KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)

Môn: An toàn thông tin

Đề bài:

1. *(3 điểm)* Trình bày giải pháp để đảm bảo an toàn cho ứng dụng Email?

_ Đảm bảo ba yếu tố trong CIA Triad:bảo mật, toàn vẹn, tính sẵn sàng.

_ Đảm bảo yếu tố xác thực xác thực,Two-Factor Authentication (2FA): thường ứng dụng gmail khi đăng nhập sẽ yêu cầu 2 thông tin khác nhau để có thể đăng nhập vô tài khoản của mình, thường được yêu cầu mật khẩu của tài khoản và một mã code được gửi thông qua tin nhắn SMS điện thoại.

_ Mật khẩu cần được đạt ở mức mật khẩu mạnh, tuân theo các chính sách đặt mật khẩu, nhưng dễ nhớ đối với bản thân, sử dụng các công cụ kiểm tra để loại bỏ những mật khẩu yếu, vì mật khẩu ngẫu nhiên do máy tính tạo rất khó nhớ (mặc dù mật khẩu mạnh) nên yêu cầu người dùng đổi mật khẩu trong lần đăng nhập đầu tiên.

_ Xác nhận các tệp (file) và người nhận trước khi gửi:

+) Người dùng phải đảm bảo rằng dữ liệu sẽ được chia sẻ;

+) Nếu bạn đăng tải tệp không chính xác, bạn sẽ được kiểm tra một lần nữa trong quá trình kiểm tra lại (trước khi gửi đi), và sau đó sẽ xác nhận tất cả các tệp đính kèm;

+) Sau đó là người nhận, phải đảm bảo rằng phần Email người nhận phải được đề xuất bởi hệ thống.

_ Chặn email đối với việc gửi nhầm file hoặc đứng file nhưng nhầm người nhận, giúp hạn chế gây rõ rĩ dữ liệu.

_ Quản lý thời gian xem Email đối với những người được gửi. Thời gian xem nội dung của Email cũng đáng được chú ý vì nó cũng mang tính bảo mật, một số thông tin chỉ được truy cập trong thời gian ngắn, ngăn không cho dữ liệu nhạy cảm tồn tại quá lâu trong các hộp thư đến. Bằng cách này, sẽ giúp quán lý thông tin tốt hơn, và giảm nguy cơ bị đánh cắp dữ liệu.

_ Gửi yêu cầu cho người nhận: bằng cách này, khi người nhận nhận được Email, chỉ cần họ nhận được yêu cầu của người nhận cũng xác minh rõ người nhận là ai.

_ Tăng hiểu biết về an toàn Email để phòng chống những cuộc tấn công, phá hoại của tác nhân tiêu cực, cũng như đảm bảo an toàn dữ liệu cá nhân và tổ chức.

_ Dữ liệu cần được mã hoá trước khi gửi, và được giải mã bởi gửi nhận, bằng cách này, cho dù dữ liệu bị đánh cắp, hoặc truyền ra ngoài, thì dữ liệu vẫn rất khó bị khai thác và tiết lộ.

_ Tạo một bộ lọc nội dung khi soạn Emal để kiểm tra nội dung nhạy cảm như là tên đăng nhập, mật khẩu của một tài khoản nào đó, tài liệu mật,… thuộc tổ chức của bạn. Bằng cách nhắc nhở như thế, bạn có thể chủ động mã hoá nó để tăng tính bảo mật loại thông tin này.

_ Đánh giá an ninh:

+) Những nhà phát triển phải xác định các khu vực có khả năng xuất hiện risk như nội dung nhạy cảm trong Email, … => tập trung bảo mật ở những khu vực này hơn

Xác định khả năng vi phạm an ninh, sập =>có thể phá huỷ hoặc hỏng cơ sở dữ liệu, rò rỉ thông tin bí mật, đánh cắp tài sản,… dường như không lường trước được, nên tìm cách ngăn chặn các cuộc tấn công ngay từ đầu;

_ Nâng cao kiến thức chuyên môn để tối ưu và hạn chế rủ ro.

Phương pháp tiếp cận nhiều lớp (không có giải pháp duy nhất)

_ Nhà phát triển phải kiểm soát các chính sách, ràng buộc, đến thiết kế (design), đến thực thi (implement) đến thực hành (operate) và đến tối ưu để hạn chế threat, risk.

_ Xác định ngôn ngữ nào có những framework hỗ trợ về an toàn thông tin hay không.

2. *(4 điểm)* Trình bày các nguyên tắc để đảm bảo an toàn cho các phần mềm ứng dụng của doanh nghiệp?

_ Đảm bảo nguyên tác CIA: confidentiality, integrity, availability

+) Tính bí mật (confidentiality): bảo mật thông tin khỏi những sự truy cập trái phép, bị lọt vào tay của những người không xác thực hoặc một phần mềm khác.

+) Tính toàn vẹn (integrity): liên quan đến duy trì tính nhất quán, độ chính xác và tin cậy đối với dữ liệu của doanh nghiệp trong vòng đời của nó. Khi được chuyển tiếp, dữ liệu sẽ không bị thay đổi. Dữ liệu chỉ được thay đổi bởi những người có thẩm quyền. Việc chỉnh sửa dữ liệu sẽ bị theo dõi.

+) Tính sẵn sàng (availability): thông tin phải luôn trong trạng thái sẵn sàng khi được yêu cầu. Thông tin luôn sẵn sàng trong mọi thời điểm.

_ Minimise attack surface area: giảm thiểu những khu vực có thể bị tấn công.

_ Least privilege: mỗi người chỉ có những quyền củ thể đối với dữ liệu

_ Defence in depth thay vì có một kiểm soát bảo mật cho quyền truy cập của người dùng, bạn sẽ có nhiều lớp xác thực, công cụ kiểm tra bảo mật bổ sung và công cụ ghi nhật ký.

_ Tách biệt các nhiệm vụ bảo mật, khi phân quyền cho các cá nhân thì cũng phải tách biệt nhiệm vụ để đảm bảo tính toàn vẹn và bảo mật.

_ Giữ việc bảo mật ở mức đơn giản: Sử dụng các kiến trúc bảo mật phù hợp, tránh sử dụng những kiến trúc phức tạp để giảm thiểu sai sót.

_ Vá lỗ hổng bảo mật một cách chính xác, phải xác định chính xác risk để sửa chữa nó, có thể design và implement lại hệ thống.

_ Không tin tưởng tuyệt đối vào dịch vụ, luôn kiểm tra tính hợp lệ của dữ liệu mà bên trung gian gửi, tránh bị lộ dữ liệu.

_ Không nên sử dụng cách che dấu để bảo mật dữ liệu vì chúng ta phải đảm bảo khi dữ liệu bị đánh cắp, người đánh cắp vẫn không thể sử dụng hoặc hiểu dữ liệu nó nghĩa là gì.

_ Xử lý lỗi hệ thống một cách an toàn.

Hướng dẫn nộp bài:

- Đặt tên file: ***MSSV_HoTen*_Ktra_PartI** (file word hoặc pdf)
- Nộp bài trên hệ thống utex.hcmute.edu.vn mục **Bài KT tự luận**