SỔ TAY AN NINH MẠNG

(2024)

---

1. Chính sách và quy trình an ninh tổng quát

- Đánh giá và cập nhật chính sách an ninh mạng thường xuyên:
  - Xem xét định kỳ tất cả các chính sách hiện hành.
  - Bổ sung các quy định mới liên quan đến các nguy cơ an ninh mới.
  - Xây dựng quy trình chuẩn bị cho các tình huống khẩn cấp.
- Đào tạo nhận thức về an ninh cho nhân viên:
  - Tổ chức các buổi đào tạo định kỳ.
  - Tích hợp các tình huống mô phỏng tấn công mạng trong đào tạo.
  - Xây dựng câu hỏi khảo sát sau đào tạo để đánh giá mức độ nhận thức.

2. An ninh mạng

- Sử dụng tường lửa và mã hóa lưu lượng mạng:
  - Cấu hình tường lửa để chọn lọc lưu lượng dựa trên quy tắc.
  - Triển khai giao thức VPN đảm bảo bí mật khi truy cập từ xa.
  - Giám sát và cập nhật các giao thức mã hóa theo xu hướng hiện đại.
- Phân đoạn mạng để hạn chế di chuyển ngang trong trường hợp bị xâm nhập:
  - Tạo các vùng mạng phân biệt dành cho tài nguyên nhạy cảm và tài nguyên thông thường.
  - Sử dụng các giao thức ACL (Điều khiển truy cập) để hạn chế truy cập.
  - Giải quyết nhanh chóng các lỗi cấu hình trong phân đoạn mạng.

3. An ninh điểm cuối

- Bảo vệ các điểm cuối bằng phần mềm chống virus và mã độc:

    - Cài đặt và duy trì các phần mềm bảo vệ trên tất cả các thiết bị đầu cuối.
    - Cập nhật định kỳ các định nghĩa virus và bản vá lỗi phần mềm bảo vệ.
    - Thực hiện quét toàn bộ hệ thống theo lịch trình.
- Mã hóa toàn bộ đĩa trên máy tính xách tay và thiết bị di động:
    - Sử dụng các công cụ mã hóa mạnh (như BitLocker hoặc FileVault).
    - Đảm bảo các thiết bị di động được bảo vệ bằng mật khẩu hoặc sinh trắc học.
    - Thiết lập quy trình xóa dữ liệu từ xa trong trường hợp thiết bị bị mất.

4. Bảo vệ dữ liệu

- Mã hóa dữ liệu trong quá trình truyền và lưu trữ:
    - Sử dụng giao thức HTTPS và TLS cho truyền dữ liệu.
    - Mã hóa các tập tin nhạy cảm trước khi lưu trữ (trong cơ sở dữ liệu hoặc đám mây).
    - Kiểm tra và xác minh hiệu quả của các hệ thống mã hóa định kỳ.
- Thực hiện sao lưu dữ liệu thường xuyên và lưu trữ sao lưu an toàn:
    - Lên lịch sao lưu định kỳ hàng ngày, hàng tuần, hoặc hàng tháng.
    - Lưu trữ sao lưu tại các địa điểm an toàn và phân tách với hệ thống chính.
    - Kiểm tra định kỳ khả năng phục hồi dữ liệu từ bản sao lưu.

5. Quản lý danh tính và truy cập

- Sử dụng xác thực đa yếu tố (MFA) cho các hệ thống và ứng dụng quan trọng:
    - Triển khai giải pháp MFA trên các hệ thống quan trọng.
    - Đảm bảo MFA áp dụng cho cả người dùng nội bộ và bên ngoài.
    - Thực hiện kiểm tra định kỳ tính hiệu quả của MFA.
- Kiểm soát và giám sát truy cập đặc quyền:
    - Thiết lập quy trình quản lý truy cập đặc quyền (PAM).
    - Giám sát hoạt động của tài khoản đặc quyền thông qua hệ thống ghi log.
    - Hạn chế và rà soát định kỳ quyền truy cập đặc quyền.

6. Quản lý truy cập đặc quyền

- Thiết lập chính sách và quy trình quản lý truy cập đặc quyền:
  - Định nghĩa rõ các quyền hạn đặc quyền trong chính sách an ninh.
  - Áp dụng nguyên tắc "ít đặc quyền nhất" (Least Privilege).
  - Tự động hóa việc quản lý tài khoản đặc quyền qua các công cụ PAM.
- Giám sát và ghi lại các phiên truy cập đặc quyền:
  - Sử dụng hệ thống giám sát để ghi lại các phiên truy cập.
  - Lưu trữ và mã hóa các bản ghi log truy cập để sử dụng trong điều tra.
  - Thực hiện đánh giá định kỳ các bản ghi để phát hiện hành vi bất thường.

7. An ninh ứng dụng

- Kiểm tra lỗ hổng bảo mật của các ứng dụng web thường xuyên:
  - Thực hiện kiểm tra lỗ hổng bằng công cụ tự động và kiểm tra thủ công.
  - Sửa chữa ngay lập tức các lỗ hổng nghiêm trọng được phát hiện.
  - Tích hợp kiểm tra bảo mật vào quy trình phát triển phần mềm (SDLC).
- Đánh giá bảo mật của các ứng dụng và thư viện bên thứ ba trước khi tích hợp:
  - Kiểm tra và xác minh nguồn gốc của các thư viện bên thứ ba.
  - Sử dụng các công cụ phân tích mã nguồn để phát hiện mã độc.
  - Theo dõi các cập nhật và bản vá bảo mật của nhà cung cấp.

8. An ninh đám mây

- Đánh giá bảo mật của các nhà cung cấp dịch vụ đám mây trước khi hợp tác:
  - Yêu cầu nhà cung cấp cung cấp báo cáo tuân thủ bảo mật (SOC 2, ISO 27001, v.v.).
  - Thực hiện đánh giá bảo mật độc lập đối với dịch vụ của nhà cung cấp.
  - Kiểm tra chính sách bảo mật của nhà cung cấp về mã hóa, sao lưu, và quyền riêng tư.
- Mã hóa dữ liệu lưu trữ trên đám mây:

- Triển khai mã hóa dữ liệu đầu cuối trước khi lưu trữ lên đám mây.
- Sử dụng các giải pháp quản lý khóa mã hóa (KMS).
- Đảm bảo dữ liệu đã mã hóa không thể truy cập nếu không có khóa hợp lệ.

9. An ninh vật lý

- Hạn chế và giám sát truy cập vào các trung tâm dữ liệu và phòng máy chủ:
  - Sử dụng hệ thống kiểm soát truy cập bằng thẻ từ hoặc sinh trắc học.
  - Đặt camera giám sát tại các khu vực nhạy cảm.
  - Thực hiện kiểm tra định kỳ để phát hiện các điểm yếu trong bảo mật vật lý.
- Sử dụng hệ thống quản lý khách truy cập:
  - Ghi nhận danh tính và mục đích của tất cả khách truy cập.
  - Phát hành thẻ khách truy cập giới hạn quyền truy cập.
  - Hướng dẫn khách về các quy định an ninh trước khi vào khu vực nhạy cảm.

10. Quản lý rủi ro nhà cung cấp và bên thứ ba

- Đánh giá và giám sát liên tục rủi ro an ninh của các nhà cung cấp và dịch vụ bên thứ ba:
  - Xây dựng quy trình thẩm định an ninh trước khi hợp tác.
  - Theo dõi và đánh giá định kỳ mức độ tuân thủ bảo mật của nhà cung cấp.
  - Yêu cầu báo cáo sự cố hoặc các thay đổi liên quan đến bảo mật từ nhà cung cấp.

11. Đào tạo và nhận thức về an ninh

- Khuyến khích nhân viên báo cáo các email đáng ngờ và các nỗ lực lừa đảo:
  - Cung cấp kênh báo cáo dễ dàng và bảo mật.
  - Tổ chức các buổi tập huấn nhận diện phishing.
  - Tặng thưởng hoặc công nhận nhân viên có hành động báo cáo tích cực.

12. Giám sát và phát hiện sự cố

- Sử dụng hệ thống quản lý thông tin và sự kiện an ninh (SIEM) để giám sát hoạt động mạng:
    - Cấu hình SIEM để phát hiện các hành vi bất thường.
    - Đảm bảo log từ tất cả hệ thống quan trọng được gửi về SIEM.
    - Định kỳ xem xét và cập nhật quy tắc phát hiện trong SIEM.
- Triển khai hệ thống phát hiện và ngăn chặn xâm nhập tại các điểm mạng quan trọng:
    - Sử dụng hệ thống IDS/IPS để phát hiện và phản hồi nhanh chóng các mối đe dọa.
    - Cấu hình cảnh báo theo mức độ ưu tiên phù hợp.
    - Thực hiện kiểm tra định kỳ hiệu quả của IDS/IPS.

13. Kiểm tra và đánh giá an ninh

- Thực hiện kiểm tra thâm nhập định kỳ để xác định các điểm yếu tiềm ẩn:
    - Lên lịch kiểm tra định kỳ hàng quý hoặc hàng năm.
    - Sử dụng các chuyên gia bên thứ ba để đảm bảo tính khách quan.
    - Cập nhật các biện pháp khắc phục dựa trên kết quả kiểm tra.

14. Kế hoạch liên tục kinh doanh và phục hồi sau thảm họa

- Thực hiện các quy trình phục hồi sau thảm họa cho các hệ thống quan trọng:
    - Tạo và kiểm tra kế hoạch phục hồi định kỳ.
    - Đảm bảo các bản sao dữ liệu và tài liệu quan trọng được lưu trữ an toàn.
    - Thực hiện diễn tập để đảm bảo tất cả nhân viên hiểu vai trò của mình.

15. Phản ứng sự cố an ninh

- Đào tạo và chuẩn bị cho các thành viên đội phản ứng sự cố:
    - Xây dựng quy trình phản ứng sự cố chi tiết.

- Cung cấp công cụ và tài nguyên cần thiết cho đội phản ứng.
- Tổ chức các bài tập giả lập sự cố để cải thiện khả năng ứng phó.

16. Hành vi an ninh của nhân viên

- Đào tạo nhân viên nhận biết các nỗ lực lừa đảo và kỹ thuật xã hội:
  - Tổ chức các buổi hội thảo và bài kiểm tra nhận thức định kỳ.
  - Cung cấp hướng dẫn về cách nhận diện email hoặc liên lạc đáng ngờ.
  - Thúc đẩy văn hóa an ninh mạng bằng các chương trình khen thưởng nhân viên có hành vi đúng đắn.

17. Giao tiếp an toàn

- Sử dụng các kênh giao tiếp an toàn giữa nhân viên và khách hàng:
  - Triển khai các nền tảng giao tiếp được mã hóa (như Signal, Teams, v.v.).
  - Hạn chế sử dụng email để trao đổi thông tin nhạy cảm.
  - Đào tạo nhân viên về nguy cơ từ các ứng dụng không an toàn.

18. Bảo vệ tài sản vật 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.

19. 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.

20. 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.

21. 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.

22. An ninh trong môi trường BYOD

- Thiết lập chính sách bảo mật cho các thiết bị cá nhân sử dụng cho công việc:
  - Yêu cầu 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.

23. 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.

24. 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.
- Thực hiện đánh giá bảo mật bên thứ ba nếu cần thiết.

25. 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.

26. 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.

27. 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.

28. 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.

29. Đào tạo an ninh cho nhân viên IT

- Đào tạo nhân viên IT về các mối đe dọa 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.

30. 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 tình huống đặc biệt.

31. 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 cấu hình tự động (Ansible, Chef, Puppet, v.v.).
    - Kiểm tra định kỳ để phát hiện và sửa lỗi cấu hình.

32. 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.