Bài: 1.5 Giới thiệu về Ethical Hacking - Kiểm soát an toàn thông tin

Xem bài học trên website để ủng hộ Kteam: 1.5 Giới thiệu về Ethical Hacking - Kiểm soát an toàn thông tin

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!

Kiểm soát an toàn thông tin

Sự đảm bảo thông tin (Information Assuarance – IA)

Information assuarance – nói ngắn gọn là **IA**, phụ thuộc vào những nhân tố **tính nguyên vẹn** (Integrity), **tính khả dụng** (Availability) và **tính xác thực** (Authenticity). Bằng sự kết hợp của các nhân tố này, sự đảm bảo thông tin và hệ thống thông tin được đảm bảo và bảo vệ trong thời gian sử dụng, trưng bày và giao tiếp. để biết rõ hơn về các nhân tố này, bạn hãy xem những chương tiếp theo.

Ngoại trừ các yếu tố đã nêu, có một vài phương thức và cách thức cũng góp sức giúp việc đảm bảo thông tin được thành công như:

- Các điều khoản và cách thức (Policies and Process)
- Xác thực mạng (Network authenticity)
- Xác thực người dùng (User Authentication)
- Điểm yếu của mang máy tính (NetworkVulnerabilities)
- Nhận dạng vấn đề và các loại tài nguyên (Identifying problems and resources)
- Những kế hoạch được thực thi cho yêu cầu nhận dạng (Implementation of plan for identified requiments)
- Điều khiển đảm bảo thiết bị thông tin (Application of information assuarance control)

Chương trình quản lý bảo mật thông tin

Chương trình quản lý bảo mật thông tin là những chương trình được đặc biệt thiết kế nhằm tập trung vào việc làm giảm những mối nguy hại và những tổn thương đến hệ thống bảo mật thông tin nhằm giúp tổ chức, người dùng có thể làm việc ở một môi trường an toàn hơn. Chương trình quản lý bảo mật thông tin là giải pháp quản trị kết hợp nhằm đạt được mức độ bảo mật an toàn với những điều lệ, những cách thức, báo cáo, cách quản lý và tiêu chuẩn được công nhận. Hãy xem biểu đồ trên trang kế tiếp để thấy được cách **EC-Council** định nghĩa Chương trình quản lí bảo mật thông tin.

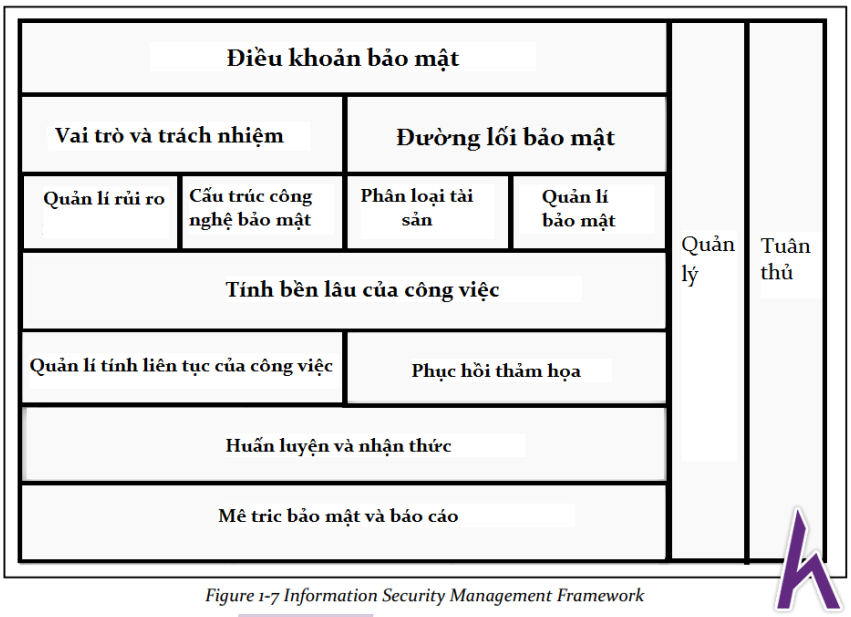


Figure 1-7 Information Security Management Framework

Mối đe dọa mẫu

Đây là quá trình giải quyết hoặc tiếp cận để nhận dạng, chẩn đoán và hỗ trợ cho các yếu điểm trên hệ thống, là bước tiếp cận đến việc quản lý các mối nguy hiểm, những thứ tập trung vào phân tích bảo mật hệ thống nhằm tiêu diệt những công cụ bảo mật. đặc điểm này của các mối đe dọa giúp chúng ta chú ý đưa ra hành động trước mỗi sự kiện để những điều ta muốn thành hiện thực

Nắm bắt dữ liệu của tổ chức, thực hiện quy trình nhận dạng, đánh giá qua những thông tin được kiểm soát để phân tích những thông tin khác - những thông tin có thể ảnh hưởng tới sự an toàn của thiết bị. Tổng quan về chương trình ứng dụng bao gồm bước nhận dạng với mục đích xác nhận giới hạn độ tin cậy và "dòng chảy" của dữ liệu. Sự phân tích một ứng dụng và nhận dạng mối nguy hiểm giúp ta có một "review" đầy đủ chi tiết hơn về chúng, về các đặc điểm của thứ đang đe dọa đến việc kiểm soát bảo mật. Bản review này cho ta biết mọi mặt của điểm yếu cũng như những thiếu sót của môi trường bảo mật.

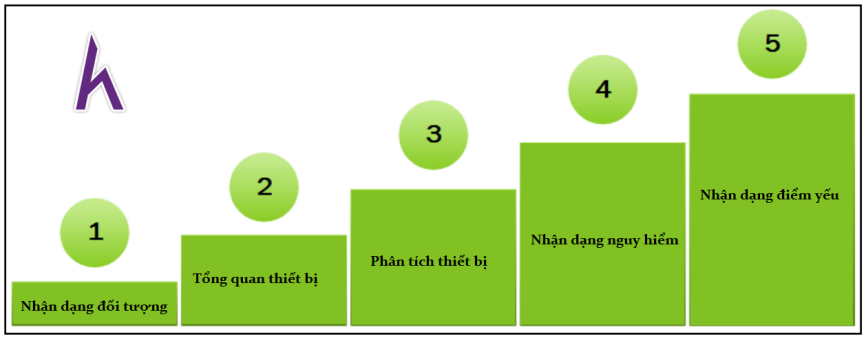
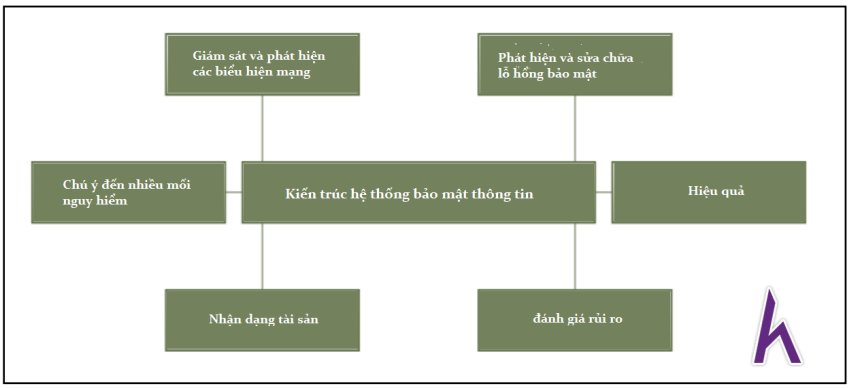


Figure 1-8 Threat Modelling

Enterprise Information Security Architecture (EISA)

Đây là sự kết hợp của yêu cầu và cách thức giúp chắc chắn, khảo sát, vận hành cấu trúc các biểu hiện của hệ thống thông tin. Dưới đây là mục tiêu của **EISA**:



Phân vùng bảo mật mạng

Quản lý, triển khai cấu trúc của một tổ chức trong những phân vùng khác nhau gọi là **Network security zoning**. Những vùng bảo mật này là bộ các mạng với mức độ bảo mật đặc biệt. Mỗi vùng bảo mật khác nhau có thể có mức độ bảo mật giống và khác nhau. Việc xác định mỗi vùng với mức độ bảo mật của chúng giúp ta điều khiển "đường đi" (inboard) lẫn "đường về" (outboard) qua hệ thống mạng.

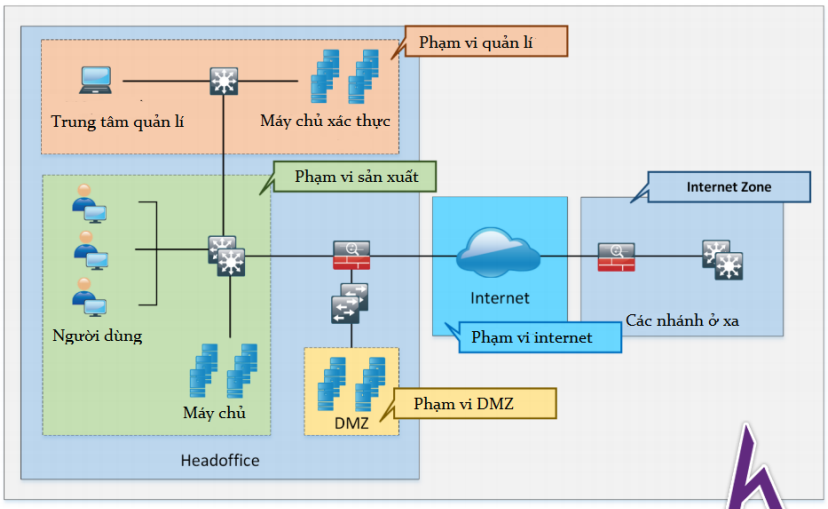


Figure 1-10 Network Security Zoning

Điều khoản bảo mật thông tin

Information Securiry Policies là yếu tố cơ bản và độc lập nhất của hệ thống bảo mật thông tin. Những yêu cầu bảo mật, những điều kiện, những luật lệ cơ bản được định ra một cách bắt buộc trong luật lệ bảo mật an toàn thông tin nhằm bảo vệ tài nguyên của tổ chức. Những điều lệ này bao phủ những nét bên ngoài của bộ máy quản lý, việc cai quản, yêu cầu bảo mật trong một kiến trúc bảo mật thông tin.

Figure 1-11 Steps to enforce Information Security

Mục tiêu cơ bản của luật an toàn thông tin là:

- Bao gồm yêu cầu bảo mật và điều kiện của tổ chức
- Bảo vệ tài nguyên của tổ chức
- Loại bỏ trách nhiệm pháp lý
- Hạn chế lãng phí tài nguyên
- Bảo vệ khỏi truy cập không được cấp phép
- Giảm bớt nguy hiểm
- Bảo đảm thông tin