NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
CỤC CÔNG NGHỆ TIN HỌC

Số: 758/CNTH8
V/v tăng cường, đảm bảo an toàn thông tin đối với Hệ thống SWIFT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 10 tháng 06 năm 2016

Kính gửi: - Các tổ chức tín dụng;
- Các chi nhánh ngân hàng nước ngoài.

Trong thời gian qua, tình hình tội phạm mạng tấn công vào hệ thống tài chính ngân hàng, đặc biệt là hệ thống thanh toán quốc tế SWIFT (Hệ thống SWIFT) có nhiều diễn biến phức tạp, đã tác động và ảnh hưởng đến hoạt động của hệ thống Ngân hàng.

Qua rà soát và đánh giá, Cục Công nghệ tin học - Ngân hàng Nhà nước nhận thấy trong quản trị, vận hành và sử dụng Hệ thống SWIFT có một số rủi ro như sau:

- Rủi ro về quy trình đối với nghiệp vụ thanh toán SWIFT: chưa ban hành hoặc đã ban hành các quy trình đối với các nghiệp vụ liên quan trong Hệ thống SWIFT nhưng tính thực thi chưa cao và không có sự kiểm soát tuân thủ. Ví dụ: cho mượn tài khoản người dùng; có thành viên SWIFT chỉ mua 1 license concurrent hoặc bố trí nhân sự chưa hợp lý nên không đảm bảo tách biệt nhân sự giữa việc tạo tin điện và kiểm duyệt; thực hiện đối chiếu tra soát tin điện không thường xuyên hoặc không kiểm soát kỹ; ...

- Rủi ro trong việc tích hợp và triển khai Hệ thống SWIFT:

+ Một số đơn vị đang thuê đối tác cung cấp dịch vụ thanh toán SWIFT, tuy nhiên không có biện pháp quản lý, giám sát dịch vụ đảm bảo an toàn, bảo mật.

+ Một số đơn vị triển khai tích hợp hệ thống khác (như corebank) với Hệ thống SWIFT sử dụng giải pháp kết nối không đảm bảo tính xác thực dẫn đến phần mềm độc hại hoặc một máy nghiệp vụ khác có thể gửi tin điện gian lận vào Hệ thống SWIFT.

- Rủi ro trong cấu hình Hệ thống SWIFT:

+ Không giới hạn số lượng máy chủ được phép kết nối với mạng SWIFT (SWIFTNet).

+ Không thiết lập kiểm duyệt tin điện trước khi gửi sang SWIFTNet.

+ Thiết lập Relationship Management Application (RMA) kết nối với các đơn vị không còn là đối tác (counterparty's BIC).

- Xác thực đăng nhập Hệ thống SWIFT và kiểm duyệt (authozire) tin điện: Hiện tại phần lớn chỉ thông qua tên đăng nhập và mã khóa bí mật. Do đó trong trường hợp đơn vị không thiết

lập độ khó của mã khóa bí mật của tài khoản người dùng hoặc tài khoản đặc quyền của ứng dụng, hệ điều hành và cơ sở dữ liệu của Hệ thống SWIFT không được quản lý và kiểm soát hợp lý dẫn đến lộ lọt thông tin tài khoản, tin tặc có thể lợi dụng để truy cập thực hiện giao dịch gian lận và sửa đổi cơ sở dữ liệu trực tiếp, xóa các nhật ký, cài đặt thêm các phần mềm trái phép, thay đổi cấu hình hệ thống, ...

+ Không thiết lập thời gian timeout của Hệ thống SWIFT hoặc có nhưng thời gian timeout quá dài.

- Rủi ro về yếu tố con người: cán bộ quản trị, vận hành và sử dụng không được phổ biến quy trình, không được đào tạo về nhận thức an toàn thông tin.

- Các rủi ro khác:

+ Không kiểm soát, giới hạn các máy trạm thực hiện nghiệp vụ được phép truy cập vào Hệ thống SWIFT.

+ Các máy trạm thực hiện nghiệp vụ SWIFT có thể truy cập mạng Internet hoặc kết nối tới các vùng mạng không an toàn; người dùng có thể cài đặt phần mềm mới và chỉnh sửa ở mức hệ điều hành; không cài đặt phần mềm phòng chống mã độc hại; không kiểm soát kết nối với các thiết bị ngoại vi.

Qua phân tích các rủi ro trên, Cục Công nghệ tin học - Ngân hàng Nhà nước đề nghị các đơn vị đang sử dụng hệ thống thanh toán SWIFT triển khai thực hiện các công việc:

- Ban hành các quy trình, quy định trong vận hành hệ thống SWIFT, tối thiểu phải có các nội dung sau:

+ Quy định trong một giao dịch:

• Đối với giao dịch thủ công, một giao dịch thanh toán cần có sự tham gia thực hiện của tối thiểu 3 người: người tạo điện, người kiểm tra và người kiểm duyệt;

• Đối với giao dịch tự động từ hệ thống ngân hàng lõi (corebanking) chuyển sang Hệ thống SWIFT, Cục Công nghệ tin học - Ngân hàng Nhà nước khuyến cáo phải qua bước kiểm duyệt trên Hệ thống SWIFT trước khi tin điện được gửi tới SWIFTNet. Trường hợp các đơn vị xây dựng quy trình chuyển tự động không qua bước kiểm duyệt trên hệ thống SWIFT cần rà soát toàn bộ quy trình, hạ tầng kỹ thuật và chịu trách nhiệm về các rủi ro (nếu có).

+ Thực hiện tra soát, đối chiếu, kiểm tra để phát hiện sớm sự sai lệch thông tin của các tin điện giữa Hệ thống SWIFT với hệ thống corebanking của đơn vị; giữa Hệ thống SWIFT của đơn vị với các đối tác.

+ Phân công và quy định rõ trách nhiệm của cán bộ quản trị, vận hành và sử dụng Hệ thống SWIFT.

+ Quy định bộ phận kiểm tra, báo cáo việc tuân thủ các quy trình, quy định liên quan đến Hệ thống SWIFT đã ban hành.

- Đối với các đơn vị đang thuê đối tác cung cấp dịch vụ thanh toán SWIFT, cần có kế hoạch chuyển Hệ thống SWIFT về đơn vị để trực tiếp quản lý và thiết lập các biện pháp đảm bảo an toàn thông tin cho hệ thống.

- Nghiên cứu, triển khai giải pháp kết nối giữa hệ thống khác với Hệ thống SWIFT nhằm đảm bảo an toàn, tính xác thực và tính toàn vẹn của tin điện.

- Rà soát, tối ưu cấu hình Hệ thống SWIFT nhằm tăng cường an toàn thông tin trong quản trị, vận hành SWIFT:

- Giới hạn các máy chủ trong Hệ thống SWIFT được phép kết nối sang SWIFTNet.

+ Đánh giá Hệ thống SWIFT theo tài liệu KB tip 5020788 - Security Guidance for Alliance và thực hiện khắc phục các rủi ro phát hiện được đồng thời nghiên cứu, triển khai các khuyến nghị an ninh bảo mật của SWIFT (tham khảo tại địa chỉ: https://www2.swift.com/uhbonline/books/protected/en_uk/aa_7_1_10_sec_guid/index.htm)

+ Tăng cường độ mạnh trong xác thực đăng nhập: thiết lập độ khó cho mã khóa bí mật của tài khoản người dùng; thiết lập thời gian timeout hợp lý; nghiên cứu việc tích hợp OTP hoặc PKI trong xác thực đăng nhập hoặc giao dịch.

+ Rà soát các tài khoản người dùng và quản trị, kết nối trong hệ thống đảm bảo người sử dụng được phân quyền đúng, loại bỏ những tài khoản không còn sử dụng, thay đổi mã khóa bí mật các tài khoản mặc định của hệ thống và đồng thời có biện pháp quản lý, bảo vệ phù hợp đối với các tài khoản đặc quyền như tài khoản thuộc các Profile SuperKey, SuperVisor, MsgEntry, MsgPartner; Administrator/Root của hệ điều hành; tài khoản quản trị cơ sở dữ liệu...

+ Rà soát các RMA và loại bỏ các RMA không sử dụng.

- Rà soát tối ưu các cấu hình hệ thống liên quan hoặc trang bị các giải pháp an ninh bảo mật hoặc dịch vụ khác để tăng cường an toàn thông tin đối với Hệ thống SWIFT:

+ Kiểm soát, giới hạn các máy trạm thực hiện nghiệp vụ kết nối vào Hệ thống SWIFT và tăng cường các biện pháp an ninh bảo mật cho các máy này, cụ thể như: đặt các máy này vào vùng mạng riêng được bảo vệ; cài đặt và cập nhật thường xuyên bản vá hệ điều hành, phần mềm phòng chống mã độc hại; hạn chế truy cập internet; phân quyền cho tài khoản người dùng đủ để người dùng sử dụng ứng dụng nghiệp vụ, không thể cài đặt phần mềm mới hoặc thay đổi hệ thống ở mức hệ điều hành; giới hạn sử dụng các thiết bị ngoại vi...

+ Nghiên cứu triển khai các giải pháp nhằm phát hiện và phòng chống các giao dịch gian lận trên Hệ thống SWIFT; phân tích và cảnh báo các giao dịch bất thường dựa trên nhật ký Hệ thống SWIFT và các hệ thống liên quan.

- Cán bộ quản trị, vận hành và sử dụng Hệ thống SWIFT được đào tạo nhận thức về an toàn thông tin, biết cách phòng tránh các rủi ro như: phát hiện các email, website độc hại; trách nhiệm trong việc quản lý và sử dụng tài khoản người dùng, thông tin nhạy cảm.

Cục Công nghệ tin học - Ngân hàng Nhà nước đề nghị các đơn vị tổ chức thực hiện.

Mọi thông tin chi tiết xin liên hệ: Phòng An ninh thông tin - Cục Công nghệ tin học, 64 Nguyễn Chí Thanh - Đống Đa - Hà Nội, số điện thoại 04.38354775, fax: 04.38358135, email: cnth8@sbv.gov.vn./.

Trân trọng./.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Phan Thái Dũng

Nơi nhận:
- Như trên;
- Cục trưởng (để b/c);
- Lưu CNTH, CNTH8.