B?o v? tài s?n v?t lý

- Sử dụng thẻ tài sản để xác định và định vị thiết bị vật lý:
  - Gắn thẻ theo dõi và kiểm kê định kỳ tất cả tài sản IT quan trọng.
  - Lưu trữ thiết bị không sử dụng trong các khu vực được bảo vệ.
  - Thiết lập quy trình báo cáo khi thiết bị bị mất hoặc hỏng.

2. **Quản trị và tuân thủ an ninh**
   - Tuân thủ các yêu cầu về bảo mật như GDPR và HIPAA:
     - Thực hiện kiểm tra định kỳ để đảm bảo tổ chức tuân thủ các quy định pháp lý.
     - Bổ nhiệm chuyên viên chịu trách nhiệm về tuân thủ dữ liệu.
     - Lưu trữ tài liệu và chứng từ liên quan đến tuân thủ an ninh mạng.
3. **Phân tích sau sự cố**
   - Thực hiện phân tích sau sự cố để cải thiện các biện pháp an ninh:
     - Tổ chức họp đánh giá sự cố để rút ra bài học kinh nghiệm.
     - Ghi lại các bước xử lý sự cố trong tài liệu chính thức.
     - Đưa ra các biện pháp khắc phục và cập nhật kế hoạch ứng phó.
4. **An ninh trong DevOps**
   - Tích hợp an ninh vào quy trình DevOps để kiểm tra và xác nhận an ninh liên tục:
     - Sử dụng các công cụ quét bảo mật trong chu trình CI/CD.
     - Tích hợp quy trình "shift-left security" để phát hiện sớm các vấn đề bảo mật.
     - Thực hiện đào tạo DevSecOps cho đội ngũ phát triển và vận hành.
5. **An ninh trong môi trường BYOD**
   - Thiết lập chính sách bảo mật cho các thiết bị cá nhân sử dụng cho công việc:
     - Yêu câu cài đặt các ứng dụng quản lý thiết bị di động (MDM).
     - Hạn chế truy cập dữ liệu nhạy cảm từ các thiết bị chưa đăng ký.
     - Cung cấp hướng dẫn rõ ràng về cách sử dụng an toàn các thiết bị cá nhân.
6. **An ninh truy cập từ xa**
   - Sử dụng giải pháp truy cập từ xa an toàn cho nhân viên làm việc từ xa:
     - Triển khai VPN hoặc Zero Trust Network Access (ZTNA).
     - Bảo mật các thiết bị cá nhân sử dụng để truy cập từ xa.
     - Theo dõi và kiểm soát lưu lượng mạng từ xa.
7. **Kiểm tra an ninh của công nghệ mới**
   - Đánh giá rủi ro và kiểm tra an ninh trước khi áp dụng công nghệ mới:
     - Tích hợp công nghệ vào môi trường sandbox để kiểm tra an ninh.
     - Thu thập thông tin bảo mật từ nhà cung cấp trước khi mua sắm.
     - Thục hiện đánh giá bảo mật bên thứ ba nếu cần thiết.
8. **Quản lý mật khẩu và xác thực**
   - Thực hiện chính sách mật khẩu mạnh và xác thực đa yếu tố:
     - Yêu cầu mật khẩu có độ dài tối thiểu 12 ký tự và phức tạp.
     - Đặt thời hạn hết hạn mật khẩu theo tiêu chuẩn bảo mật.
     - Khuyến khích sử dụng trình quản lý mật khẩu để tránh tái sử dụng.
9. **Phân đoạn và cô lập mạng**
   - Phân đoạn mạng để cô lập các hệ thống quan trọng khỏi lưu lượng mạng chung:

    - Áp dụng VLAN để phân đoạn các khu vực mạng khác nhau.
    - Kiểm tra và sửa chữa các lỗi cấu hình mạng định kỳ.
    - Sử dụng công nghệ micro-segmentation để tăng tính cô lập.
10. **Bảo vệ dữ liệu đám mây**
    - Mã hóa dữ liệu lưu trữ trên đám mây:
        - Sử dụng mã hóa đầu cuối để bảo vệ dữ liệu lưu trữ và truyền tải.
        - Kiểm tra chính sách sao lưu và khôi phục dữ liệu của nhà cung cấp.
        - Đảm bảo khả năng kiểm soát và thu hồi dữ liệu khi kết thúc hợp tác.
11. **Quản lý lỗ hổng bảo mật**
    - Quét và đánh giá hệ thống thường xuyên để phát hiện lỗ hổng bảo mật:
        - Sử dụng các công cụ quét bảo mật tự động (Nessus, OpenVAS, v.v.).
        - Đánh giá các lỗ hổng dựa trên mức độ rủi ro và tác động.
        - Triển khai các bản vá hoặc giải pháp thay thế kịp thời.
12. **Đào tạo an ninh cho nhân viên IT**
    - Đào tạo nhân viên IT về các mối đe đọa an ninh mạng mới nhất:
        - Cung cấp tài liệu và khóa học liên tục về các xu hướng bảo mật.
        - Thực hành các bài tập mô phỏng tấn công mạng trong môi trường an toàn.
        - Đánh giá và nâng cấp kỹ năng đội ngũ IT định kỳ.
13. **Nhận thức an ninh trong vai trò tiếp xúc khách hàng**
    - Đào tạo nhân viên tiếp xúc khách hàng về cách xử lý dữ liệu khách hàng một cách an toàn:
        - Thực hiện các buổi hướng dẫn ngắn gọn và dễ hiểu.
        - Xây dựng tài liệu tham khảo nhanh về các quy tắc bảo mật dữ liệu khách hàng.
        - Giám sát và hỗ trợ nhân viên khi xử lý các tỉnh huống đặc biệt.
14. **Quản lý cấu hình an toàn**
    - Duy trì cấu hình an toàn cho các thiết bị và hệ thống mạng:
        - Lưu trữ và quản lý tất cả cấu hình trong hệ thống kiểm soát phiên bản.
        - Sử dụng các công cụ quản lý cầu hình tự động (Ansible, Chef, Puppet, v.v.).
        - Kiểm tra định kỳ để phát hiện và sửa lỗi cầu hình.
15. **Sao lưu và phục hồi dữ liệu**
    - Thực hiện kế hoạch sao lưu dữ liệu định kỳ và lưu trữ sao lưu ngoài site:
        - Sử dụng các giải pháp sao lưu tự động để đảm bảo tính liên tục.
        - Thực hiện kiểm tra khôi phục dữ liệu định kỳ để xác nhận khả năng phục hồi.
        - Đảm bảo sao lưu dữ liệu quan trọng tại các trung tâm dữ liệu khác nhau.

Revision #1
Created 17 September 2025 10:46:00 by Hieu Nguyen
Updated 17 September 2025 10:47:19 by Hieu Nguyen