Bài tập Chương 09 – Chỉ số Rủi ro trọng yếu (KRI)

Đề bài tập: Hãy đề xuất một Chỉ số rủi ro trọng yếu (KRI) thuộc 1/3 loại: Con người, Quy trình và Công nghệ và soạn bài làm theo Dàn bài sau đây.

Tình huống/ngữ cảnh:

Công ty GreenTech là một doanh nghiệp chuyên cung cấp giải pháp công nghệ thông minh cho ngành năng lượng tái tạo (ví dụ: năng lượng mặt trời, gió). Với hơn 8 năm hoạt động, công ty đang mở rộng quy mô và đối mặt với nhiều thách thức liên quan đến rủi ro vận hành và bảo mật, bao gồm:

a) **Tài sản thông tin:** Dữ liệu khách hàng, dữ liệu dự đoán sản lượng năng lượng (theo thời tiết, vị trí), thông tin thầu và hợp đồng, cùng các báo cáo phân tích hiệu suất hệ thống.

b) **Tài sản phần mềm:** Phần mềm quản lý và giám sát hệ thống năng lượng, ứng dụng AI dự đoán sản lượng, và cơ sở dữ liệu thiết kế các giải pháp lắp đặt.

c) **Tài sản vật lý:** Các thiết bị giám sát từ xa (remote monitoring devices), máy chủ tại trung tâm dữ liệu, và các bộ lưu trữ điện năng kết nối IoT.

d) **Tài sản con người:** Đội ngũ chuyên gia CNTT và kỹ sư năng lượng có kinh nghiệm, cùng đội ngũ vận hành bảo trì tại chỗ.

e) **Quy trình:** Các quy trình giám sát, bảo trì hệ thống từ xa qua nền tảng IoT, quy trình xử lý sự cố hệ thống, và quy trình cung cấp dịch vụ khách hàng.

1. **ĐIỂM YẾU:** *(ghi ra nội dung điểm yếu)*
   Thiếu biện pháp bảo mật tiên tiến và cơ chế cập nhật thường xuyên cho thiết bị IoT.
2. **MỐI ĐE DỌA:** *(ghi ra nội dung mối đe dọa)*

   Tin tặc khai thác lỗ hổng IoT để thực hiện các cuộc tấn công xâm nhập hoặc đánh cắp dữ liệu.

3. **RỦI RO TIỀM ẨN:** *(ghi ra nội dung sự kiện tiềm ẩn có thể xảy ra gây tổn hại cho doanh nghiệp khi mối đe dọa có thể khai thác được điểm yếu)*
   - Hệ thống bị gián đoạn dẫn đến mất dữ liệu và thời gian phục hồi kéo dài.
   - Đối thủ cạnh tranh có thể tiếp cận thông tin nhạy cảm.
   - Thiệt hại tài chính từ việc khôi phục hệ thống và mất uy tín khách hàng.
   - Mất quyền kiểm soát hệ thống thiết bị IoT, gây gián đoạn vận hành năng lượng tái tạo
4. **NGUỒN RỦI RO ('Risk Source')**: *(phát biểu Nguồn rủi ro là một yếu tố ('element') (riêng lẻ hay kết hợp với yếu tố khác) phát sinh từ một sự kiện nào đó khiến rủi ro tăng lên (tức là RỦI RO có thể từ rủi ro tiềm ẩn trở thánh một rủi ro có khả năng xảy ra cao hay đã xảy ra tại doanh nghiệp) - :*
   - Sự kiện xảy ra: Tin tặc phát hiện lỗ hổng bảo mật chưa được vá trên các thiết bị IoT của công ty và thực hiện tấn công.
   - Hệ thống không kiểm soát được lưu lượng tấn công tăng đột biến, làm giảm khả năng phòng thủ.
5. **METRICS đo lường rủi ro tiềm ẩn:**

Metrics (tập các số liệu đo được là tỷ lệ tấn công mạng vượt qua hệ thống bảo mật hàng tháng):

Tỷ lệ tấn công mạng vượt qua hệ thống bảo mật (%)

1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 – 10 – 11 – 12

: Khi giá trị vượt quá 3%, khả năng xảy ra rủi ro (Occ) tăng lên.

6. **Thiết lập KRI:** *(phát biểu định nghĩa KR) dựa theo các thông tin đã nêu ra ở trên kèm theo công thức tính - Ví dụ: Tỷ lệ % người lao động nghỉ việc trong năm = (Số lượng người lao động nghỉ việc trong năm) * 100 / (Tổng số Người lao động của doanh nghiệp trong năm))*
   - **KRI:**
     - Định nghĩa: Là tỷ lệ tin tặc vượt qua hệ thống bảo mật phản ánh mức độ yếu kém của các biện pháp bảo vệ hệ thống.
     - Công thức tính: KRI = (Số lượng tấn công vượt qua hệ thống bảo mật x 100) / (Tổng số tấn công mạng).
   - **KPI:** Được Giám đốc Công ty chỉ định giá trị nên không có công thức tính ở đây.

7. **Ngưỡng giá trị của KRI:** *(phát biểu một giá trị ('value') là một con số (Number) đo đếm được mà nếu giá trị KRI (ở mục 5.) vượt quá ngưỡng này, một hành động phải được thực hiện để giảm rủi ro cho doanh nghiệp.*
   - **KRI <= 3%** (Tỷ lệ các cuộc tấn công vượt qua hệ thống bảo mật).
   - Giải thích: Một tỷ lệ tấn công vượt quá 3% sẽ cảnh báo rằng hệ thống bảo mật không còn hiệu quả để bảo vệ thiết bị IoT, AI, và dữ liệu.

8. **Tần suất giám sát KRI**
   - Bộ phận CNTT giám sát KRI hàng ngày để duy trì ngưỡng KRI <= 3% và báo cáo các trường hợp KRI vượt ngưỡng (>3%) ngay lập tức.
   - Sử dụng KRI > 3% làm cảnh báo để áp dụng biện pháp cải thiện nhanh chóng, như nâng cấp tường lửa hoặc vá lỗi hệ thống, để giảm thiểu rủi ro xâm nhập.

(*)Xem Bài tập mẫu có tên (Sample)BaiTap_Ch.09(KRI).pdf để tìm hiểu cách điền thông tin theo dàn bài này./.