Quản trị hệ thống thông tin. Nhóm 1.

51403239 – Lâm Phúc Nghi.

51403417 – Đậu Minh Lượng.

Bài tập chương 7.

1. **Giả sử doanh nghiệp của bạn có một trang web thương mại điện tử bán hàng và chấp nhận thanh toán bằng thẻ tín dụng. Hãy trình bày về các mối đe dọa bảo mật chính đối với trang web này và tác động của chúng. Có thể làm gì để giảm thiểu những mối đe dọa này?**

* Gian lận tài chính:

+ Gian lận thẻ tín dụng:

Dùng thẻ tín dụng bị đánh cắp để mua sản phẩm. Thông thường, địa chỉ giao hàng và địa chỉ thanh toán khác nhau. Giải pháp: cài đặt hệ thống xác minh địa chỉ - AVS (Address verification service). AVS kiểm tra độ khớp giữa các địa chỉ thanh toán do người sử dụng thẻ và địa chỉ thanh toán của chủ thẻ trên hồ sơ ngân hàng.

+ Tin tặc gửi yêu cầu giả mạo hoàn tiền.

* Lừa đảo:

Email giả mạo cửa hàng chứa trang web giả lừa người dùng chia sẻ tài khoản. Giải pháp: triển khai bộ lọc spam phát hiện virus; cập nhật bản vá lỗi bảo mật; cài đặt giải pháp chống virus; lên lịch cập nhật chữ ký, và theo dõi trạng thái chống virus trên các thiết bị trong công ty; mã hóa thông tin quan trọng.

* Tấn công DDoS:

Tấn công DDoS, máy chủ nhận được một lượng lớn các yêu cầu từ nhiều địa chỉ IP không thể theo dõi khiến nó gặp sự cố, gây gián đoạn trang web. Giải pháp: giới hạn số kết nối tại một thời điểm; sử dụng cloudflare; sử dụng Firewall cứng chống tấn công DDoS;…

* Malware:

Cài đặt các chương trình độc hại: phần mềm gián điệp, Trojan, ransomware, worm, adware, spyware, fileless malware, the hybrid attack. Các chương trình có thể lấy dữ liệu. Giải pháp: tránh cài đặt phần mềm không rõ nguồn gốc; cập nhật phần mềm virus…

* Khai thác lỗ hỏng:

+ SQL Injection: tin tặc gửi các biểu mẫu truy vấn truy cập cơ sở dữ liệu, làm hỏng cơ sở dữ liệu bằng mã lây nhiễm, thu thập dữ liệu và sau đó xóa sạch dấu vết.

+ Cross-Site Scripting (XSS): cấy đoạn mã JavaScript độc hại trên trang thương mại điện tử. Những mã độc truy cập cookie của khách hàng.

* Dò mật khẩu bằng brute force. Giải pháp: thay đổi mật khẩu thường xuyên, đảm bảo mật khẩu phức tạp khó đoán.

*Một số biện pháp giảm thiểu những mối đe dọa:*

* HTTPS và chứng chỉ SSL: giao thức HTTPS giữ an toàn cho dữ liệu nhạy cảm của người dùng bằng cách bảo vệ dữ liệu truyền lại giữa server và thiết bị người dùng. SSL (Secure Sockets Layer): tiểu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết được mã hóa giữa máy chủ web và trình duyệt.
* Sử dụng phần mềm chống virus, malware.
* Bảo mật cổng thanh toán: tránh lưu trữ thông tin thẻ tín dụng của khách hàng trên cơ sở dữ liệu. Để bên thứ ba như PayPal và Stripe xử lý các giao dịch thanh toán.
* Đào tạo, hướng dẫn nhân viên và khách hàng: đảm bảo nhân viên và khách hàng được hướng dẫn về những cập nhật mới nhất về việc xử lý dữ liệu người dùng và cách tương tác với trang web một cách an toàn. Xóa thông tin chi tiết nhân viên cũ và thu hồi tất cả quyền truy cập của họ vào hệ thống.

Tham khảo

1. Getastra.com 10 E-commerce Security Threats That Are Getting Stronger By The Day!

<https://www.getastra.com/blog/knowledge-base/ecommerce-security-threats/>

1. Securitybox.vn Tấn công Phishing là gì? Giải pháp chống Phishing.

<https://securitybox.vn/1797/tan-cong-phishing-la-gi-giai-phap-chong-phishing/>

1. Hostingviet.vn 6+ cách phòng chống DDoS cho trang web của bạn.

<https://hostingviet.vn/ba-cach-phong-chong-ddos-cho-trang-web>

1. Digistar.vn Chứng chỉ SSL là gì?

<https://www.digistar.vn/chung-chi-ssl-la-gi/>