**Bài tập Chương 6 – Chiến lược QLRR (Risk Management Strategy)**

**Đề bài tập: Hãy đề xuất chiến lược QLRR ATTT cho một rủi ro CNTT**

Đề xuất kết hợp 2 chiến lược QLRR ATTT đối với ủi ro về bảo mật khi mạng nội bộ của nhân viên, mạng máy chủ và mạng khách tại Công ty XYZ đều sử dụng cùng một subnet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I. NHÓM YÊU CẦU – YÊU CẦU:  Rủi ro thuộc về nhóm:  *Nhóm A.13 "Communications security", Yêu cầu A.13.1 "Network security management"* | | | | |
| II. ĐIỀU KHOẢN VI PHẠM  Sinh viên đã phát hiện sự không phù hợp tại điều khoản sau:  A.13.1.3 Segregation in networks  *Control: Groups of information services, users and information systems shall be segregated on networks.* | | | | |
| III. NỘI DUNG PHÁT HIỆN VI PHẠM  *Tình huống/ngữ cảnh:* *Mạng nội bộ của nhân viên, mạng máy chủ và mạng khách tại Công ty XYZ đều sử dụng chung một subnet, không có sự phân tách giữa các nhóm người dùng và hệ thống.*   1. ĐIỂM YẾU: Thiếu ranh giới bảo mật giữa các lớp mạng cho nhân viên, khách và máy chủ. 2. MỐI ĐE DỌA: Tin tặc hoặc nhân viên nội bộ tấn công vào mạng. 3. RỦI RO TIỀM ẨN: Một thiết bị bị xâm nhập (ví dụ: thiết bị của khách bị nhiễm mã độc) có thể lây lan sang toàn bộ hệ thống. Gây gián đoạn hoạt động kinh doanh hoặc vi phạm pháp luật về luật An Ninh Mạng 4. KHẢ NĂNG XẢY RA RỦI RO: 95% 5. HỆ QUẢ:  * Thiệt hại tài chính lớn, tổn thất 500 triệu VNĐ * Công ty XYZ mất uy tín với khách hàng và đối tác. * Gây gián đoạn hoạt động kinh doanh | | | | |
| IV. CHIẾN LƯỢC QUẢN LÝ RỦI RO ATTT   1. Chọn chiến lược nào trong 4 chiến lược sau đây: *(đánh dấu ‘x’ vào 1 hoặc hơn 1 trong 4 chọn lựa)*  * Chấp nhận rủi ro (‘Risk Retention’): ☐ * Giảm nhẹ rủi ro (‘Risk Mitigation’): ☐ * Tránh né rủi ro (‘Risk Avoidance’): ⌧ * Chuyển giao rủi ro (‘Risk Transfer’): ⌧  1. Giải thích: 2. Lý do chọn chiến lược:   - Chọn Risk Avoidance – Tránh né rủi ro: Ngừng sử dụng chung một subnet cho các mạng khác nhau, đảm bảo an toàn thông tin tối đa.  - Chọn Risk Transfer – Chuyển giao rủi ro: Chuyển một phần trách nhiệm và thiệt hại tài chính cho bên thứ ba thông qua bảo hiểm An ninh mạng   1. Mục tiêu là gì: *(mục tiêu phải cụ thể (S.M.A.R.T) và có con số đo lường kết quả để có thể kiểm chứng được bằng các thang đo phù hợp):* Phân tách 100% mạng nội bộ, mạng máy chủ và mạng khách thành các subnet riêng biệt; đảm bảo mạng nội bộ công ty XYZ được an toàn 100%; giảm số lần xảy ra sự cố bảo mật do thiếu phân tách về 0. 2. Biện pháp kiểm soát rủi ro *(tham khảo ‘Control’ trong Phụ lục A – ISO 27001 rồi triển khai theo hướng dẫn trong ‘Implementation Guidance’ trong ISO 27002)* để thực hiện chiến lược QLRR là gì:   Triển khai phân tách mạng bằng cách sử dụng các subnet riêng biệt. Sử dụng VLAN (Virtual Local Area Networks) để phân chia logic các mạng. Cấu hình tường lửa (firewall) và danh sách kiểm soát truy cập (ACLs) để giới hạn giao tiếp giữa các subnet. Kết hợp mua bảo hiểm An ninh mạng để bồi thường thiệt hại tài chính. | | | | |
| V. KẾ HOẠCH HÀNH ĐỘNG: | | | | |
| Các bước triển khai biện pháp kiểm soát rủi ro (hay phương án xử lý rủi ro) cho từng chiến lược QLRR đã chọn được thực hiện theo kế hoạch như sau: | **Dự kiến nguồn lực, chi phí để thực hiện** | **Đơn vị/ cá nhân thực hiện** | **Lịch trình triển khai** | **Thời hạn hoàn thành** |
| - Bước 1. Đánh giá hiện trạng mạng và lập kế hoạch phân tách subnet: thu thập thông tin về cấu trúc mạng hiện tại, thiết kế sơ đồ phân tách subnet.  - Bước 2. Triển khai phân tách mạng: Cấu hình router/switch để tạo subnet riêng, cài đặt và cấu hình firewall giữa các subnet  - Bước 3. Cài đặt và cấu hình IDS/IPS: mua và cài đặt phần mềm IDS/IPS, cấu hình quy tắc giám sát và cảnh báo.  - Bước 4. Đào tạo nhân viên: tổ chức hội thảo về chính sách sử dụng mạng an toàn, cung cấp tài liệu hướng dẫn.  - Bước 5. Kiểm tra và đánh giá: thực hiện kiểm tra bảo mật sau triển khai, điều chỉnh nếu cần thiết.  - Bước 6. Triển khai thực tế | - Chuyên viên IT của Phòng CNTT trực thuộc Công ty XYZ  - Liên hệ Chuyên gia An Ninh Mạng MyVNPT để có giá tư vấn về việc cấu hình mạng: 15.000.000 VNĐ | - Ông Lê Khuyến Dương - Trưởng Phòng CNTT tại Công ty XYZ  - Bà Trần Cẩm Lan - Chuyên gia An Ninh Mạng tại MyVNPT | Triển khai từ ngày 16/04/2025 | 15 ngày |
| 2) Chiến lược chuyển giao rủi ro – Mua Bảo hiểm Dữ liệu và An ninh mạng của Tập đoàn Bảo Việt  Tham gia Bảo hiểm Dữ liệu và An ninh mạng của Tập đoàn Bảo Việt qua ứng dụng BaoViet Direct Ipay để được bảo vệ trong suốt 01 năm kể từ thời điểm đăng ký dịch vụ. Tra cứu tại: [Tổng công ty Bảo hiểm Bảo Việt - Bảo hiểm dữ liệu và an ninh mạng](https://baovietonline.com.vn/vi/bao-hiem-doanh-nghiep/34/bao-hiem-du-lieu-va-an-ninh-mang.html)  Tải ứng dụng tại: [BaoViet Direct - Ứng dụng trên Google Play](https://play.google.com/store/apps/details?id=com.baohiembaoviet.baovietid&hl=vi&pli=1) ; [Baoviet Direct on the App Store](https://apps.apple.com/us/app/baoviet-direct/id1372421282) | 6.990.000 VNĐ/tháng | Liên hệ bà Nguyễn Việt Hương – Giám đốc Chi nhánh Phía Nam (0941.049.053) tại Văn phòng Công ty Bảo hiểm Bảo Việt tại Lầu 6, 610 Võ Văn Kiệt, Phường Cầu Kho, Quận 1, Thành phố Hồ Chí Minh  *Hoặc thông qua hotline: 1900 558899* | Triển khai từ ngày 25/04/2025 | 07 ngày |