**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 rủi ro về bảo mật đối với dữ liệu quan trọng chưa được mã hoá khi lưu trữ trên máy chủ CSDL nội bộ.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I. NHÓM YÊU CẦU – YÊU CẦU:  Rủi ro thuộc về nhóm:  *Nhóm A.10 “Cryptography”, Yêu cầu A.10.1 “Cryptography controls”*  *Nhóm A.9 “Access Control”, Yêu cầu A.9.2 “User access management” và Yêu cầu A.9.4 “System and application access control”* | | | | |
| II. ĐIỀU KHOẢN VI PHẠM  Sinh viên đã phát hiện sự không phù hợp tại điều khoản sau:  A.10.1.1. Policy on the use of cryptographic controls  *Control: A policy on the use of cryptographic controls for protection of information shall be developed and implemented*  A.9.2.3. Management of privileged access rights  *Control: The allocation and use of privileged access rights shall berestricted and controlled.*  A.9.4.1. Information access restriction  *Control: Access to information and application system functions shall be restricted in accordance with the access control policy* | | | | |
| III. NỘI DUNG PHÁT HIỆN VI PHẠM  *Tình huống/ngữ cảnh:* *Tại bệnh viện Tư nhân ABC, tất cả thông tin về bệnh nhân (bao gồm hồ sơ khám chữa bệnh, kết quả xét nghiệm, chẩn đoán và kế hoạch điều trị…) đều được lưu trữ trên hệ thống máy chủ CSDL nội bộ. Ngoài ra, các bác sĩ và nhân viên y tế thường sử dụng thiết bị di động (máy tính bảng, smartphone, laptop) để truy cập vào và cập nhật thông tin y tế trong quá trình chăm sóc bệnh nhân. Hiện tại, hệ thống của bệnh viện chưa có kiểm soát truy cập cũng như mã hóa dữ liệu quan trọng khi lưu trữ trên máy chủ. Do đó, khi có sự cố về bảo mật như xâm nhập trái phép vào hệ thống CSDL thì các thông tin nhạy cảm của bệnh nhân sẽ dễ bị lộ ra ngoài. Điều này không chỉ vi phạm quyền riêng tư của bệnh nhân mà còn làm suy giảm uy tín và độ tin cậy của bệnh viện, ảnh hưởng đến mối quan hệ giữa bệnh viện và cộng đồng.*   1. ĐIỂM YẾU:   Doanh nghiệp chưa mã hóa và kiểm soát truy cập vào dữ liệu quan trọng khi lưu trữ trên máy chủ CSDL nội bộ   1. MỐI ĐE DỌA: Tin tặc xâm nhập trái phép vào hệ thống 2. RỦI RO TIỀM ẨN: dẫn đến rò rỉ thông tin cá nhân và y tế của bệnh nhân. Nguy hiểm hơn là tin tặc sẽ thay đổi/phá hỏng toàn bộ dữ liệu của hệ thống. 3. KHẢ NĂNG XẢY RA RỦI RO: 95% 4. HỆ QUẢ:  * Vi phạm quyền riêng tư: Thông tin bệnh nhân sẽ bị tiết lộ ra ngoài, gây vi phạm quyền riêng tư và có thể làm tổn hại đến danh dự, sự riêng tư của cá nhân và gia đình họ. * Mất uy tín và niềm tin từ cộng đồng: Một sự cố bảo mật lớn sẽ làm bệnh viện mất đi lòng tin từ bệnh nhân cũng như cộng đồng, ảnh hưởng trực tiếp đến danh tiếng và khả năng duy trì dịch vụ chăm sóc sức khỏe. * Hậu quả pháp lý và tài chính: Vi phạm tiêu chuẩn bảo mật thông tin có thể dẫn đến các vụ kiện tụng, phạt hành chính từ các cơ quan quản lý và tổn thất tài chính lên đến 50 tỉ VNĐ. * Ảnh hưởng đến hoạt động y tế: Khi thông tin bị lỗi thời hoặc bị chỉnh sửa trái phép, quá trình chăm sóc, chẩn đoán và điều trị bệnh nhân có thể gặp trở ngại, từ đó ảnh hưởng trực tiếp đến sức khỏe và an toàn của bệnh nhân. | | | | |
| 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: Để ngăn chặn hoàn toàn nguy cơ xâm nhập trái phép và lộ thông tin bệnh nhân, đảm bảo dữ liệu được bảo vệ tối đa nhờ mã hóa dữ liệu và kiểm soát truy cập vào hệ thống.  - Chọn Risk Transfer – Chuyển giao rủi ro: Dự phòng rủi ro ngoài dự tính, chuyển giao thông qua hợp đồng bảo hiểm an ninh mạng giúp bồi thường thiệt hại nếu xảy ra sự cố..   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):* Kiểm soát 100% các truy cập vào hệ thống, mã hóa 100% dữ liệu nhạy cảm trên máy chủ CSDL, giảm số vụ vi phạm về truy cập/xử lý dữ liệu xuống 0 sau khi triển khai xong. 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:   Mã hoá và Kiểm soát truy cập: Sử dụng mã hoá AES 256 cho dữ liệu kết hợp với CP-ABE và kiểm soát truy cập ABAC, đảm bảo chỉ những người có thuộc tính phù hợp với chính sách truy cập vào hệ thống CSDL thì mới có thể truy cập để sử dụng (xem/thêm/xoá/sửa) dữ liệu. Kết hợp việc mua bảo hiểm an ninh mạng của nhà cung cấp dịch vụ bảo hiểm để bồi thường thiệt hại khi xảy ra sự cố bảo mật. | | | | |
| 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** |
| 1) Chiến lược tránh né rủi ro – Mã hoá và Kiểm soát truy cập vào hệ thống CSDL  - Bước 1: Khảo sát & Phân tích hệ thống CSDL nhằm xác định chính xác dữ liệu nhạy cảm cần mã hoá.  - Bước 2: Xác định thuộc tính và chính sách truy cập: Các lãnh đạo cấp cao của Bệnh viện cung cấp các thuộc tính của nhân sự trong bệnh viện, đồng thời họ phải cung cấp chính xác các chính sách truy cập vào CSDL của hệ thống.  - Bước 3: Thiết kế thuật toán mã hoá CSDL:  + Lựa chọn mode GCM cho AES 256 và scheme AC17 cho CP-ABE.  + Với mỗi trường dữ liệu, tạo 1 Random Key (RK) có lenRK = 12288 bit, sau đó sử dụng thuật toán băm an toàn SHA3\_256 để băm RK, ta được đầu ra là dữ liệu 256 bit cũng chính là khoá AES\_Key của AES-GCM-256 để bảo vệ trường dữ liệu đó luôn.  + Đảm bảo các Random Key và AES\_Key là duy nhất, không được trùng nhau.  + Sử dụng CP-ABE-AC17 để mã hoá RK ta được encRK  + Sử dụng AES-GCM-256 để mã hoá dữ liệu của CSDL ta được Ciphertext.  + Kết hợp các dữ liệu trên thành dữ liệu mã hoá cuối gồm: lenRK + encRK + Ciphertext => encData  + Khi giải mã, thuật toán sẽ đi theo chiều ngược lại: tách các thành phần trong encData => sau đó giải mã encRK trước => được RK, băm RK với SHA3\_256 => có được AES\_Key => có AES\_Key => Giải mã được dữ liệu ban đầu.  Bước 4. Triển khai kiểm soát truy cập theo ABAC. Cài đặt và cấu hình kiểm soát truy cập dựa trên thuộc tính đã có được từ Bước 2.  Bước 5. Kiểm thử & Đào tạo: Kiểm tra hiệu quả hệ thống, đào tạo nhân viên vận hành.  Bước 6. Chính thức đưa vào vận hành | - Chuyên viên IT của Bộ phận CNTT trực thuộc Bệnh viện Tư nhân ABC.  - Liên hệ Chuyên gia An Toàn Thông Tin Viettel để có giá tư vấn về thuật toán mã hoá, cách cấu hình thuật toán: 30.000.000 VNĐ | - Ông Lưu Đức Hoa - Trưởng Bộ phận CNTT Bệnh viện Tư nhân ABC  - Ông Nguyễn Văn An - Chuyên gia An Toàn Thông Tin của Viettel | Triển khai từ ngày 14/04/2025 | 10 ngày |
| 2) Chiến lược chuyển giao rủi ro – Mua bảo hiểm An ninh mạng của Công ty TNHH Bảo hiểm Chubb Việt Nam  Tham gia Bảo hiểm An ninh mạng của công ty Chubb Việt Nam để được bảo vệ kể từ thời điểm đăng ký thuê dịch vụ. Tra cứu thông tin bảo hiểm thông qua: [Bảo hiểm an ninh mạng – Chubb tại Việt Nam](https://www.chubb.com/vn-vn/business/cyber-insurance.html?) | 3.000.000 VNĐ/tháng | Liên hệ ông Nguyễn Sơn Tùng – Chuyên viên tư vấn bảo hiểm (0919.686.868) tại Văn phòng Công ty TNHH Bảo hiểm Chubb Việt Nam tại Tầng 21 Tòa nhà Sun Wah, 115 Nguyễn Huệ - Phường Bến Nghé - Quận 1 - TP. Hồ Chí Minh  *Hoặc thông qua hotline: 028-38278989* | Triển khai từ ngày 18/04/2025 | 07 ngày |