VẤN ĐỀ AN NINH MẠNG TRONG HOẠT ĐỘNG DỊCH VỤ NGÂN HÀNG ĐIỆN TỬ CỦA VIETINBANK

● LÝ THỊ THÚY

TÓM TẮT:

Nhằm không ngừng nâng cao, bảo vệ chất lượng dịch vụ ngân hàng, đặc biệt là các sản phẩm dịch vụ ngân hàng điện tử trước nguy cơ rủi ro từ các tấn công của tội phạm công nghệ cao. Trong nhiều năm qua, VietinBank luôn ưu tiên công tác đảm bảo an toàn công nghệ thông tin, bảo đảm an ninh thông tin, dữ liệu của ngân hàng. Tuy nhiên, công tác bảo đảm an toàn bảo mật hiện nay đang trở nên ngày càng phức tạp, đối mặt với nhiều khó khăn và thách thức. Bài viết đề cập về những thành tựu mà VietinBank đã đạt được nhờ các sản phẩm dịch vụ ngân hàng điện tử và những thách thức, khó khăn của an ninh mạng đối với dịch vụ này.

Từ khóa: Vietinbank, ngân hàng điện tử, an ninh mạng.

I. Đặt vấn đề

Ngày nay, công nghệ thông tin đang ngày càng hát triển ở Việt Nam, kèm theo đó là sự phát triển ủa smartphone. Chỉ cần một chiếc smartphone và nternet, khách hàng đã có thể giao dịch được hiều hình thức khác nhau như mua sắm online, ặt vé máy bay, xem phim, khách sạn... Dựa theo êu chí: "Khách hàng là trung tâm trong mọi hoạt ộng của VietinBank. VietinBank cam kết mang ến những sản phẩm, dịch vụ và phong cách phục ụ đồng nhất; một VietinBank duy nhất đáp ứng ất nhất mọi nhu cầu phù hợp của khách hàng". Do ó, VietinBank đã cho ra một loại hình thức mới đó à ngân hàng điện tử (E-Banking). Thay vì đến gân hàng giao dịch như trước đây, thì bây giờ chỉ ới một chiếc điện thoại thông minh, khách hàng ã có thể giao dịch như chuyển tiền, gửi tiết kiệm, anh toán hóa đơn điện nước, ..

Tuy nhiên công nghệ tiện ích này lại kéo theo iều vấn đề phải đau đầu đặc biệt là vấn đề về an nh mạng. Đây cũng là mối nguy hại cho dịch vụ ngân hàng điện tử nói riêng và ngành Ngân hàng nói chung. Nếu như có lỗi trong hệ thống an ninh mạng thì thông tin của khách hàng sẽ bị rò rỉ, kéo theo đó khách hàng có thể bị mất tiền oan hoặc phải chi trả một khoản nợ lớn mà họ không hề hay biết. Từ đó, uy tín của VietinBank sẽ bị suy giảm và VietinBank có thể sẽ phải đối diện với nhiều mối nguy khác. Đó là lý do vì sao mà cần phải tìm ra những giải pháp phòng chống và giải quyết vấn đề này.

II. Thực trạng phát triển ngân hàng điện tử ở Vietinbank

E-Banking là dịch vụ ngân hàng điện tử dùng để truy vấn thông tin tài khoản và thực hiện các giao dịch chuyển khoản, thanh toán qua mạng internet. E-Banking cho phép khách hàng thực hiện giao dịch trực tuyến mà không cần đến ngân hàng. Chỉ cần một chiếc máy vi tính hoặc điện thoại di động có kết nối internet và mã truy cập do ngân hàng cung cấp, khách hàng đã có thể thực hiện các giao dịch với ngân hàng mọi lúc mọi nơi một cách an toàn.

Ngân hàng điện tử cung cấp cho cá nhân những tiện ích sau:

* VietinBank iPay.
* iPay Mobile.
* SMS Banking.
* Bank Plus.

Ngân hàng điện tử cung cấp cho doanh nghiệp tiện ích sau:

* VietinBank eFast.

Năm 2015, VietinBank đầu tư nâng cao chất lượng các sản phẩm, dịch vụ, nhằm đáp ứng nhu cầu khách hàng cá nhân. Sự tín nhiệm và tin dùng của khách hàng được ghi nhận từ số lượng khách hàng, số lượng giao dịch và doanh số giao dịch trên kênh ngân hàng điện tử ngày càng tăng nhanh. Sản phẩm, dịch vụ của VietinBank được ghi nhận với Danh hiệu Sao Khuê 2015 cho ứng dụng VietinBank iPay Mobile App.

Năm 2016, VietinBank gây được tiếng vang với sự ra đời của ứng dụng VietinBank iPay Mobile App phiên bản 3.0. Ứng dụng đã đạt danh hiệu Sao Khuê, là ứng dụng ngân hàng điện tử được yêu thích, giải pháp ngân hàng điện tử tốt nhất do các tổ chức uy tín trao tặng.

Năm 2017, VietinBank đã đồng loạt cho triển khai các tính năng mới: Nộp thuế điện tử; Mua vé xem phim trên ứng dụng; Kích hoạt và khóa thẻ online; Tích lũy điểm thưởng cho Khách hàng thân thiết (Loyalty), đăng ký trực tuyến...

Ngoài ra, với tính năng QRPay, VietinBank tiếp tục mở rộng chuỗi merchant thanh toán cho các nhu cầu giải trí, mua sắm tại các chuỗi cửa hàng, rạp Chiếu phim Quốc gia hay mua hàng trực tuyến bằng mã QR (tại VnShop). Đặc biệt, VietinBank còn là ngân hàng đầu tiên và duy nhất cung cấp dịch vụ thanh toán QRPay cho cước viễn thông VNPT tại 63 tỉnh/thành và cước di động mạng VinaPhone.

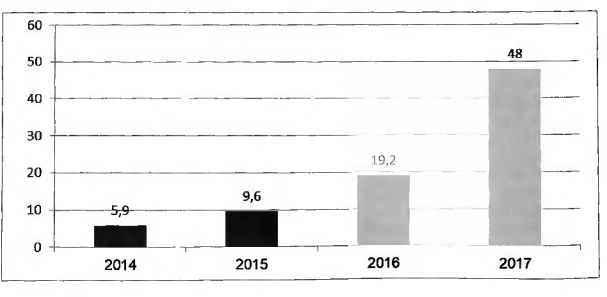
Việc triển khai những tính năng mới kết hợp đẩy mạnh các chương trình khuyến mãi đã thu hút sự quan tâm của đông đảo khách hàng, số lượng khách hàng VietinBank iPay đã tăng mạnh. Tính đến hết tháng 10/2017, số lượng khách hàng mới tăng gấp 2,5 lần so với cả năm 2016, số lượng khách hàng tải và kích hoạt ứng dụng VietinBank iPay Mobile cũng tăng gấp đôi so với cả năm 2016. Biểu đồ 1.

III. Những thách thức khó khăn của an ninh mạng mà các ngân hàng nói chung, trong đó có Vietinbank đang phải đối diện trong sự phát triển ngân hàng điện tử

Ngành Ngân hàng với đặc thù đến 90% là áp dụng hệ thống công nghệ thông tin cho hoạt động kinh doanh, vấn đề bảo mật và an toàn thông tin theo đó mang tính sống còn. Mọi sự cố về an toàn thông tin có thể gây thiệt hại nặng nề về mất tài chính và uy tín của doanh nghiệp.

Trong năm 2015, đã có khoảng 2 triệu máy tính bị tấn công bằng mã độc nhằm mục đích lấy cắp tài khoản cá nhân (thống kê từ hãng Gartner - Công ty Tư vấn và Nghiên cứu công nghệ thông tin tại Mỹ). Phần lớn khách hàng được hỏi đều

Biểu đồ 1: Số lượng giao dịch trên kênh Vietinbank E-Banking tăng trưởng qua các năm, từ năm 2014 - 2017



thừa nhận dịch vụ ngân hàng ngày càng hiện đại và tiện ích hơn nhưng họ cũng bày tỏ sự lo lắng khi giao dịch trực tuyến qua các ứng dụng trên thiết bị di động sẽ ảnh hưởng tới việc bảo mật tài sản cá nhân.

Tại Việt Nam, thời gian qua tình hình an ninh thông tin cũng diễn biến rất phức tạp, tội phạm công nghệ cao (trong nước và quốc tế) gia tăng nhiều hình thức tấn công nguy hiểm vào các hạ tầng thông tin trọng yếu của quốc gia và các lĩnh vực kinh tế quan trọng. Hoạt động ngân hàng tại Việt Nam đang nổi lên các vấn đề an ninh thông tin sau:

* Việt Nam nằm trong nhóm 10 nước có tỷ lệ gia tăng lừa đảo trực tuyến cao nhất thế giới;

* Xuất hiện một số đường dây mua bán, sử dụng trái phép thông tin thẻ tín dụng của người nước ngoài để mua hàng online, thanh toán trực tuyến tại Việt Nam;

* Hệ thống máy ATM của các ngân hàng trở thành mục tiêu tấn công của tội phạm công nghệ cao là người nước ngoài như ăn cắp thông tin thẻ ATM của khách hàng, tạo thẻ giả để rút tiền;

* Tội phạm lợi dụng hệ thống thanh toán trực tuyến để rửa tiền hoặc cá đô, đánh bạc có tổ chức với quy mô lớn qua mạng internet. *(Biểu đồ 2).*

Qua bảng số liệu, có thể thấy rằng dịch vụ ngân hàng trực tuyến và kỹ thuật số là dịch vụ mà tội phạm công nghệ nhắm vào nhiều nhất. Tin tặc nhắm vào hệ thống dịch vụ này bởi đây là nơi lưu giữ thông tin bảo mật của nhiều khách hàng, nếu có điều gì xảy ra sẽ ảnh hưởng trực tiếp đến ngân hàng và khách hàng. Đây là con số đáng quan tâm của hệ thống an ninh mạng ngành Ngân hàng.

Tại ngày An toàn thông tin năm 2017, đại diện của VNISA đã công bố kết quả khảo sát hiện trạng, đánh giá chỉ số An toàn thông tin năm 2017 đối với các nhóm doanh nghiệp, theo đó ngành Ngân hàng hiện tại là nhóm có chỉ số an toàn thông tin cao nhất, tuy nhiên chỉ số này mới dừng ở mức 59.9%, vẫn là mức trung bình.

IV. Giải pháp đảm bảo an toàn an ninh mạng tại Vietinbank

1. Đối với ngân hàng

Xây dựng chiến lược và giải pháp an ninh thông tin:

- Tăng cường khả năng giám sát, vận hành an toàn, ổn định cho hệ thống hạ tầng công nghệ thông tin thông qua các trung tâm quản lý tập trung của từng tổ chức.

- Tổ chức hệ thống kiểm toán nội bộ giám sát sự tuân thủ các quy trình, quy định quản lý vận hành hệ thống hạ tầng công nghệ thông tin.

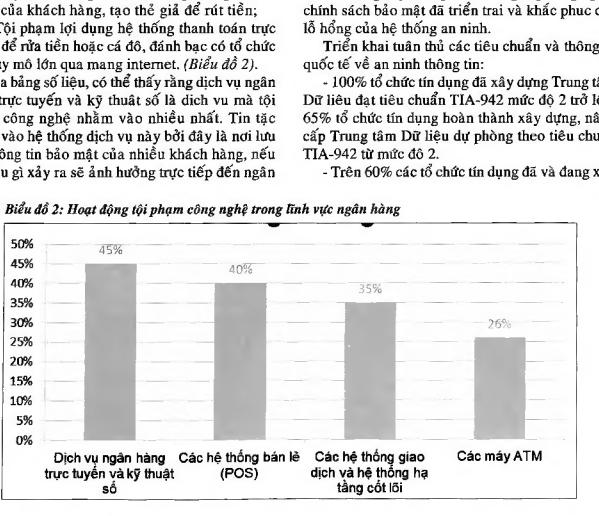
- Thường xuyên cập nhật, nâng cấp công nghệ, chính sách bảo mật đã triển trai và khắc phục các lỗ hổng của hệ thống an ninh.

Triển khai tuân thủ các tiêu chuẩn và thông lệ quốc tế về an ninh thông tin:

- 100% tổ chức tín dụng đã xây dựng Trung tâm Dữ liệu đạt tiêu chuẩn TIA-942 mức độ 2 trở lên, 65% tổ chức tín dụng hoàn thành xây dựng, nâng cấp Trung tâm Dữ liệu dự phòng theo tiêu chuẩn TIA-942 từ mức độ 2.

- Trên 60% các tổ chức tín dụng đã và đang xây

Biểu đồ 2: Hoạt động tội phạm công nghệ trong lĩnh vực ngân hàng



dựng hệ thống quản lý an toàn bảo mật thông tin theo tiêu chuẩn quốc tế ISO 27001 và triển khai chuẩn an ninh dữ liệu thẻ (PCI DSS). Trong đó, có hơn 20% tổ chức tín dụng đã lấy được chứng chỉ đạt tiêu chuẩn này.

Triển khai tuân thủ các tiêu chuẩn về thông lệ quốc tế về an ninh thông tin:

- Ngân hàng đã có chính sách tuyển dụng, đãi ngộ, sử dụng hợp lý đội ngũ cán bộ công nghệ thông tin cũng như an ninh thông tin nhằm thu hút được các nhân tài, phục vụ lâu dài cho ngân hàng.

- Thường xuyên đào tạo và đào tạo lại đội ngũ cán bộ chuyên trách về công nghệ thông tin ngân hàng, đủ năng lực tiếp nhận, chuyển giao công nghệ hiện đại và làm chủ được khoa học kỹ thuật trong thời kỳ mới, đủ khả năng thiết kế và sản xuất những gói phần mềm chuyên dụng cho hoạt động ngân hàng, bảo đảm chất lượng và an toàn.

- Thường xuyên phổ cập kiến thức công nghệ thông tin cho đội ngũ cán bộ quản lý và cán bộ nghiệp vụ ngân hàng theo yêu cầu phát triển của kỹ thuật công nghệ mới cũng như nâng cao nhận thức về an ninh thông tin cho cán bộ ngân hàng để phòng ngừa, giảm thiểu các rủi ro, sự cố từ phía người dùng.

Ngoài ra, ngân hàng có thể thực hiện một số nhiệm vụ, giải pháp cơ bản:

- Tăng cường giáo dục cán bộ, nhân viên trong ngân hàng nâng cao phẩm chất đạo đức, trách nhiệm nghề nghiệp, ý thức chấp hành pháp luật, các quy định, quy trình nội bộ của đơn vị.

- Nâng cao tinh thần cảnh giác, ngăn ngừa mọi diễn biến phức tạp có thể xảy ra ảnh hưởng đến cán bộ, tài sản và uy tín hoạt động của ngân hàng.

- Tăng cường đầu tư cơ sở vật chất, hệ thống công nghệ thông tin, điều kiện phương tiện làm việc, bảo đảm phục vụ tốt cho công tác bảo đảm an ninh, an toàn hoạt động ngân hàng.

2. Đối với khách hàng

Phần mềm độc hại được thiết kế bắt chước 20 phần mềm ứng dụng ngân hàng sử dụng trên điện thoại ở Australia, New Zealand, Thổ Nhĩ Kỳ và có thể mô phỏng màn hình đăng nhập của Paypal, Skype, Ebay và Whatsapp. Phần mềm này chặn tên đăng nhập và mật khẩu hoặc số tài khoản và mật khẩu của người sử dụng khi họ đăng nhập hệ thống. Sau đó, nếu ngân hàng sử dụng hệ thống xác nhập kép để gửi một mã số thông qua tin nhắn tới điện thoại của người đăng ký tài khoản đang đăng nhập, phần mềm này sẽ chặn tin nhắn và gửi nội dung này tới cho tin tặc.

Khách hàng cần cẩn trong trong việc sử dụng các ứng dụng ngân hàng trên điện thoại. Các chuyên gia cảnh báo khi khách hàng sử dụng điện thoại chạy hệ điều hành Android đăng nhập tài khoản qua một phần mềm nhái, thông tin ngân hàng sẽ bị đánh cắp và hệ thống bảo vệ an ninh bị ngăn chặn.

Theo một quan chức của Google, những người sử dụng điện thoại chạy hệ điều hành Android không nên tải bất cứ phần mềm ứng dụng nào từ internet, chỉ tải ứng dụng từ các trang có nguồn đáng tin cậy.

Ngoài ra, khách hàng cũng cần chú ý:

- Không trả lời thông báo e-mail hoặc pop-up yêu cầu cung cấp thông tin cá nhân và các tài khoản của bạn.

- Kiểm tra URL khi truy cập vào các trang web. Phải chắc chắn rằng mình đang truy cập vào một trang web đáng tin cậy. Những URL lừa đảo có nội dung dễ gây nhầm lẫn với các URL của trang web thật.

- Sử dụng phần mềm antivirus, tường lửa và luôn luôn cập nhật chúng.

- Không gửi các thông tin các nhân hoặc tài chính qua e-mail.

- Kiểm tra thẻ tín dụng và sao kê tài khoản ngân hàng ngay sau khi bạn nhận được thông báo trừ tiền trong tài khoản.

- Hãy thận trọng về việc mở hoặc tải về bất kỳ tập tin, liên kết từ e-mail, tin nhắn trên mạng xã hội.

- Sử dụng bộ lọc thư rác để hạn chế các e-mail lừa đảo.

- Cập nhật các trình duyệt để kiểm tra lại danh sách các trang web lừa đảo được biết đến và có thể ngăn lưu trữ các tập tin cookie không an toàn.

- Sử dụng các phương pháp xác thực an toàn ví dụ như dùng phương pháp xác minh hai bước, mỗi khi người dùng đăng nhập hệ thống phải gửi thông tin xác nhận tới người dùng qua điện thoại để xác thực lần nữa, như vậy, ngay cả khi hacker chiếm được thông tin về tài khoản người dùng thì chúng không thể giả mạo người dùng sử dụng tài khoản đó ■

TÀI LIỆU THAM KHẢO:

1. Giáo trình Quản trị ngân hàng - PGS. TS. Nguyễn Đăng Dờn.

2. www.vietinbank.vn

3. www.investor.vietinbank.vn

4. www.thebank.vn

5. www.news.bankcardvn.com

6. www.securitybox.vn

Ngày nhận bài: 21/03/2018
Ngày phản biện đánh giá và sửa chữa: 31/03/2018
Ngày chấp nhận đăng bài: 10/04/2018

Thông tin tác giả:
ThS. LÝ THỊ THÚY
Khoa Tài chính Ngân hàng - Trường Đại học Kinh tế Kỹ thuật Công nghiệp
Email: ltthuy@uneti.edu.vn

NETWORK SECURITY ISSUES IN E-BANKING SERVICES OF VIETINBANK

● MA. LY THI THUY
Faculty of Banking and Finance
University of Economic and Technical Industries

ABSTRACT:

To continuously improve and protect the quality of banking services, especially electronic banking products and services are under the risk of high technology crime attacks, VietinBank has always prioritized the work of ensuring the security of information technology, ensuring the security of information and data of the bank. However, security is now becoming increasingly complex, facing many difficulties and challenges. This article discusses what VietinBank has achieved thanks to the electronic banking products and the challenges of network security for this service.

Keywords: Vietinbank, electronic banking, network security.