một cuộc tấn công từ hệ thống sự cố. Đội ngũ này có sự tham gia của nhân viên IP, HR, cơ quan quan hệ công chúng, ban hỗ trợ tư pháp, cơ quan an ninh đầu não

- Trách nhiệm cơ bản của đội ngũ này là **thực hiện những hành động theo kế hoạch ứng cứu sự cố** (**Incident Response Plan-IRP**). Nếu không xác định được IRP, hoặc không thể áp dụng IRP trong trường hợp đó, tổ ứng cứu phải theo sát người đứng đầu kiểm tra để hợp sức giải quyết.
- Kiểm tra và định lượng tình huống, xác định hư hại hoặc phạm vi của cuộc tấn công.
- Thu thập tài liệu
- Nếu cần, nhờ tới sự trợ giúp của chuyên gia bảo mật hoặc cố vấn
- Nếu cần, nhờ tới sự trợ giúp của ban hỗ trợ tư pháp địa phương
- Sưu tập sự việc.
- Báo cáo.

**Mindmap**