Quản lý an toàn thông tin

* Quản lý
* Lập kế hoạch
* Tổ chức
* Chỉ đạo
* Điều chỉnh
* Kiểm soát

Quản lý an toàn thông tin:

* Là các hành động lên các đối tượng tham gia đối với hệ thống thông tin của một cơ quan tổ chức, nhằm đảm bảo tính bí mật, toàn vẹn, tính sẵn sàng của hệ thống thông tin của cơ quan, tổ chức

Hệ thống quản lý an toàn thông tin

ISMS là phương tiện quản lý cấp cao nhằm quản lý và kiểm soát mức độ an toàn, giảm thiểu tối đa các rủi ro và đảm bảo mức độ an toàn tiếp tục đáp ứng được yêu cầu của doanh nghiệp, khách hàng, pháp luật.

Hiểm hoạ, điểm yếu, rủi ro

3 khái niệm quan trọng cần hiểu để quản lý an toàn thông tin:

Hiểm hoạ (Threat)

Điểm yếu (Vulnerability)

Rủi ro (Risk)

RISK = f(Asset,Threat,Vuln)

Chính sách an toàn thông tin

Là tập hợp những chỉ thị và hướng dẫn về ATTT

Là tập hợp các điều luật, các quy định bảo đảm sự bảo vệ có hiệu quả các hệ thống xử lý thông tin chống lại các hiểm hoạ ATTT

Là tập hợp các điều luật, các quy định và các giải pháp thực tế để giám sát sự điều khiển, sự bảo vệ và việc phân phối các thông tin nhạy cảm trong hệ thống. (“Sách da cam” - 1983)

* Thể hiện ý chí và quyết tâm của các cấp lãnh đạo đối với việc bảo vệ HTTT, bao gồm đầy đủ các yếu tố thông tin, hạ tầng thông tin (phần cứng, phần mềm, mạng và các hệ thống khác,…) và các ứng dụng.

Các hiểm hoạ và các dạng tấn công

1. Hiểm họa ngẫu nhiên

Bảo vệ tài khoản không an toàn

Sử dụng các trang thiết bị không đúng cách

Đặt mật khẩu không an toàn

2. Trộm cắp

3. Rò rỉ thông tin

4. Lây nhiễm mã độc

5. Xâm nhập bất hợp pháp

Tấn công mạng máy tính

Tấn công từ Internet:

* Từ chối dịch vụ
* Phát tán mã độc qua lỗ hổng phần mềm
* Xâm nhập trái phép
* Chặn thu thông tin
* Lừa đảo trực tuyến

Nguyên tắc quản lý ATTT

Đại diện ban lãnh đạo ATTT (Giám đốc) là lãnh đạo cao nhất của tổ chức

Các lãnh đạo tổ chức cần nhận ra các rủi ro …

1. Tập trung vào khách hàng

2. Lãnh đạo

3. Sự tham gia của mọi người

4. Cách tiếp cân hệ. thống đối với quản lý

5. Cải tiến liên tục

6. Cách tiếp cận theo quy trình

7. Cách tiếp cận thực tế để ra quyết định

8. Các mối quan hệ nhà cung cấp cùng có lợi

Sáu chữ P:

Planning: lập kế hoạch

Policy: chính sách

Programs

Chương 2: Luật Pháp Việt Nam Trong Quản Lý An Toàn Thông Tin

Tầm quan trọng của luật pháp…

Phương pháp bảo vệ

Mã hoá

Quy chế

Cưỡng chế

Giáo dục

Vật lý

Phần cứng

Phần mềm

Tổ chức

Luật pháp

Ngăn cản

Đạo đức

Phương tiện bảo vệ

Kiểm soát truy cập

Tầm quan trọng của luật pháp///

Năng lực bên tấn công quá lớn?

Nhà cung cấp vì lợi nhuận mà sử

Chương 3: Quản ký và xây dựng kế hoạch chiến lược an toàn thông tin

Vai trò của việc xây dựng kế hoạch

* Lập kế hoạch là phương tiện chủ đạo để quản lý tài nguyên
* Đòi hỏi việc liệt kê một chuỗi các hành động nhằm đạt được các mục tiêu

Xây dựng kế hoạch chiến lược

Các thành phần cơ bản

1. Tóm tắt
2. Tuyên bố sứ mệnh, tầm nhìn và giá trị
3. Hồ sơ và lịch sử tổ chức
4. Các vấn đề và thách thức chiến lược
5. Mục tiêu của tổ chức
6. Mục tiêu của đơn vị kinh doanh chính
7. Phụ lục

Quản trị an toàn thông tin

* Là quá trình tạo và duy trì cấu trúc tổ chức quản lý chức năng ATTT trong 1 tổ chức
* 5 mục tiêu chính:
  + Điều chỉnh chiến lược ATTT và các mục tiêu kinh doanh
  + Sử dụng các phượng pháp quản lý rủi ro để hướng dẫn việc ra quyết định của ATTT
  + Thực hiện các thực hành quản lý tài nguyên tài nguyên hợp lý cho các chương trình ATTT
  + Đo lường hiệu suất của các chức năng ATTT
  + Mang lại giá trị cho tổ chức
* 4 thực hành cần thiết
  + Đặt ATTT vào Ctr làm việc của hội đồng quản trị
  + Xác định các nhà lãnh đạo ATTT, quy trách nhiệm cho họ và đảm bảo hỗ trợ họ
  + Đảm bảo tính hiệu quả của CSATTT của tổ chức thông qua việc xem xét và phê duyệt
  + Chỉ định ATTT cho một uỷ ban chính và đảm bảo hỗ trợ đầy đủ cho uỷ ban đó
* Lợi ích
  + Gia tăng giá trị cổ phiếu
  + Tăng khả năng dự đoán và giảm tính không chắc chắn của hoạt động
* Chương trình quản trị ATTT gồm:
  + Phương pháp quản lý rủi ro
  + Chiến lược AT toàn diện được liên kế rõ ràng với các mục tiêu kình doanh và CNTT
  + Cơ cấu tổ chức AT hiệu quả
  + Chiến lược AT nói về giá trị của thông tin được bảo vệ và cung cấp
  + Các CSAT giải quyết từng khía cạnh của chiến lược, kiểm soát và quy định
  + Bộ tiêu chuẩn AT hoàn chỉnh cho từng CS để đảm bảo rằng các thủ tục, hước dẫn tuân thủ CS
  + Các quy trình giám sát được thể chế hoá để đảm bảo tuân thủ và cung cấp phản hồi về tính hiệu quả và giảm thiểu rủi ro
  + Quy trình để đảm bảo tiếp tục đánh giá và cập nhật các CS, tiêu chuẩn, thủ tục và rủi ro AT

Xây dựng kế hoạch triển khai đảm bảo ATTT

* Việc triển khai ATTT được bắt đàu theo một trong hai cách: từ trên xuống và từ dưới lên

Trách nhiệm trong kế hoạch ATTT

* Giám đốc THông tin (CIO): chịu trách nhiệm phát triển và duy trì một chương trình ATTT toàn cơ quan
* Chủ sở hữu HTTT: chịu trách nhiệm về việc mua sắm, phát triển, tích hợp, sửa đổi tổng thể hoặc vận hành và bảo trì HTTT.
* Chủ sở hữu TT: có thẩm quyền theo luật định hoặc hoạt động đối với TT cụ thể và chịu trách nhiệm thiết lập các biện pháp kiểm soát đối với việc tạo ra, thu thập, xử lý, phổ biến, loại bỏ TT đó và có các trách nhiệm liên quan đến các kế hoạch ATTT.
* Cán bộ ATTT: chịu trách nhiệm là người liên lạc chính của CIO với chủ sở hữu HTTT của cơ quan và cán bộ AT HTTT
* Cán bộ uỷ quyền là quan chức quản lý cấp cao, hoặc nhà điều hành có thẩm quyền: chịu trách nhiệm vần hành HTTT
* Phê duyệt kế hoạch ATTT:
  + Cần xác định rõ ai chịu trách nhiệm phê duyệt kế hoạch ATTT và các thủ tục được phát triển

Phân loại hệ thống

KHẢ NĂNG TÁC ĐỘNG

Mục tiêu an toàn

Bí mật Duy trì các hạn chế được phép đối với quyền tryu cậpvà tiết lộ TT, gồm các phương tinrj để bảo vệ quyền riêng tư cá nhân và thông tin độc quyền

THẤP

Việc tiết lộ thông in

TRUNG BÌNH

CAO

Chủ sở hữu hệ thống