**Đồ án Quản lí rủi ro an toàn thông tin - POLICY**

***20522019 – Võ Thành Tín***

***20520454 – Trần Trí Đức***

***20521291 – Huỳnh Thế Hào***

***20521858 – Nguyễn Ngọc Tài***

* **Firewall + IPS:**
  + Quy trình cấu hình luật tường lửa:
    - Không có bất kỳ Rules nào Any Any
    - Việc cấu hình FW phải qua ít nhất 2 người, 1 user cấu hình và 1 user duyệt
    - Luật tường lửa phải được rà soát định kỳ
  + Quy trình quản lý truy cập hệ thống thông tin
    - User sử dụng VPN phải được sự phê duyệt của người có thẩm quyền
    - Truy cập VPN phải qua xác thực 2 lớp
    - Chỉ sử dụng VPN trong trường hợp khẩn cấp
    - Tuyệt đối không sử dụng các phần mềm điều khiển từ xa như Teamview…
  + Quy định về quản lý truy cập mạng công cộng
    - Nghiêm cấm truy cập các trang chia sẻ dữ liệu như Google Drive, Onedrive
    - Không sử dụng các mạng xã hội
    - Chỉ sử dụng công cụ chat do công ty quy định là Skype
* **Endpoint Security:**
  + Quy định Quản lý tài sản
    - Tất cả các tài sản phần cứng và phần mềm phải được lập thành văn bản. Đối với các tài sản phần cứng phải được gán nhãn.
    - Tất cả các máy phải được cài đặt Endpoint Security
    - Phải chặn hết các cổng USB của các máy
    - Phải thực hiện Block BIOS tất cả các máy
    - Người dùng có nhu cầu sử dụng USB phải được sự phê duyệt của Quản lý, gửi phiếu yêu cầu về cho bộ phận IT
    - Phần mềm nằm ngoài danh mục phải thực hiện gửi phiếu yêu cầu về cho bộ phận IT đánh giá
    - Khi mang thiết bị ra vào tòa nhà phải có giấy xác nhận của trưởng đơn vị
    - Không mang các thiết bị lưu trữ ngoài vào cơ quan nếu không được phê duyệt
    - Khi có phát hiện, cảnh báo bất thường trên máy, người dùng có trách nhiệm thông báo ngay lập tức cho phòng bảo mật.
    - Tất cả các máy tính mà người dùng sử dụng là tài sản chung của công ty, khi có sự bất thường trên hệ thống, phòng bảo mật có toàn quyền xử lý máy của người dùng, bao gồm cả việc cài lại hệ điều hành.
* **Vulnerability Assessment:**
  + Quy định đánh giá an toàn thông tin
    - Tất cả các máy chủ phải được đánh giá ATTT Trước khi đưa vào vận hành
    - Tất cả các ứng dụng phải được đánh giá ATTT Trước khi đưa vào vận hành
    - Định kỳ hàng quý thực hiện quét toàn hệ thống bằng công cụ quản lý lỗ hổng Nessus
    - Định kỳ thực hiện dò quét lỗ hổng, đối với các lỗ hổng Critical (CVSS Score > 7.0), bộ phận bảo mật phải gửi mail cho quản trị viên và lên kế hoạch update trong vòng 5 ngày làm việc. Trong trường hợp không thể Update, Quản trị viên cần phải trình bày rõ ly do và thực hiện ký vào bản đăng ký rủi ro.
    - Định kỳ hàng quý thực hiện lên kế hoạch Update các bản vá mới cho máy chủ
    - Định kỳ bản vá hàng tháng Update các mới cho máy trạm
    - Định kỳ hàng năm thuê các dịch vụ Pentest của bên thứ 3 cung cấp
  + Quy trình quản lý thay đổi:
    - Các cấu hình của máy chủ phải được Hardenning theo tiêu chuẩn CIS và được định kỳ đặt lịch dò quét.
    - Phòng bảo mật thực hiện giám sát việc thay đổi cấu hình máy chủ. Phối hợp ngay với SysAdmin để xác minh ngay khi có thay đổi cấu hình bất thường.
    - Đối với các môi trường Live, không được phép cài đặt công cụ phát triển ứng dụng lên máy chủ live.
* **Privilege Access Management,**
  + Quy định quản lý tài khoản đặc quyền
    - Phải lập ma trận phân quyền cho tất cả hệ thống, máy chủ, quy định trách nhiệm và quyền hạn của từng cán bộ
    - Phải sử dụng hệ thống PAM để cấp phát và thu hồi quyền truy cập
    - Phải sủ dụng tính năng Video Recording khi thực hiện thao tác trên các hệ thống quan trọng
    - Thực hiện cấu hình 2FA(factor authentication) dể truy cập vào các hệ thống quan trọng
    - Việc Monitor trên giao diện của các giải pháp trong SOC như Firewall, IPS, SIEM, SOAR… phải được thực hiện trên hệ thống Bastion Host, JUMP.
    - Việc truy cập từ xa RDP, SSH vào các máy chủ phải được phê duyệt và quản lý qua PAM.
    - Các tài khoản đặc quyền như Administrators, root phải được niêm phong vào bỏ vào két sắt
    - Định kỳ thực hiện thay đổi tài khoản đặc quyền (có biên bản xác nhận)
    - Các phong bì cất giữ tài khoản đặc quyền phải được đánh mã và gán nhãn.
    - Định kỳ rà soát quyền truy cập, đảm bảo đúng quyền, và đảm bảo rằng các nhân sự đã nghỉ việc phải bị disable account.
* **SIEM + SOAR**
  + Quy định an toàn bảo mật hệ thống
    - Thành lập Phòng bảo mật, chịu trách nhiệm quản lý các vấn đề về an toàn thông tin. Phòng bảo mật phải tách biệt với các thành phần khác như Phát triển ứng dụng (DEV) và hạ tầng (Infrastructure)
    - Tất cả các máy chủ phải gửi log về hệ thống SIEM
    - Phòng bảo mật có trách nhiệm giám sát các cảnh báo của SIEM 24/7 và thực hiện phản ứng nhanh trên hệ thống SOAR
    - Hệ thống SIEM phải lưu log tối thiểu một năm
    - Đối với các sự cố về mã độc, phải ngay lập tức xử lý tự động bằng hệ thống SOAR
    - Phòng bảo mật có trách nhiệm định kỳ hàng tháng báo cáo hoạt động An ninh thông tin của hệ thống cho CIO
    - Hệ thống SIEM phải cảnh báo tự động việc người dùng VPN ngoài giờ hành chính.
    - Hệ thống SIEM phải cảnh báo được việc người dùng truy cập sai vào một hệ thống nhiều lần
    - Hệ thống SIEM và hệ thống SOAR phải thích hợp và phối hợp với nhau, đảm bảo khi có cảnh báo từ SIEM thì SOAR sẽ tự động phản ứng với các case thường gặp.
    - Hệ thống SOAR phải tích hợp việc ngăn chặn với các hệ thống hiện có, đảm bảo đủ quyền ngăn chặn tự động trên Firewall, IPS, Endpoint.