ÁP DỤNG CÁC PHƯƠNG PHÁP TIẾP CẬN RỦI RO CÓ CHIẾN LƯỢC TẠI THỊ TRƯỜNG VIỆT NAM
APPLICATION OF STRATEGIC RISK APPROACHES IN VIETNAM MARKET

Viên Thị Ngọc Trâm, Trần Gia Long, Nguyễn Trần Quốc Vỹ, Phạm Khắc An
Trường Đại Học Kinh Tế - Tài Chính UEF

Tóm tắt: *Thương mại điện tử đề cập đến tất cả các loại giao dịch điện tử giữa các bên cho dù đó là giao dịch tài chính hay trao đổi thông tin phi tài chính hoặc các dịch vụ khác. Thương mại điện tử đã biến đổi ngành công nghiệp thương mại mạnh mẽ bằng việc giới thiệu các dịch vụ mua hàng, vận chuyển và các dịch vụ khách hàng tốt hơn. Các dịch vụ kinh doanh này tạo và sử dụng thông tin nhạy cảm như thông tin mua hàng của khách hàng, thông tin tài chính và cá nhân có giá trị cao đối với những kẻ tấn công. Chính vì vậy, chúng tôi đã nhận ra một vấn đề cần được giải quyết lúc này là làm thế nào để đảm bảo tính toàn vẹn về thông tin khách hàng và bảo mật hệ thống thông tin trước những rủi ro tiềm ẩn trong hệ thống thương mại điện tử. Bảo mật hệ thống thương mại điện tử yêu cầu quản lý rủi ro bảo mật có ý thức về các mối đe dọa bảo mật đang phát triển. Công trình nghiên cứu này phân tích và đề xuất việc sử dụng phương pháp STRIDE (phân tích mối đe dọa bảo mật) để hỗ trợ phương pháp ISSRM (Quản lý rủi ro bảo mật hệ thống thông tin) trong việc tiếp cận và quản lý rủi ro bảo mật trong hệ thống thương mại điện tử, trong bài nghiên cứu sẽ đưa ra các yếu tố tại sao phương pháp trên có thể áp dụng tại Việt Nam, cụ thể là Shopee. Kết quả của phương pháp này đưa ra nhận dạng tài sản thương mại điện tử, phân tích mối đe dọa và xác định rủi ro, với quyết định xử lý rủi ro bảo mật.*

Từ khóa: *Thương mại điện tử, STRIDE, ISSRM, Bảo mật thương mại điện tử, Quản lý rủi ro.*

1. MỞ ĐẦU:

Thương mại điện tử đề cập đến tất cả các loại giao dịch điện tử giữa các bên cho dù đó là giao dịch tài chính hay trao đổi thông tin phi tài chính hoặc các dịch vụ khác. Hệ thống thương mại điện tử bao gồm các thành phần (phần mềm, phần cứng, quy trình, dịch vụ và tương tác với hệ thống của bên thứ ba) có tác dụng tạo, phổ biến và thao túng thông tin tài chính để cung cấp các giao dịch và dịch vụ thương mại qua internet. Những thông tin đó bao gồm thông tin tài chính, sản phẩm, khách hàng hoặc đơn đặt hàng cho phép các quy trình cốt lõi của hệ thống. Ngành thương mại điện tử đã phải hứng chịu một số vụ vi phạm an ninh lớn trong những năm gần đây như cuộc tấn công vào Adidas (2018) và cuộc tấn công Ebay (2014). Tác động của những vi

phạm bảo mật này bao gồm đánh cắp danh tính do mất thông tin cá nhân và tài chính của khách hàng, tổn thất tiền tệ cho cả chủ doanh nghiệp và khách hàng, mất lòng tin của khách hàng đối với việc sử dụng thương mại điện tử và mất danh tiếng của công ty. Để ngăn chặn những vi phạm bảo mật như vậy, phân tích mối đe dọa bảo mật và quản lý rủi ro bảo mật được thực hiện (Matulevicius, 2017). Phân tích mối đe dọa bảo mật nhắm mục tiêu các mối đe dọa đối với các hệ thống lợi dụng các lỗ hổng hiện có để gây ra tác động nguy hiểm. Những mối đe dọa bảo mật này gây ra rủi ro bảo mật trong một hệ thống và yêu cầu quản lý.

2. NỘI DUNG:

2.1. Tổng quan

Hiện nay, "Quản lý rủi ro bảo mật trong thương mại điện tử" cũng như việc đảm bảo tuyệt đối những thông tin của khách hàng đang được quan tâm và là mục tiêu, tiêu chuẩn để các doanh nghiệp thương mại điện tử tạo nên sự uy tín và nhận được niềm tin của khách hàng. Năm 2018, "Adidas cảnh báo một số người tiêu dùng về sự cố bảo mật dữ liệu tiềm ẩn" của họ và năm 2014, eBay cũng đã cung cấp cho người dùng một bài báo về "Các câu hỏi thường gặp về Thay đổi mật khẩu eBay", chứng tỏ vấn đề bảo mật luôn luôn được coi trọng ở bất kì doanh nghiệp nào sử dụng thương mại điện tử. Bởi vậy, việc nghiên cứu các yếu tố bảo mật khác nhau trong một hệ thống thông tin thương mại điện mại để từ đó phát hiện và phân tích những rủi ro tiềm năng có thể xảy đồng thời tìm cách khắc phục tác động xấu mà chúng đem lại một cách tối ưu nhất.

Nghiên cứu này sẽ kết hợp hai phương pháp ISSRM và STRIDE để đưa ra những rủi ro cụ thể nhất và đề xuất cách khắc phục chúng. Trong một quy trình mua hàng, chúng tôi lựa chọn quy trình thanh toán (payment) của SHOPEE để phân tích cho nghiên cứu này, bởi đây là một quy trình đặc biệt thú vị, nơi cần có thông tin nhạy cảm về khách hàng, người bán và doanh nghiệp để hoàn tất giao dịch. Các tài sản trong quy trình này đòi hỏi tính bảo mật cao, cần tính bảo mật, tính toàn vẹn và tính sẵn sàng. Quá trình này cung cấp một bề mặt tấn công đáng kể để phân tích mối đe dọa bảo mật và quản lý rủi ro cũng như nghiên cứu trường hợp phức tạp hợp lý.

Mô hình đề xuất gồm: xác định tài sản có liên quan trong một hệ thống thương mại điện tử (SHOPEE), xác định các rủi ro bảo mật, thực hiện các quy trình xử lý rủi ro bảo mật và đưa ra quyết định giảm thiểu những rủi ro đã được phát hiện đó.

2.2. Đề xuất mô hình

Từ tổng quan nghiên cứu, nhóm tác giả đã đề xuất mô hình chính là kết hợp hai phương pháp phân tích mối đe dọa bảo mật – STRIDE

để hỗ trợ một phương pháp quản lý rủi ro bảo mật đã chọn – ISSRM (Quản lý rủi ro bảo mật hệ thống thông tin).

Hình 1. Mô hình nghiên cứu đề xuất

Nhóm quyết định phân tích các yếu tố trong mô hình đề xuất rõ hơn để tiếp cận vấn đề hiệu quả hơn.

(H1) Xác định các tài sản có liên quan cho một hệ thống thương mại điện tử.

Dựa trên mô hình miền của ISSRM[2] có thể xác định được tài sản của một hệ thống thương mại điện tử. Tài sản là bất cứ thứ gì có giá trị và góp phần hoàn thành các mục tiêu của tổ chức. Các tài sản quan trọng của một hệ thống phải được xác định và bảo vệ trong quy trình quản lý rủi ro bảo mật. Bao gồm tài sản kinh doanh và tài sản hệ thống. Tài sản kinh doanh được định nghĩa là thông tin, dữ liệu và quy trình mang lại giá trị cho một tổ chức. Tài sản hệ thống/IS là tài sản hỗ trợ tài sản kinh doanh.

(H2) Xác định các rủi ro bảo mật đối với hệ thống thương mại điện tử.

Từ tổng quan nghiên cứu, quy trình thanh toán Shopee[3] được sử dụng để phân tích rủi ro bảo mật. Các mối đe dọa bảo mật là kết quả của sự tồn tại của các tác nhân đe dọa và các lỗ hổng trong tài sản hệ thống. Một số nội dung hệ thống được chọn để phân tích. Điều này bao gồm Giao diện đăng nhập Shopee, Máy chủ Shopee và Shopee để thể hiện phương pháp tiếp cận dựa trên mối đe dọa. Chúng tôi đã sử dụng cơ sở dữ liệu lỗ hổng CWE[4] (CWE, 2020) để xác định các lỗ hổng tiềm ẩn của các tài sản hệ thống được xem xét.

(H3) Thực hiện các quy trình xử lý rủi ro cho một hệ thống thương mại điện tử.

Dựa vào các yếu tố rủi ro từ phương pháp STRIDE, các yêu cầu bảo mật (SReq) đã được đưa ra cho từng kịch bản rủi ro để đảm bảo hệ thống chống lại từng rủi ro.

Các biện pháp đối phó như vậy bao gồm cơ chế kiểm tra đầu vào, Chặn tài khoản khách hàng, Chấm dứt các phiên khách hàng khác. Các yêu cầu bảo mật được đưa ra để giảm thiểu rủi ro bảo mật được đánh giá theo các đặc điểm chất lượng mà một đặc tả yêu cầu tốt phải tôn trọng (Alexander và Stevens, 2002), (Davis và cộng sự, 1993).

(H4) Đưa ra quyết định giảm thiểu rủi ro đối với những rủi ro được phát hiện.

Nhóm sẽ có cái nhìn tổng quan về các yếu tố bảo mật đó, từ các rủi ro, các biện pháp đã có, nhóm sẽ sử dụng phương pháp research, phân tích, sáng tạo và tổng hợp dữ liệu để đưa ra các quyết định giảm thiểu hợp lý.

2.3. Phương pháp nghiên cứu

Nhóm đi đến quyết định kết hợp tư duy, brainstorming và tham khảo để thực hiện các nghiên cứu đầy đủ và dễ tiếp cận nhất.

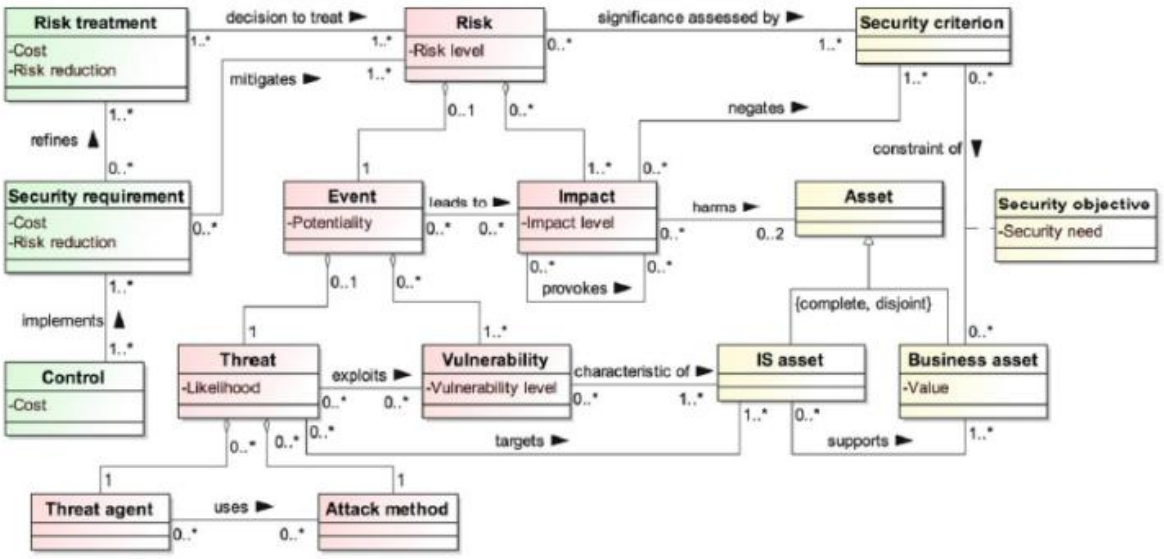
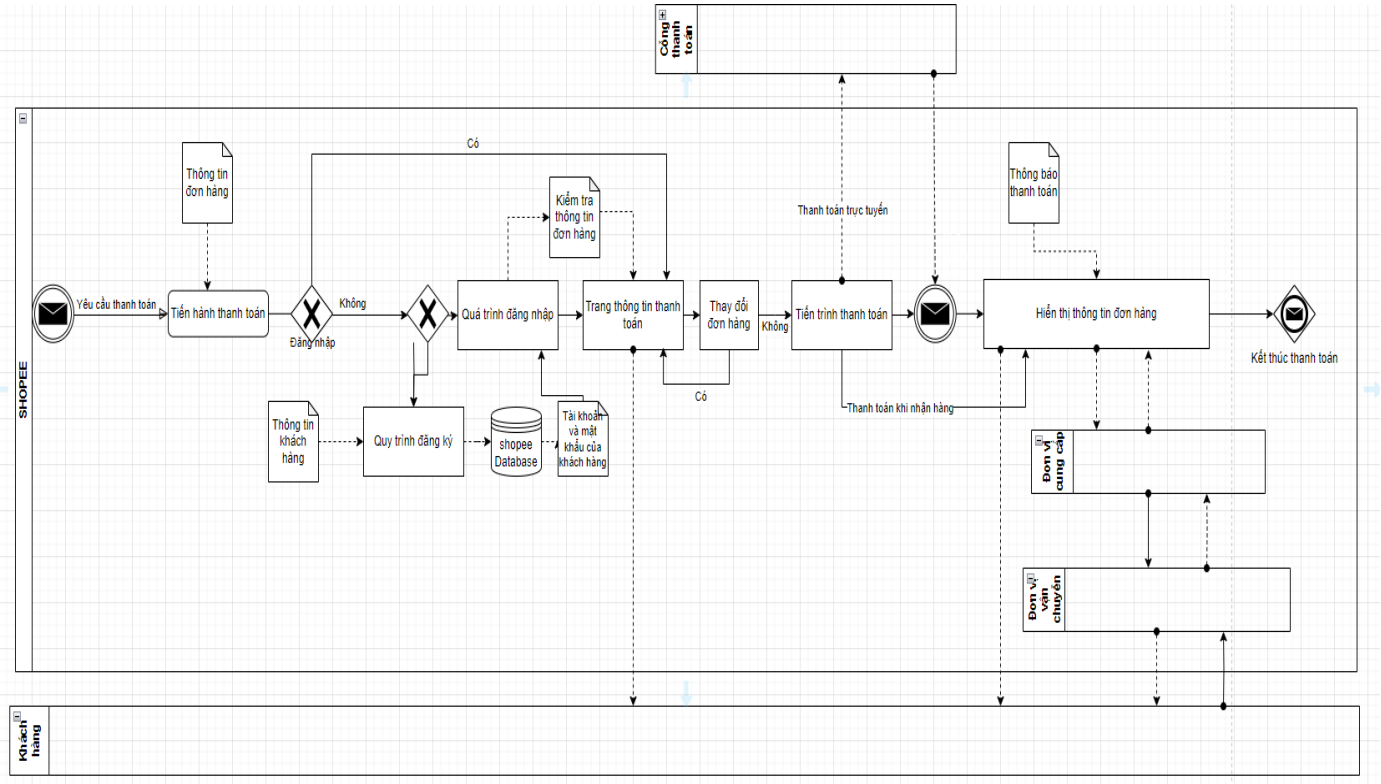


Fig. 1. ISSRM Domain Model, adapted from (Dubois et al., 2010), (Matulevičius, 2017)

Hình 2. Mô hình miền ISSRM

Dựa vào mô hình này, nhóm đi giải quyết vấn đề (H1) là xác định tài sản liên quan của hệ thống thương mại điện tử. Mô hình này gồm 3 nhóm khái niệm chính: tài sản, rủi ro và xử lý rủi ro.

Từ sơ đồ quy trình hệ thống thanh toán này, nhóm đã đưa ra được hai yếu tố quan trọng của hệ thống là: tài sản hệ thống và tài sản kinh doanh được hỗ trợ. Đồng thời đưa ra bốn quá trình đó là yêu cầu đăng nhập, yêu



cầu thanh toán, tạo phiên đăng nhập và nhật ký máy chủ Shopee.

Hình 3: Sơ đồ hệ thống thanh toán.

Tài sản hệ thống	**Tài sản kinh doanh được hỗ trợ**
Giao diện đăng nhập Shopee, Khách hàng, Cơ sở dữ liệu Shopee	Tiến hành thủ tục đăng nhập, Tên đăng nhập và Mật khẩu, Thông tin khách hàng
Máy Chủ Shopee, trang chủ shopee, dữ liệu khách hàng	Dịch vụ Thanh toán trên shopee, Thông tin Đặt hàng Thanh toán
Máy chủ shopee, Khách hàng	ID phiên khách hàng
Cơ sở dữ liệu shopee, Máy chủ shopee	Nhật ký máy chủ ShopeeS

Bảng 1. Bảng tài sản trong chương trình hệ thống Shopee

Từ sơ đồ quy trình thanh toán hình 3 nhóm đã rút ra được là tài sản hệ thống sẽ được hỗ trợ bởi tài sản kinh doanh nên chúng sẽ đi

theo cặp. Như ở mục yêu cầu đăng nhập, tài sản hệ thống sẽ bao gồm: Giao diện đăng nhập Shopee, Khách hàng, Cơ sở dữ liệu Shopee bên cạnh đó tài sản kinh doanh được hỗ trợ sẽ bao gồm: Tiến hành thủ tục đăng nhập, Tên đăng nhập và Mật khẩu, Thông tin khách hàng. Tiếp đến ở mục 2 sẽ là yêu cầu thanh toán, tài sản hệ thống của yêu cầu đăng nhập sẽ bao gồm: Máy Chủ Shopee, trang chủ shopee, dữ liệu khách hàng và tài sản kinh doanh được hỗ trợ sẽ bao gồm: Dịch vụ Thanh toán trên shopee, Thông tin Đặt hàng Thanh toán. Mục thứ 3 sẽ là tạo phiên khách hàng sau khi đăng nhập, tài sản hệ thống sẽ có máy chủ shopee và thông tin khách hàng bên cạnh đó tài sản kinh doanh được hỗ trợ sẽ có ID Phiên khách hàng. ID phiên khách hàng sẽ được cấp mỗi khi khách hàng đăng nhập vào Shopee. Cuối cùng sẽ là nhật ký máy chủ Shopee đối với tài sản hệ thống sẽ bao gồm: Cơ sở dữ liệu shopee, Máy chủ shopee và tài sản kinh doanh được hỗ trợ sẽ có nhật ký máy chủ Shopee để ghi lại các lần đăng nhập, đăng xuất của khách hàng.

Tiếp theo, để giải quyết vấn đề (H2) chính là bằng cách sử dụng CWE để nhóm xác định lỗ hổng tiềm năng của hệ thống SHOPEE, kết quả của việc áp dụng CWE này là bảng dưới đây

Tài sản hệ thống	**Lỗ hổng tiềm ẩn**	**CWE2020**
Cửa hàng trực tuyến shopee	Quyền truy cập: người mua hàng đăng nhập trên một thiết bị lạ và quên đăng xuất; hoặc người dùng bị hack tài khoản dẫn đến các đơn đặt hàng ảo. Thông tin trên hệ thống: người dùng bị lộ thông tin cá nhân như tên, số điện thoại, địa chỉ,... dẫn đến bị làm phiền, hoặc nghiêm trọng hơn là đe dọa qua các phương thức liên hệ cá nhân.	CWE-521
Thanh toán của shopee	Rất nhiều trường hợp người mua đã tạo lệnh thanh toán xong và số dư bị trừ tiền nhưng trên Shopee lại không xác nhận đơn hàng đã "thanh toán thành công". Cũng có trường hợp, cùng một đơn hàng nhưng người mua lại bị trừ tiền nhiều lần.	CWE-20

Máy chủ Shopee	Mặc dù Shopee đã có cam kết bảo mật thông tin người dùng nhưng vẫn xảy ra những vụ để lộ thông tin khách hàng. Shopee gặp rất nhiều trường hợp về giả mạo đơn hàng của Shopee. khách hàng bị lừa đảo bởi những đơn hàng mà người kia biết rõ bạn đã mua gì, shop nào, địa chỉ và thông tin chi tiết, khiến khách hàng không đề phòng mà thanh toán. Có những trường hợp khách hàng bị ăn cắp thông tin để đặt hàng trên Shopee mặc dù khách hàng không hề tự tay đặt những đơn hàng đó.	CWE-117 CWE-285 CWE-770

Bảng 2. Lỗ hổng trong hệ thống của Shopee

Dựa vào **CWE** mà nhóm em đã đưa ra được các lỗ hổng của Shopee. *CWE là common weakness enumeration* là liệt kê điểm yếu chung. Dựa vào thư viện CWE 2020 chúng em đã đưa ra được những lỗ hổng tiềm năng trong hệ thống shopee. Trước tiên nhóm đã chia ra 3 loại tài sản chính có tiềm năng lỗ hổng là cửa hàng trực tuyến của Shopee, trang thanh toán của shopee và máy chủ shopee. Ở mỗi loại tài sản sẽ có từng lỗ hổng tiềm năng khác nhau, như ở cửa hàng trực tuyến Shopee sẽ có các lỗ hổng tiềm năng như quyền truy cập: người mua hàng đăng nhập trên một thiết bị lạ và quên đăng xuất; hoặc người dùng bị hack tài khoản dẫn đến các đơn đặt hàng ảo. Thông tin trên hệ thống: người dùng bị lộ thông tin cá nhân như tên, số điện thoại, địa chỉ,... dẫn đến bị làm phiền, hoặc nghiêm trọng hơn là đe dọa qua các phương thức liên hệ cá nhân. Đối với trang thanh toán của Shopee sẽ xuất hiện hai lỗi khách hàng thường gặp như là rất nhiều trường hợp người mua đã tạo lệnh thanh toán xong và số dư bị trừ tiền nhưng trên Shopee lại không xác nhận đơn hàng đã "thanh toán thành công". Cũng có trường hợp, cùng một đơn hàng nhưng người mua lại bị trừ tiền nhiều lần. Cuối cùng là máy chủ Shopee đây là nơi có nhiều lỗ hổng nhất và dễ bị tấn công nhất, những lỗ hổng tiêu biểu như mặc dù Shopee đã có cam kết bảo mật thông tin người dùng nhưng vẫn xảy ra những vụ để lộ thông tin khách hàng. Shopee gặp rất nhiều trường hợp về giả mạo đơn hàng của Shopee. khách hàng bị lừa đảo bởi những đơn hàng mà người kia biết rõ bạn đã mua gì, shop nào, địa chỉ và thông tin chi tiết, khiến khách hàng không đề phòng mà thanh toán. Có những trường hợp khách hàng bị ăn cắp thông tin để đặt hàng trên Shopee mặc dù khách hàng không hề tự tay đặt những đơn hàng đó.

Tiếp theo là chúng em sẽ áp dụng STRIDE để phân tích các rủi ro và đưa ra các yêu cầu bảo mật cần thiết với bảng dưới đây:

Loại mối đe dọa	Phân tích tác động	Rủi ro bảo mật	Yêu cầu bảo mật
Spoofing	ST1: Có những trường hợp khách hàng bị ăn cắp thông tin để đặt hàng trên Shopee mặc dù khách hàng không hề tự tay đặt những đơn hàng đó. V: Thông tin từ máy chủ Shopee dễ bị xâm nhập . Impact: Mất tính bảo mật ID của khách hàng	SR1: Kẻ tấn công sẽ giả mạo địa chỉ email, tên, số điện thoại, SMS hoặc URL trang web Shopee để đánh lừa khách hàng làm cho họ nghĩ rằng đây là trang chính thức của Shopee và khách hàng sẽ điền thông tin cá nhân của mình vào dẫn đến việc tài khoản của khách hàng bị lấy mất và dẫn đến mất tính bảo mật ID của khách hàng. SR2 : man in the attack	SR1.SReq1: Sẽ có thông báo về số điện thoại khách hàng khi tài khoản của khách hàng đăng nhập trên thiết bị lạ. Khi thông báo đến Email hoặc số điện thoại nội dung đều được ghi rõ làm người dùng có thể biết được mã xác thực đến để làm gì (ví dụ: Mã xác thực để đăng nhập trên thiết bị mới, Mã xác thực để đổi mật khẩu,...) SR1.SReq2: Sử dụng giao thức mã hóa an toàn SR1.SReq3: Webshop sẽ không cho phép các phiên người dùng đồng thời trùng lặp, bắt nguồn từ các máy khác nhau.
Tampering	TT1:Trong thời gian vừa rồi, Shopee gặp rất nhiều trường hợp về giả mạo đơn hàng của Shopee, khách hàng bị lừa đảo bởi những đơn hàng mà người kia biết rõ bạn đã mua gì, shop nào, địa chỉ và thông tin chi tiết, khiến khách hàng không đề phòng mà thanh toán. V: Giả mạo đơn hàng của máy chủ Shopee Impact: mất tính toàn vẹn của đơn đặt hàng Shopee	TR1: Kẻ tấn công sẽ dùng các loại mã để sửa đổi thông tin của người mua và người bán(địa chỉ giao hàng và số tiền phải thanh toán, ID tài khoản ngân hàng) dẫn đến mất tính toàn vẹn .	TR1.SReq1: Sau khi khách hàng tiến hành thanh toán hóa đơn sẽ được lưu cố định lại và không được sửa đổi đơn hàng đó. TR1.SReq2: Shopee sẽ lưu thông tin các đơn hàng trước đó của khách nếu có sự thay đổi diễn ra sẽ thông báo lại cho khách hoặc người bán qua phương thức xác thực đã được quy định trước. TR1.SReq3: Shopee ngăn chặn tham nhũng trái phép thông tin đơn đặt hàng

Repudiation	RT1: Khi đơn hàng **đã được thực hiện** những kẻ tấn công phủ nhận việc mua hàng và từ chối thanh toán. Hay việc kẻ tấn công sẽ từ chối trong nhận việc thay đổi thông tin đơn hàng cho một giao dịch trực tuyến và từ chối trách nhiệm. V: Nhật ký máy chủ Shopee không trung hòa đúng cách Impact: Mất tính toàn vẹn của máy chủ Shopee	RR1: Từ chối thanh toán (Payment repudiation): Kẻ tấn công từ chối công nhận và thanh toán các giao dịch đã được thực hiện. Ví dụ, người mua có thể phủ nhận việc mua hàng và từ chối thanh toán, dẫn đến mất tiền của người bán.	RR1.SReq1: Shopee sẽ sử dụng mã hóa nhằm ngăn chặn việc truy cập và sửa đổi thông tin trái phép từ bên ngoài vào cơ sở dữ liệu được lưu trữ. .
Information disclosure	IT1: người dùng bị lộ thông tin cá nhân như tên, số điện thoại, địa chỉ,... dẫn đến bị làm phiền, hoặc nghiêm trọng hơn là đe dọa qua các phương thức liên hệ cá nhân. V: Thiếu xác thực đầu vào và mã hóa của giao diện Shopee. Impact: mất tính toàn vẹn bảo mật của Shopee	IR1: Kẻ tấn công sẽ chiết xuất thông tin của khách hàng bằng cách đánh cấp thông tin của Shopee như thẻ ngân hàng, địa chỉ nhà, chứng minh thư, số điện thoại… và qua đó sẽ đe dọa qua các liên hệ cá nhân dẫn đến mất đi tính toàn vẹn của bảo mật shopee.	R1.SReq1: Shopee xác thực người dùng (Authentication) xác minh thông tin đăng nhập của một người dùng hoặc thiết bị cố gắng truy cập vào một hệ thống. IR1.SReq2: Chắc chắn rằng việc thông báo lỗi sẽ không chứa các thông tin, dữ liệu nhạy cảm. IR1.SReq3: Chỉ sử dụng những cách thức hoạt động và thủ tục lưu trữ được số hóa để truy vấn. IR1.SReq4 : Các thông tin cá nhân nhạy cảm của khách hàng sẽ bị mã hóa 1 phần khi hiển thị

Denial of service	DT1: Kẻ tấn công làm cạn kiệt tài nguyên của dịch vụ thanh toán trên Shopee bằng cách tạo nhiều yêu cầu thanh toán. V: Thiếu sự phân bổ nguồn lực không giới hạn ở trang thanh toán Shopee Impact: Mất tính khả dụng của trang thanh toán Shopee	DR1: Kẻ tấn công làm tràn ngập máy chủ Shopee với nhiều yêu cầu thanh toán bằng các tài khoản giả mạo và làm cạn kiệt dịch vụ thanh toán Shopee bằng cách khai thác việc phân bổ tài nguyên Không giới hạn hoặc Điều tiết của máy chủ Shopee, dẫn đến việc dịch vụ thanh toán Shopee mất khả dụng.	DR1.SReq1: Các thành phần Shopee sẽ có các giới hạn về quy mô được định cấu hình DR1.SReq2: Shopee sẽ có các hành vi được chấp nhận được chỉ định khi phân bổ tài nguyên đạt đến giới hạn. DR1.SReq3: Khách hàng bắt buộc phải xác minh là con người khi thực hiện thanh toán.
Elevation of privilege	ET1: Do cấu trúc mật khẩu bảo mật của shopee còn yếu nên kẻ tấn công có thể dễ dàng khai thác để có toàn quyền đối với thông tin của khách hàng V: Do mật khẩu của Shopee còn yếu nên xác thực được cấu hình trong cửa hàng trực tuyến. Impact: mất đi tính toàn vẹn và bảo mật trong thông tin khách hàng.	ER1: Kẻ tấn công khai thác xác thực dựa trên mật khẩu yếu được định cấu hình trong Shopee Để giành toàn bộ đặc quyền đối với Thông tin khách hàng dẫn đến mất Tính bảo mật và tính toàn vẹn của Thông tin khách hàng.	ER1.SReq1: Cấu hình chính sách về mật khẩu mạnh hơn đưa ra các yêu cầu về mật khẩu (ví dụ: phải có ký tự trong mật khẩu) ER1.SReq2: Đưa ra giới hạn về thời gian xác thực tài khoản và số lần cố gắng đăng nhập. ER1.SReq3: Phương pháp xác thực hai yếu tố khi đăng nhập trên thiết bị lạ

Bảng 3: Bảng phân tích tác động và yêu cầu bảo mật của Shopee

Như đã được nói ở trên STRIDE sẽ bao gồm 6 rủi ro spoofing, tampering, repudiation,information disclosure và elevation of privilege.

Đầu tiên nói đến spoofing rủi ro spoofing của shopee SR1: Kẻ tấn công sẽ giả mạo địa chỉ email, tên, số điện thoại, SMS hoặc URL trang web Shopee để đánh lừa khách hàng làm cho họ nghĩ rằng đây là trang chính thức của Shopee và khách hàng sẽ điền thông tin cá nhân của mình vào dẫn đến việc tài khoản của khách hàng bị lấy mất. Tác động/impact

mà spoofing gây ra là mất tính bảo mật ID của khách hàng dẫn đến ST1: Có những trường hợp khách hàng bị ăn cắp thông tin để đặt hàng trên Shopee mặc dù khách hàng không hề tự tay đặt những đơn hàng đó. Những yêu cầu bảo mật mà nhóm em đã đưa ra gồm SR1.SReq1: Sẽ có thông báo về số điện thoại khách hàng khi tài khoản của khách hàng đăng nhập trên thiết bị lạ. Khi thông báo đến Email hoặc số điện thoại nội dung đều được ghi rõ làm người dùng có thể biết được mã xác thực đến để làm gì (ví dụ: Mã xác thực để đăng nhập trên thiết bị mới, Mã xác thực để đổi mật khẩu,...). SR1.SReq2: Sử dụng giao thức mã hóa an toàn. SR1.SReq3: Webshop sẽ không cho phép các phiên người dùng đồng thời trùng lặp, bắt nguồn từ các máy khác nhau.

Mối rủi ro thứ 2 sẽ là tampering ở trường hợp của shopee TR1: Kẻ tấn công sẽ dùng các loại mã để sửa đổi thông tin của người mua và người bán(địa chỉ giao hàng và số tiền phải thanh toán, ID tài khoản ngân hàng). Tác động/impact sẽ làm mất tính toàn vẹn của đơn đặt hàng Shopee dẫn đến TT1:Trong thời gian vừa rồi, Shopee gặp rất nhiều trường hợp về giả mạo đơn hàng của Shopee, khách hàng bị lừa đảo bởi những đơn hàng mà người kia biết rõ bạn đã mua gì, shop nào, địa chỉ và thông tin chi tiết, khiến khách hàng không đề phòng mà thanh toán. Những yêu cầu bảo mật cần thiết cho rủi ro tampering này là TR1.SReq1: Sau khi khách hàng tiến hành thanh toán hóa đơn sẽ được lưu cố định lại và không được sửa đổi đơn hàng đó. TR1.SReq2: Shopee sẽ lưu thông tin các đơn hàng trước đó của khách nếu có sự thay đổi diễn ra sẽ thông báo lại cho khách hoặc người bán qua phương thức xác thực đã được quy định trước. TR1.SReq3: Shopee ngăn chặn tham nhũng trái phép thông tin đơn đặt hàng.

Mối rủi ro thứ 3 sẽ là Repudiation hay còn gọi là khước từ nhưng ở trường hợp của Shopee là RR1: Từ chối thanh toán (Payment repudiation): Kẻ tấn công từ chối công nhận và thanh toán các giao dịch đã được thực hiện. Ví dụ, người mua có thể phủ nhận việc mua hàng và từ chối thanh toán, dẫn đến mất tiền của người bán. Tác động/impact mà repudiation để lại là mất tính toàn vẹn của máy chủ Shopee cũng như niềm tin của người bán dẫn đến RT1: Khi đơn hàng đã được thực hiện những kẻ tấn công phủ nhận việc mua hàng và từ chối thanh toán. Hay việc kẻ tấn công sẽ từ chối trong nhận việc thay đổi thông tin đơn hàng cho một giao dịch trực tuyến và từ chối trách nhiệm. Những yêu cầu bảo mật mà nhóm đã đưa ra gồm RR1.SReq1: Shopee sẽ sử dụng mã hóa nhằm ngăn chặn việc truy cập và sửa đổi thông tin trái phép từ bên ngoài vào cơ sở dữ liệu được lưu trữ.

RR1.SReq2: Xác định chắc chắn rằng đầu ra của dữ liệu sẽ được trung hòa đúng cách.

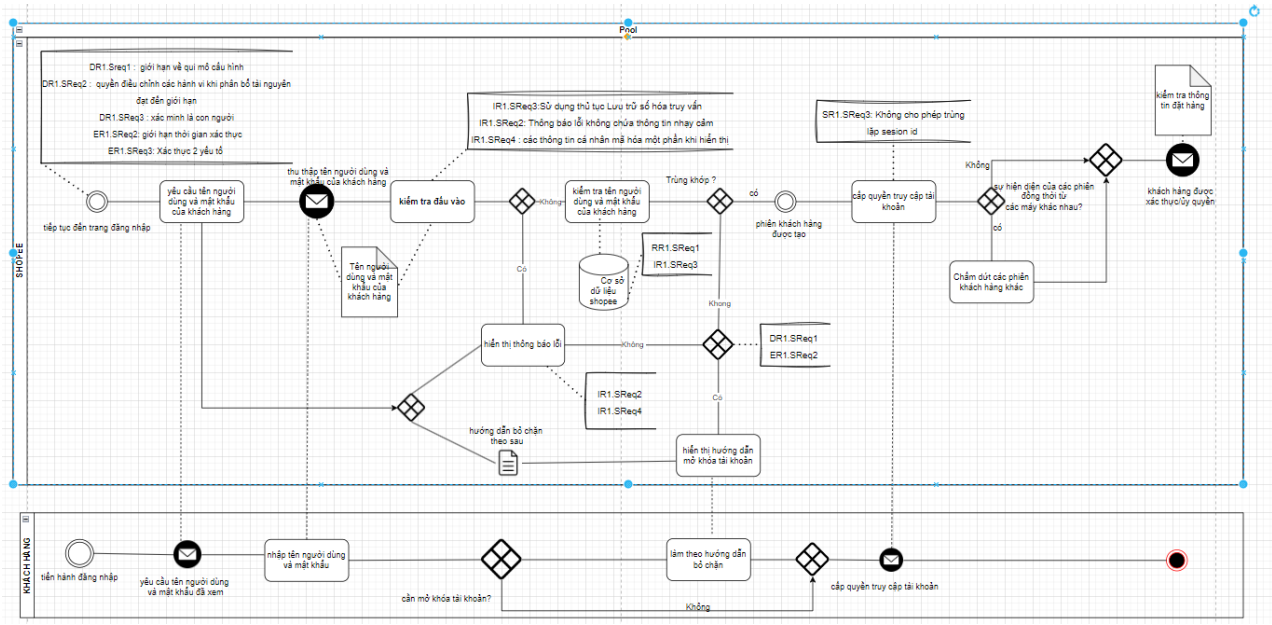
Rủi ro thứ 4 sẽ là Information disclosure với rủi ro này của shopee IR1: Kẻ tấn công sẽ chiết xuất thông tin của khách hàng bằng cách đánh cấp thông tin của Shopee như thẻ ngân hàng, địa chỉ nhà, chứng minh thư, số điện thoại… và qua đó sẽ đe dọa qua các liên hệ cá nhân dẫn đến mất đi tính toàn vẹn của bảo mật shopee. Tác động/impact mà rủi ro này gây ra làm mất tính toàn vẹn bảo mật của Shopee dẫn đến IT1: người dùng bị lộ thông tin cá nhân như tên, số điện thoại, địa chỉ,... dẫn đến bị làm phiền, hoặc nghiêm trọng hơn là đe dọa qua các phương thức liên hệ cá nhân. Yêu cầu bảo mật mà nhóm đã đưa ra gồm IR1.SReq1: Shopee xác thực người dùng (Authentication) xác minh thông tin đăng nhập của một người dùng hoặc thiết bị cố gắng truy cập vào một hệ thống. IR1.SReq2: Chắc chắn rằng việc thông báo lỗi sẽ không chứa các thông tin, dữ liệu nhạy cảm. IR1.SReq3: Chỉ sử dụng những cách thức hoạt động và thủ tục lưu trữ được số hóa để truy vấn. IR1.SReq4 : Các thông tin cá nhân nhạy cảm của khách hàng sẽ bị mã hóa một phần khi hiển thị.

Rủi ro thứ 5 sẽ là Denial of service (DOS), ở rủi ro này DR1: Kẻ tấn công làm tràn ngập máy chủ Shopee với nhiều yêu cầu thanh toán bằng các tài khoản giả mạo và làm cạn kiệt dịch vụ thanh toán Shopee bằng cách khai thác việc phân bổ tài nguyên Không giới hạn hoặc điều tiết của máy chủ Shopee, dẫn đến việc dịch vụ thanh toán Shopee mất khả dụng. Tác động/impact của rủi ro này sẽ mất tính khả dụng của trang thanh toán Shopee dẫn đến DT1: Kẻ tấn công làm cạn kiệt tài nguyên của dịch vụ thanh toán trên Shopee bằng cách tạo nhiều yêu cầu thanh toán. Yêu cầu bảo mật cho rủi ro này bao gồm DR1.SReq1: Các thành phần Shopee sẽ có các giới hạn về quy mô được định cấu hình. DR1.SReq2: Shopee sẽ có các hành vi được chấp nhận được chỉ định khi phân bổ tài nguyên đạt đến giới hạn. DR1.SReq3: Khách hàng bắt buộc phải xác minh là con người khi thực hiện thanh toán.

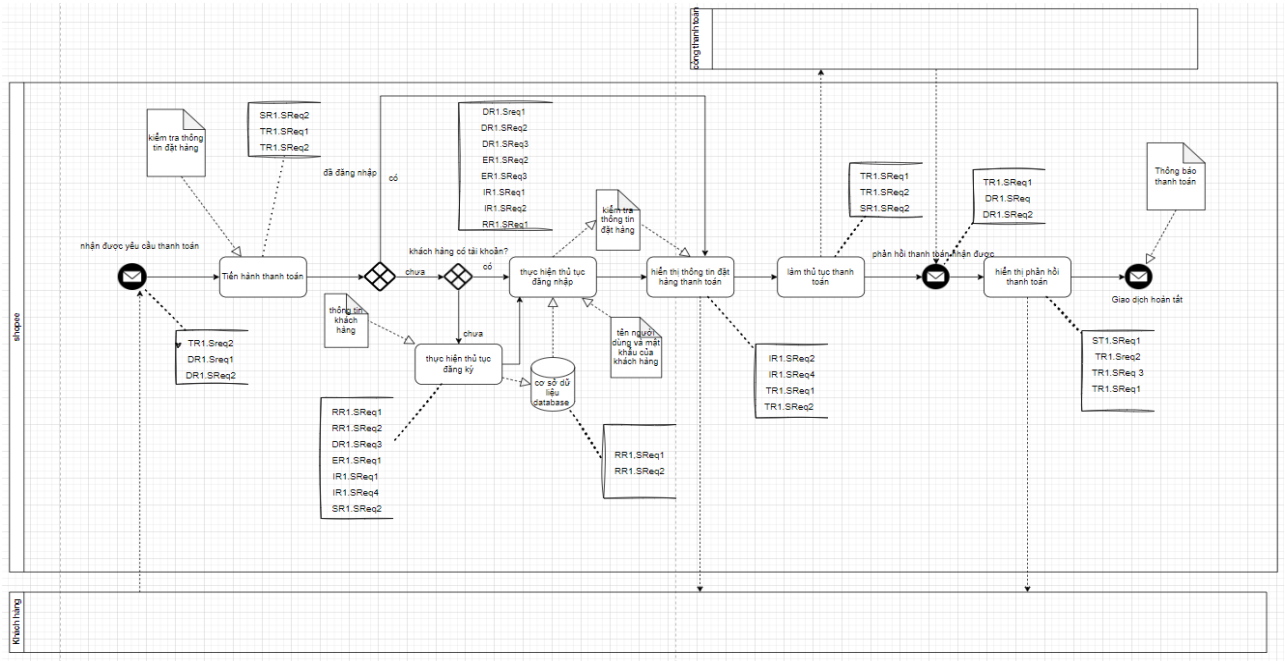
Rủi ro thứ 6 là elevation of privilege, ở rủi ro này Shopee sẽ bị ER1: Kẻ tấn công khai thác xác thực dựa trên mật khẩu yếu được định cấu hình trong Shopee Để giành toàn bộ đặc quyền đối với thông tin khách hàng. Tác động/impact của rủi ro này dẫn đến mất đi tính toàn vẹn bảo mật của khách hàng dẫn đến ET1: cấu trúc mật khẩu bảo mật của shopee còn yếu nên kẻ tấn công có thể dễ dàng khai thác để có toàn quyền đối với thông tin của khách hàng. Yêu cầu bảo mật mà nhóm em đưa ra cho Shopee là ER1.SReq1: Cấu hình chính sách về mật khẩu mạnh hơn đưa ra các yêu cầu về mật khẩu (ví dụ: phải có ký tự trong mật khẩu). ER1.SReq2: Đưa ra giới hạn

về thời gian xác thực tài khoản và số lần cố gắng đăng nhập. ER1.SReq3: Phương pháp xác thực hai yếu tố khi đăng nhập trên thiết bị lạ

Sơ đồ biện pháp đối phó rủi ro trong quá trình đăng nhập và quá trình thanh toán:



Hình 4. Sơ đồ biện pháp đối phó rủi ro trong quá trình đăng nhập



Hình 5. Sơ đồ biện pháp đối phó rủi ro trong quá trình thanh toán

2.3.1.Xây dựng thang đo

Trong bài nghiên cứu thang đo này chỉ mức độ ưu tiên của từng loại tấn công nhằm vào hệ thống. Được xác định theo các yếu tố như:

- Tác động của loại hình tấn công đó (tác động gây ảnh hưởng lớn đến nhiều khách hàng hay tác động vào hệ thống.)
- Các cách thức, phương pháp để đối phó với các loại tấn công.
- Hậu quả của các loại hình tấn công.

Rủi ro	**Mức độ ưu tiên**
Giả mạo thương hiệu	Thấp
Giả mạo tham số	Cao
Tấn công khước từ	Trung
Rủi ro lấy cắp thông tin	Thấp
Tấn công từ chối dịch vụ	Cao
Khai thác lỗ hổng	Thấp

Đối với rủi ro đầu tiên **giả mạo thương hiệu** mức ưu tiên trong bài nghiên cứu này là thấp, trong khoảng thời gian qua các tình trạng giả mạo website giả mạo tin nhắn vẫn còn phổ biến nhưng đa số người dùng đã cảnh giác hơn về loại dùng này và ảnh hưởng của việc giả mạo đều được các tổ chức cảnh báo khách hàng cũng như việc rà soát thông tin của cơ quan chức năng cũng tích cực hoạt động nhằm giảm thiểu việc **giả mạo thương hiệu** nhằm mục đích chiếm đoạt tài sản.

Với rủi ro **giả mạo tham số(Tampering)** là một trong những cách thức tấn công tinh vi nhằm qua mặt khách hàng cũng như hệ thống khi kẻ tấn công sẽ can thiệp vào dòng chảy dữ liệu của khách hàng và hệ thống nhằm chiếm đoạt quyền, thay đổi thông tin, thu thập thông tin và giả mạo thông tin, nhằm lợi dụng những điều đó để lừa đảo khách hàng hay sử dụng các thông tin khách hàng nhằm mục đích xấu, với loại tấn công này rất khó để người dùng có thể phát hiện.

Tấn công khước từ loại hình tấn công này hiệu quả không quá cao và cũng không mang lại hậu quả quá bất lợi nhưng nó vẫn nằm trong danh sách những rủi ro có thể xảy ra trong hệ thống bán hàng,

Lấy cắp thông tin Khác với tấn công giả mạo thông tin để thu thập dữ liệu, lấy cắp thông tin nhằm vào cơ sở dữ liệu của hệ thống nhằm chiếm đoạt thông tin của hàng ngàn người dùng trong đó để sử dụng cho mục đích mua bán hoặc một số các loại hình lừa đảo,...do những năm gần đây các hệ thống bảo mật ngày càng tối ưu nên gần như hiện

tại kẻ tấn công khó có thể tiếp cận đến những thông tin quan trọng của khách hàng.

Tấn công từ chối dịch vụ loại hình tấn công phổ biến nhiều kẻ tấn công sử dụng nó nhằm mục đích hạ bệ các website và hệ thống đối thủ làm hệ thống đó tê liệt và mất đi 1 chức năng hoạt động nào đó, một loại hình tấn công rất dễ dàng có thể thực hiện nhưng mang lại hậu quả rất nghiêm trọng khi hệ thống bị tê liệt cùng theo đó là những thiệt hại về mặt tài chính cũng như sự uy tín của doanh nghiệp.

Khai thác lỗ hổng nhằm tìm kiếm lỗ hổng trong bảo mật dữ liệu người dùng hoặc sự sơ ý của người dùng dẫn đến việc kẻ tấn công có thể khai thác nó để chiếm quyền kiểm soát tài khoản cá nhân của khách hàng từ đó thực hiện vi gây hậu quả xấu đối với người sử dụng cũng như hệ thống.

2.3.2. Phương pháp thu thập và phân tích dữ liệu

Tổng thể đối tượng nghiên cứu là hai phương pháp ISSRM và STRIDE, chính sách bảo mật SHOPEE, quy trình thanh toán SHOPEE, điều khoản sử dụng của SHOPEE. Nhóm thu thập thông tin từ trang chủ shopee, dữ liệu đầu ra đầu vào dựa trên bài báo về hai phương pháp trên.

Sử dụng công cụ mindmap và diagram để tổng hợp kiến thức, sơ đồ hóa thông tin thu thập được, rút ngắn khối lượng thông tin và dữ liệu dư thừa. Tổng hợp bảng đánh giá, thang đo kết hợp tư duy.

2.4. Phân tích kết quả

Bằng phương pháp tiếp cận lỗ hổng ISSRM và phương pháp tiếp cận rủi ro STRIDE nhóm em đã tổng hợp được những rủi ro mà hệ thống thanh toán shopee có thể gặp phải sắp xếp mức độ ưu tiên và đưa ra các phương pháp giảm thiểu rủi ro.

Những rủi ro có thể gặp phải:

Giả mạo thông tin hoặc URL trang web Shopee dẫn đến tài khoản của khách hàng bị lấy mất và mất tính bảo mật ID của khách hàng.

Kẻ tấn công dùng các loại mã để sửa đổi thông thanh toán, giả mạo các loại đơn làm cho giống với những đơn mình đã đặt dẫn đến mất tính toàn vẹn của đơn đặt hàng gây ảnh hưởng đến hệ thống thông tin và trải nghiệm của người dùng.

Từ chối thanh toán (Payment repudiation) Kẻ tấn công từ chối công nhận và thanh toán các giao dịch đã được thực hiện làm ảnh hưởng đến công việc kinh doanh của các thương nhân trên sàn.

Kẻ tấn công sẽ chiết xuất thông tin của khách hàng bằng cách đánh cấp thông tin của Shopee như thẻ ngân hàng, địa chỉ nhà, chứng minh thư, số điện thoại… và qua đó sẽ đe dọa qua các liên hệ cá nhân dẫn đến mất đi tính

toàn vẹn của bảo mật shopee và sự an toàn của người dùng.

Kẻ tấn công làm cạn kiệt tài nguyên của dịch vụ thanh toán trên Shopee bằng cách tạo nhiều yêu cầu thanh toán. Dẫn đến nhiều người mua hàng không thể thanh toán, các thương nhân và shopee phải chịu các chi phí do thiệt hại gây ra.

Kẻ tấn công lợi dụng lỗ hổng bảo mật do cấu hình bảo mật yếu của shopee từ đó chiếm quyền kiểm soát thông tin người dùng mạo danh để trục lợi hoặc gây ảnh hưởng đến các người dùng khác.

Qua các rủi ro được xác định từ phương pháp STRIDE nhóm em đã xác định và phân loại được các rủi ro thông qua mức độ nguy hại mà rủi ro đó gây ra. Từ đó đưa ra các phương pháp như trên để giảm thiểu thiệt hại có thể xảy ra.

KẾT LUẬN:

Quản lý rủi ro bằng cách tiếp cận có mục tiêu để phân tích mối đe dọa bảo mật khi sử dụng sự kết hợp giữa 2 phương pháp STRIDE và ISSRM trong quy trình thanh toán tại thị trường Việt Nam. Dựa trên tài liệu "Security Risk Management in E-commerce Systems: A Threat-driven Approach" của Baltic J. Modern Computing và một số tài liệu liên quan, tài liệu đã xác thực tính khả thi khi kết hợp hai phương pháp STRIDE và ISSRM để tiếp cận rủi ro trên các mối đe dọa được đánh giá bởi các chuyên gia bảo mật và họ đã đưa ra được kết quả rất khả thi. Với phương pháp trên STRIDE sẽ là phương pháp hỗ trợ cho ISSRM bằng cách lập mô hình các mối đe dọa để phân loại, tìm ra nguồn gốc, đưa ra những điều kiện bảo mật và những đề xuất đối phó để có thể quản lý những rủi ro về bảo mật. Và chúng tôi đã sử dụng phương pháp trên để áp dụng cho một doanh nghiệp tại Việt Nam (Shopee) để phân tích việc quản lý rủi ro của doanh nghiệp này và đã đưa ra được kết quả về thông tin tài sản hệ thống và các lỗ hổng tiềm ẩn liên quan và dựa trên một số các yêu cầu về bảo mật nhằm giảm thiểu các ảnh hưởng của rủi ro đó. loại mối đe dọa đưa ra một số rủi ro sẽ gặp phải. Nên bài nghiên cứu đã đánh giá được mức độ khả thi và những lợi ích mà phương pháp kết hợp giữa phương pháp tiếp cận lỗ hổng ISSRM và phương pháp tiếp cận rủi ro STRIDE mang lại.

Một số khuyến nghị: Đối với những hệ thống càng lớn càng phức tạp thì theo đó là càng có nhiều rủi ro ở mức độ khác nhau, tùy thuộc vào mỗi hệ thống có các cách thức kiểm tra và đưa ra yêu cầu về bảo mật khác nhau, mỗi thị trường đều có những rủi ro khác nhau vậy nên các doanh nghiệp nên có các phương pháp tiếp cận rủi ro phù hợp với hệ thống.

Phương pháp tiếp cận rủi ro trên không chỉ mang lại lợi ích cho các hệ thống

doanh nghiệp mà còn giúp người dùng có thể hiểu hơn về một số cách thức mà bên tấn công có thể khai thác lỗ hổng để khách hàng tránh những trường hợp gây ra thiệt hại không mong muốn.

TÀI LIỆU THAM KHẢO

1. *eBay Inc. Staff (2014) Frequently Asked Questions on eBay Password Change*
2. *Herzogenaurach/Portland (28/06/2018) ADIDAS ALERTS CERTAIN CONSUMERS OF POTENTIAL DATA SECURITY INCIDENT*
3. *Nguyễn Hưng (26/06/2021) IP spoofing là gì? Tìm hiểu về các loại IP spoofing*
4. *Baltic J. Modern Computing. Security Risk Management in E-commerce Systems: A Threat-driven Approach, Vol. 8, Iss.2*