**Họ và tên: Nguyễn Quốc Huy**

**MSSV: 22133026**

**Phân tích và đề xuất giải pháp an ninh mạng cho hệ thống CNTT doanh nghiệp.**

Giải pháp an ninh mạng cho hệ thống CNTT doanh nghiệp cần được xây dựng dựa trên những nguyên tắc cơ bản của an toàn thông tin, bao gồm: Confidentiality (Bảo mật), Integrity (Tính toàn vẹn), Availability (Khả dụng).

1. **Phân thích an ninh mạng cho hệ thống CNTT doanh nghiệp:**
   1. **Đánh giá hiện trạng bảo mật của hệ thống:**

* Kiểm tra hệ thống kiểm soát truy cập: Xem xét các quyền truy cập được cấp cho từng người dùng và các biện pháp kiểm soát để ngăn chặn truy cập trái phép. Nguyên tắc Least Privilege và Separation of Duties nên được áp dụng để giới hạn quyền truy cập.
* Kiểm tra việc triển khai các giải pháp bảo vệ: Xác định các giải pháp bảo mật hiện có như firewall, IDS/IPS, xác thực đa yếu tố (MFA), và các biện pháp mã hóa cho dữ liệu nhạy cảm.
* Đánh giá việc quản lý và bảo vệ dữ liệu: Xác định các biện pháp bảo mật dữ liệu đang có (như mã hóa và kiểm soát truy cập) và các giải pháp bảo vệ tính toàn vẹn dữ liệu, đảm bảo dữ liệu không bị sửa đổi trái phép.
* Phân tích nhật ký hệ thống (logs): Kiểm tra logs để phát hiện các dấu hiệu truy cập bất thường, có thể là hành vi đáng ngờ hoặc các cuộc tấn công từ bên ngoài.
  1. **Xác định mối đe dọa tiềm ẩn:**
* Tấn công bằng mã độc: Các nguy cơ từ email phishing, mã độc đính kèm qua email, cần triển khai các giải pháp như lọc nội dung email và quét mã độc tự động.
* Tấn công bằng kỹ thuật injection (như SQL injection): Những hệ thống trực tuyến dễ bị tấn công injection nếu không bảo mật tốt. Lớp Application Layer cần được bảo vệ chặt chẽ bằng các kỹ thuật kiểm tra đầu vào.
* Tấn công tràn bộ đệm: Các hệ thống cần triển khai biện pháp Stackshield hoặc canary để chống lại các tấn công tràn bộ đệm.
* Truy cập trái phép với thông tin xác thực bị đánh cắp: Cần bổ sung xác thực đa yếu tố (MFA) để giảm thiểu rủi ro.
* Mã hóa không đầy đủ: Kiểm tra việc mã hóa giao tiếp trên mạng (như SSH thay cho Telnet) để tránh nghe lén và giả mạo thông tin.

1. **Đề xuất các giải pháp bảo mật phù hợp cho hệ thống:**
   1. **Tăng cường kiểm soát truy cập:**

* Áp dụng mô hình kiểm soát truy cập: Áp dụng Role-Based Access Control (RBAC) hoặc Attribute-Based Access Control (ABAC) để phân quyền truy cập dựa trên vai trò và thuộc tính của người dùng.
* Least Privilege và Separation of Duties: Đảm bảo mỗi người chỉ có quyền truy cập tối thiểu cần thiết để thực hiện công việc.

- Xác thực đa yếu tố (MFA): Đặc biệt là cho các tài khoản có quyền truy cập vào hệ thống nhạy cảm hoặc quản trị mạng.

**b. Củng cố lớp bảo vệ hệ thống mạng và các dịch vụ:**

**-** Triển khai Firewall và IDS/IPS: Firewall nên được cấu hình kỹ càng để chặn các kết nối không cần thiết, trong khi IDS/IPS giúp phát hiện và ngăn chặn các cuộc tấn công trong thời gian thực.

**-** DHCP Snooping và Port Security trên Switch: Giảm thiểu nguy cơ từ các thiết bị giả mạo và chặn kết nối từ các địa chỉ MAC không xác định

- Sử dụng VPN cho kết nối từ xa: Mã hóa kết nối và kiểm soát chặt chẽ quyền truy cập từ các thiết bị bên ngoài vào hệ thống nội bộ.

**c. Bảo vệ ứng dụng và dữ liệu:**

**-** Chống SQL injection và buffer overflow: Các ứng dụng web cần triển khai biện pháp kiểm tra đầu vào và kiểm soát bộ nhớ.

**-** Mã hóa dữ liệu: Đảm bảo các dữ liệu nhạy cảm được mã hóa ở cả trạng thái nghỉ (data-at-rest) và trong khi truyền (data-in-transit).

**-** Triển khai hệ thống giám sát mạng với SNMP: Để giám sát lưu lượng mạng và phát hiện các bất thường hoặc tấn công ngay khi có dấu hiệu.

**d. Quản lý bảo mật liên tục và nâng cao nhận thức:**

**-** Cập nhật bản vá và phần mềm bảo mật: Đảm bảo hệ điều hành và ứng dụng luôn được cập nhật để khắc phục các lỗ hổng bảo mật mới nhất.

**-** Đào tạo nhân viên về an toàn thông tin: Tăng cường nhận thức về an ninh mạng, tránh rủi ro từ các cuộc tấn công phishing và social engineering.

**-** Xây dựng kế hoạch khắc phục sự cố: Chuẩn bị và thường xuyên thử nghiệm kế hoạch đối phó sự cố để sẵn sàng phản ứng nhanh chóng khi xảy ra tấn công.