NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
Số: 769 /CNTT6
V/v Hướng dẫn tăng cường an toàn thông tin hệ thống phần mềm CITAD tại thành viên Hệ thống TTĐTLNH

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

Hà Nội, ngày 01 tháng 6 năm 2022

Kính gửi:
- Các thành viên Hệ thống Thanh toán điện tử liên ngân hàng;
- Công ty Cổ phần Thanh toán Quốc gia Việt Nam.

Ngày 07/02/2022, Cục Công nghệ thông tin (Cục CNTT) có Công văn số 163/CNTT6 gửi các thành viên/đơn vị thành viên trực tiếp của Hệ thống Thanh toán điện tử liên ngân hàng, Tổ chức chủ trì hệ thống bù trừ điện tử (sau đây gọi tắt là thành viên) cho ý kiến góp ý đối với "Hướng dẫn tăng cường an toàn thông tin hệ thống phần mềm CITAD tại thành viên Hệ thống TTĐTLNH" (sau đây gọi tắt là Hướng dẫn ATTT).

Sau khi tổng hợp, tiếp thu ý kiến của các thành viên, Cục CNTT ban hành Hướng dẫn ATTT (nội dung Hướng dẫn được đăng tải tại địa chỉ *https://www.sbv.gov.vn* chuyên mục *Thanh toán & ngân quỹ -> Các hệ thống thanh toán trong nền kinh tế ->Hệ thống thanh toán điện tử liên ngân hàng*).

Đề nghị các Ông/Bà Tổng Giám đốc (Giám đốc) thông báo và chỉ đạo các đơn vị liên quan triển khai thực hiện Hướng dẫn ATTT. Quá trình thực hiện nếu có vướng mắc, xin liên hệ Cục Công nghệ thông tin (hotrotinhoc@sbv.gov.vn) để phối hợp xử lý.

Trân trọng cảm ơn sự phối hợp công tác của Quý thành viên./.

Nơi nhận:
- Như trên;
- PTĐ Phạm Tiến Dũng; (để b/c)
- Cục trưởng;
- Lưu CNTT, CNTT4, CNTT5, CNTT8, CNTT6 (TTSon).

Đính kèm:
- Hướng dẫn ATTT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

Phan Thái Dũng

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

CỤC CÔNG NGHỆ THÔNG TIN

HƯỚNG DẪN

TĂNG CƯỜNG AN TOÀN THÔNG TIN HỆ THỐNG PHẦN MỀM CITAD TẠI THÀNH VIÊN HỆ THỐNG THANH TOÁN ĐIỆN TỬ LIÊN NGÂN HÀNG QUỐC GIA

(Kèm theo Công văn số 769/CNTT6 ngày 01 tháng 6 năm 2022 của Cục trưởng Cục Công nghệ thông tin)

Năm 2022

MỤC LỤC

I. MỤC ĐÍCH, PHẠM VI ÁP DỤNG 1
1. Mục đích 1
2. Phạm vi áp dụng 1
II. NGUYÊN TẮC KIỂM SOÁT AN TOÀN THÔNG TIN 1
III. PHẠM VI KIỂM SOÁT AN TOÀN THÔNG TIN 3
IV. TỔNG QUAN CÁC KIỂM SOÁT AN TOÀN THÔNG TIN 6
V. CHI TIẾT CÁC YÊU CẦU 7
1. Bảo vệ an toàn môi trường hoạt động 7
1.1. Kiểm soát truy cập Internet 7
1.1.1. Hạn chế truy cập Internet 7
1.2. Bảo vệ các hệ thống thông tin quan trọng với môi trường CNTT dùng chung 8
1.2.1. Bảo vệ môi trường CITAD 8
1.2.2. Kiểm soát tài khoản đặc quyền của hệ điều hành 12
1.2.3. Bảo vệ môi trường ảo hóa 14
1.3. Giảm bề mặt tấn công và các lỗ hổng 15
1.3.1. Cập nhật bảo mật 15
1.3.2. Nâng cao bảo mật hệ thống 16
1.3.3. Bảo vệ luồng dữ liệu truyền bên ngoài 18
1.3.4. Kiểm soát giao dịch 19
1.3.5. Nâng cao bảo mật ứng dụng 20
1.4. Bảo mật vật lý môi trường hoạt động 20
1.4.1. An toàn vật lý 20
2. Kiểm soát và giới hạn các truy cập 22
2.1. Ngăn chặn xâm phạm thông tin đăng nhập 22
2.1.1. Xác thực đa thành tố 22
2.2. Quản trị định danh và các đặc quyền 24
2.2.1. Thẩm tra nhân sự 24
2.2.2. Lưu trữ mật khẩu theo hình thức vật lý hoặc logic 25
3. Ứng phó sự cố an ninh mạng 26
3.1. Kế hoạch ứng phó sự cố an ninh mạng 26
3.1.1. Lập kế hoạch ứng phó sự cố an ninh mạng 26
VI. MA TRẬN KIỂM SOÁT RỦI RO 28
VII. LỘ TRÌNH ÁP DỤNG 30
VIII. SO SÁNH VỚI CÁC TIÊU CHUẨN VÀ QUY ĐỊNH HIỆN HÀNH 31
PHỤ LỤC 1: DANH MỤC TÀI LIỆU THAM KHẢO 34
PHỤ LỤC 2: MẪU BÁO CÁO DÀNH CHO THÀNH VIÊN 35

DANH MỤC TỪ NGỮ VIẾT TẮT, THUẬT NGỮ

STT	Từ viết tắt, thuật ngữ	Giải thích
1	Môi trường máy chủ (Server Environment)	Trung tâm dữ liệu hoặc môi trường vật lý để đặt các máy chủ.
2	Môi trường CNTT dùng chung (General /Enterprise IT environment)	Cơ sở hạ tầng CNTT dùng chung sử dụng tại thành viên
3	Vùng an toàn (Secure Zone)	Vùng tách biệt với khu vực dùng chung, chứa các hệ thống liên quan đến Hệ thống CITAD và các hệ thống khác được lựa chọn để bảo vệ.
4	Máy vận hành dùng chung (General purpose operator PCs)	Máy tính được thiết lập trong môi trường CNTT dùng chung và được sử dụng cho các hoạt động nghiệp vụ hàng ngày.
5	Máy vận hành chuyên dùng (Dedicated operator PC)	Máy tính được thiết lập trong vùng an toàn và dành riêng để tương tác với các thành phần của vùng an toàn.
6	Máy chủ trung gian (Jump server)	Máy chủ được sử dụng để cung cấp kết nối đến vùng an toàn từ môi trường mạng của người dùng (ví dụ: sử dụng giải pháp ảo hóa VDI - Virtual Desktop Infrastructure hoặc giải pháp Remote Desktop)
7	Phần mềm truy cập từ xa (Remote Desktop)	Quá trình sử dụng phần mềm sẵn có của Hệ điều hành Windows hoặc phần mềm ứng dụng của bên thứ ba như TeamViewer, VNC, PC Anywhere, Any Desk,... để kết nối đến một máy tính khác.
8	Truy cập từ xa (Remote access)	Quy trình của việc truy cập các tài nguyên mạng từ mạng khác, hoặc từ một thiết bị đầu cuối mà không được kết nối vĩnh viễn, theo cách vật lý hoặc logic, tới mạng mà nó đang truy cập[1].
9	Đăng nhập từ xa (Remote log-in)	Quá trình đăng nhập vào một hệ thống bằng cách khởi tạo một kết nối mạng từ xa thay vì thực hiện đăng nhập từ một máy trạm được thiết lập trong mạng cục bộ.
10	Virtual Desktop Infrastructure	Giải pháp ảo hóa về ứng dụng hoặc máy trạm

[1] Theo định nghĩa tại Tiêu chuẩn quốc gia TCVN 9801-1:2013 (ISO/IEC 27033-1:2009) về Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng - Phần 1: Tổng quan và khái niệm

STT	Từ viết tắt, thuật ngữ	Giải thích
11	Thiết bị mạng (Network devices)	Các thành phần được sử dụng để hỗ trợ quản lý, định tuyến và bảo mật mạng (ví dụ: bộ định tuyến, bộ chuyển mạch, tường lửa).
12	Dịch vụ CNTT (IT services)	Nhóm các dịch vụ CNTT được thực hiện trong vùng an toàn, ví dụ phát hành phiên bản, cập nhật bản vá lỗi, dịch vụ thư mục - Active Directory
13	Dịch vụ CNTT dùng chung (General IT services)	Các dịch vụ hỗ trợ cơ sở hạ tầng CNTT, gồm: dịch vụ xác thực, cơ sở dữ liệu, lưu trữ dữ liệu, dịch vụ bảo mật (ví dụ: vá lỗi) và dịch vụ mạng (ví dụ: DNS- Domain Name System, NTP – Network Time Protocol,..),…
14	Giao diện Webservice (Webservice Interface)	Cung cấp khả năng tương tác, trao đổi thông tin giữa Hệ thống CITAD với các hệ thống thông tin nội bộ của thành viên thông qua dịch vụ Webservice. Quá trình trao đổi sử dụng định dạng trao đổi dữ liệu IBPS2.5 do NHNN phát hành để trao đổi thông tin.
15	Giao diện truyền thông (Communication Interface)	Cung cấp khả năng tương tác, trao đổi thông tin giữa Hệ thống CITAD với Trung tâm xử lý của Hệ thống TTĐLNH qua dịch vụ tin điện (Oracle Tuxedo Message Queue), gửi nhận tập tin (SFPT); trao đổi với các hệ thống thông tin nội bộ của thành viên gửi nhận tập tin (SFPT/FPT), kết nối trực tiếp đến CSDL. Quá trình trao đổi sử dụng định dạng trao đổi dữ liệu IBPS2.5 do NHNN phát hành để trao đổi thông tin.
16	Giao diện đồ họa người dùng (GUI)	Giao diện đồ họa của phần mềm ứng dụng cung cấp cho người dùng
17	Người dùng cuối (End User)	Các cá nhân có yêu cầu truy cập tương tác vào ứng dụng để thực hiện các hoạt động (tạo lập/kiểm soát/duyệt giao dịch, giám sát hoạt động hệ thống, kiểm soát truy cập hệ thống,…).
18	Người quản trị (Administrator)	- Quản trị ứng dụng (Application Administrator): chịu trách nhiệm cấu hình, duy trì và thực hiện các hoạt động đặc quyền thông qua giao diện ứng dụng. - Quản trị hệ thống (System Administrator): chịu trách nhiệm cấu hình, duy trì và thực hiện các hoạt động đặc quyền khác thông qua hệ điều hành hoặc truy cập trực tiếp (không qua giao diện người dùng).
19	Người vận hành (Operator)	Là cách gọi chung của người dùng cuối và người quản trị

STT	Từ viết tắt, thuật ngữ	Giải thích
20	Tài khoản ứng dụng (Application account)	Tài khoản được sử dụng cho phần mềm ứng dụng, dùng để tích hợp, trao đổi thông tin với các phần mềm ứng dụng khác (ví dụ: sử dụng dịch vụ Webservice, API,..).
21	Tài khoản hệ điều hành (Operating system accounts)	Là tài khoản người dùng được tạo bởi hệ điều hành trong quá trình cài đặt và được sử dụng cho các mục đích quản trị hệ thống (ví dụ: tài khoản Adminstrator trên hệ điều hành Windows; tài khoản root trên hệ điều hành Linux/Unix)
22	Tài khoản ứng dụng của người dùng (User application accounts)	Là tài khoản người dùng được thiết lập tại ứng dụng, được sử dụng để truy cập, sử dụng ứng dụng hoặc có thể dùng để khởi tạo và cấp quyền truy cập ứng dụng cho các tài khoản khác.
23	PIN (Persional Identification Number)	Số nhận dạng cá nhân – dòng mã hoặc mật khẩu mà người dùng/khách hàng sở hữu, dùng để xác minh danh định.
24	Danh sách kiểm soát truy cập mạng (Network access control list -ACL)	Các luật, thông tin kiểm soát (địa chỉ IP, cổng – Port) trên các thiết bị mạng để kiểm soát lưu lượng vào và ra.
25	Chế độ bảo trì (Single user or safe mode)	Chế độ vận hành giới hạn các đặc quyền của người dùng (hệ điều hành Linux/Unix gọi là chế độ đơn người dùng – single user mode; hệ điều hành Windows gọi là chế độ an toàn – safe mode).
26	Véc-tơ tấn công (Attack vector)[2]	Là con đường hay cách thức mà đối tượng tấn công có thể truy cập vào một máy tính hay máy chủ mạng để chuyển các phần mềm độc hại vào

[2] Thuật ngữ 4.10, TCVN 11780:2017 (ISO/IEC 27032:2012)

DANH MỤC HÌNH VẼ

Hình 1: Nguyên tắc kiểm soát an toàn thông tin 2
Hình 2: Mô hình kết nối tổng quát Hệ thống CITAD tại thành viên 3
Hình 3: Phạm vi bảo vệ an toàn thông tin Hệ thống CITAD 3
Hình 4: Mô hình tham chiếu giao diện các phần mềm ứng dụng Hệ thống CITAD 5
Hình 5: Mô hình tham chiếu an toàn thông tin Hệ thống CITAD 5
Hình 6: Lộ trình áp dụng các yêu cầu 30

DANH MỤC BẢNG

Bảng 1: Bảng tổng hợp các yêu cầu kiểm soát an toàn thông tin.....6
Bảng 2: Ma trận kiểm soát rủi ro.....28

I. MỤC ĐÍCH, PHẠM VI ÁP DỤNG

1. Mục đích

Hướng dẫn tăng cường an toàn thông tin hệ thống phần mềm CITAD (Credit Institution Terminal Access Devices) tại thành viên Hệ thống Thanh toán điện tử liên ngân hàng Quốc gia (Hệ thống TTĐTLNH) được xây dựng với mục đích:

– Cụ thể hóa các biện pháp đảm bảo an toàn thông tin làm cơ sở cho việc triển khai, vận hành hệ thống phần mềm CITAD (Hệ thống CITAD) tại các thành viên/đơn vị thành viên trực tiếp của Hệ thống TTĐTLNH, Tổ chức chủ trì hệ thống bù trừ điện tử (sau đây gọi tắt là thành viên) được an toàn, hiệu quả, góp phần nâng cao hoạt động của Hệ thống TTĐTLNH.

– Cung cấp thông tin hỗ trợ thành viên trong việc lựa chọn giải pháp cơ sở hạ tầng, trang thiết bị phần cứng, giải pháp ứng dụng phần mềm cho việc thiết lập môi trường, hoạt động vận hành Hệ thống CITAD tại thành viên.

– Thông qua báo cáo tình trạng triển khai, áp dụng các chính sách an ninh, bảo mật tại thành viên để tăng cường hơn nữa công tác quản lý nhà nước đối với hoạt động triển khai, vận hành hoạt động Hệ thống CITAD tại thành viên, hướng tới vận hành theo nguyên tắc, tiêu chuẩn quốc tế.

2. Phạm vi áp dụng

– Hướng dẫn tăng cường an toàn thông tin hệ thống phần mềm CITAD tại thành viên Hệ thống TTĐTLNH (sau đây gọi là Hướng dẫn ATTT) có phạm vi áp dụng tại các thành viên.

II. NGUYÊN TẮC KIỂM SOÁT AN TOÀN THÔNG TIN

Hệ thống CITAD là hệ thống thông tin cấp độ 3[3], do đó các thành viên phải đảm bảo tuân thủ các quy định tại Thông tư số 09/2020/TT-NHNN ngày 21/10/2020, Thông tư số 35/2016/TT-NHNN ngày 29/12/2016[4] đã được sửa đổi bổ sung hoặc Quyết định số 1820/QĐ-NHNN ngày 26/10/2020[5].

Hướng dẫn ATTT được xây dựng dựa trên các quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng được ban hành bởi Ngân hàng Nhà nước (NHNN) và thông lệ tốt nhất trong quá trình vận hành, khai thác Hệ thống CITAD tại thành viên.

Hướng dẫn ATTT bao gồm các yêu cầu kiểm soát (sau đây gọi tắt là yêu cầu) áp dụng bắt buộc hoặc mang tính tư vấn, khuyến nghị cho thành viên. Cùng với sự gia tăng, ngày càng phát triển của các mối đe dọa an ninh mạng, Hướng dẫn ATTT sẽ được cập nhật bổ sung, thay đổi các yêu cầu để phù hợp với các khuyến nghị an

---

[3] Theo tiêu chí tại khoản c điểm 4 Điều 5 Thông tư số 09/2020/TT-NHNN ngày 21/10/2020

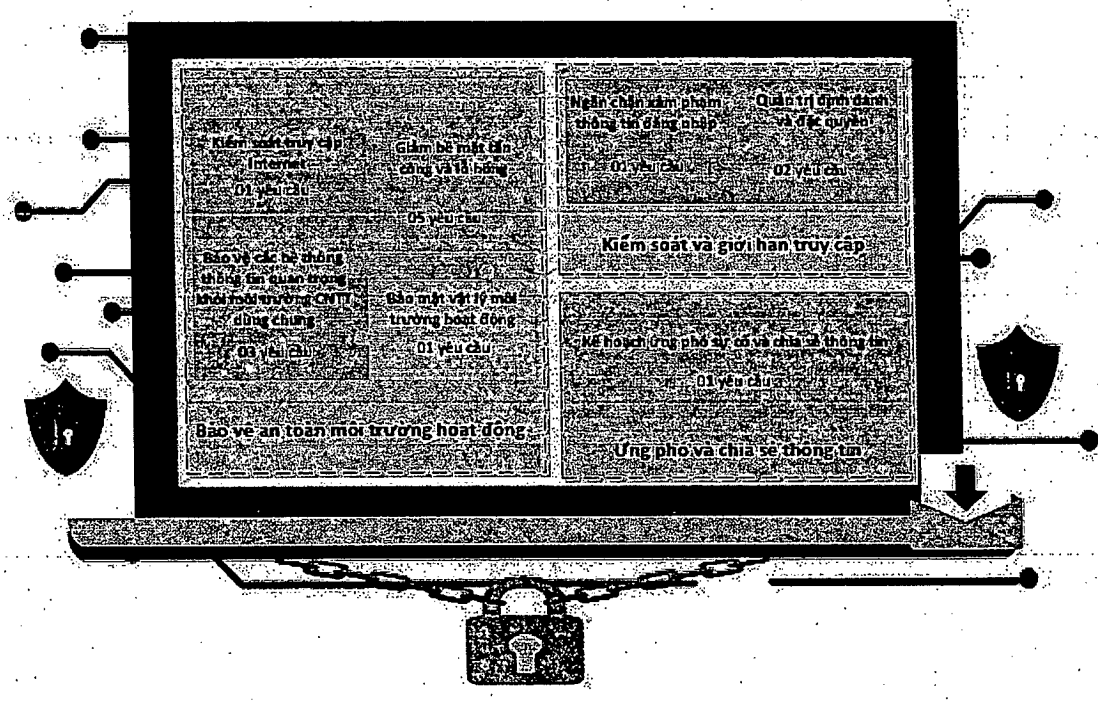
[4] Áp dụng đối với thành viên/đơnvị thành viên là ngân hàng, chi nhánh ngân hàng nước ngoài, Kho bạc Nhà nước Trung ương tham gia Hệ thống TTLNH; Tổ chức chủ trì hệ thống bù trừ điện tử.

[5] Áp dụng đối với với thành viên/đơn vị thành viên là Ngân hàng Nhà nước.

ninh bảo mật, tình hình an ninh mạng, một số yêu cầu mang tính tự vấn, khuyến nghị có thể trở thành bắt buộc.

Thành viên triển khai các giải pháp phù hợp với hiện trạng cơ sở hạ tầng, quy định chính sách nội bộ và đảm bảo khả năng an toàn thông tin tối thiểu như các yêu cầu tại Hướng dẫn ATTT. Đối với các yêu cầu chưa đáp ứng hoặc việc triển khai, áp dụng phụ thuộc chính sách của ngân hàng mẹ[6], thành viên xây dựng phương án, lộ trình cụ thể gửi NHNN (Cục Công nghệ thông tin) để phối hợp thực hiện, đảm bảo an toàn thông tin chung cho toàn hệ thống TTĐTLNH. Định kỳ hằng năm (tháng 11), thành viên gửi NHNN (Cục Công nghệ thông tin) báo cáo kết quả thực hiện các yêu cầu áp dụng bắt buộc và tùy chọn của Hướng dẫn ATTT tại thành viên (theo mẫu tại Phụ lục 02).

Các yêu cầu tập trung vào 03 nhóm mục tiêu: (i) Bảo vệ an toàn môi trường vận hành; (ii) Kiểm soát và giới hạn truy cập; (iii) Ứng phó sự cố an ninh mạng.



Hình 1: Nguyên tắc kiểm soát an toàn thông tin

Mỗi nhóm mục tiêu áp dụng các nguyên tắc bảo mật an toàn thông tin tương ứng như sau:

– Bảo vệ an toàn môi trường hoạt động:

+ Kiểm soát truy cập Internet;

+ Bảo vệ các hệ thống thông tin quan trọng khỏi môi trường CNTT dùng chung;

+ Giảm bề mặt tấn công[7] và lỗ hổng;

+ Bảo mật vật lý môi trường hoạt động.

[6] Thành viên là chi nhánh ngân hàng nước ngoài

[7] Bề mặt tấn công là tất cả các điểm mà kẻ tấn công có thể xâm nhập

– Kiểm soát và giới hạn truy cập:

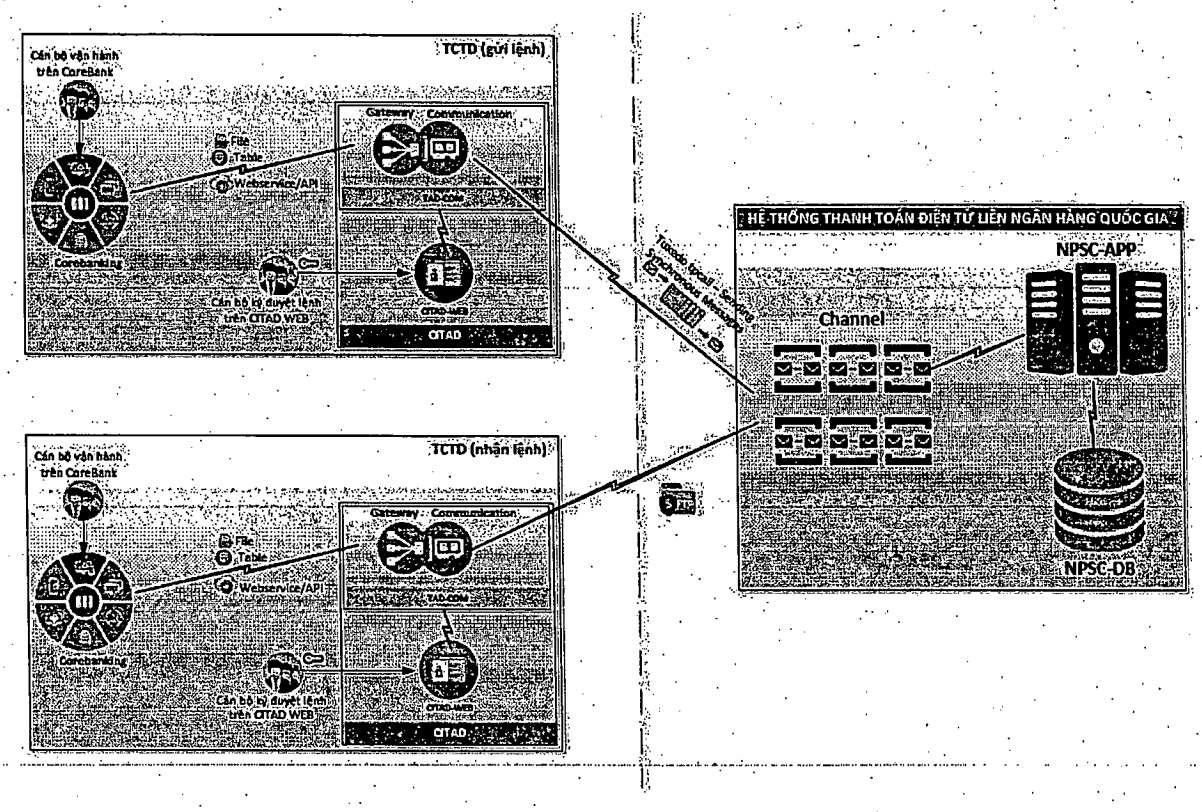
+ Ngăn chặn xâm phạm thông tin đăng nhập;

+ Quản trị định danh và đặc quyền.

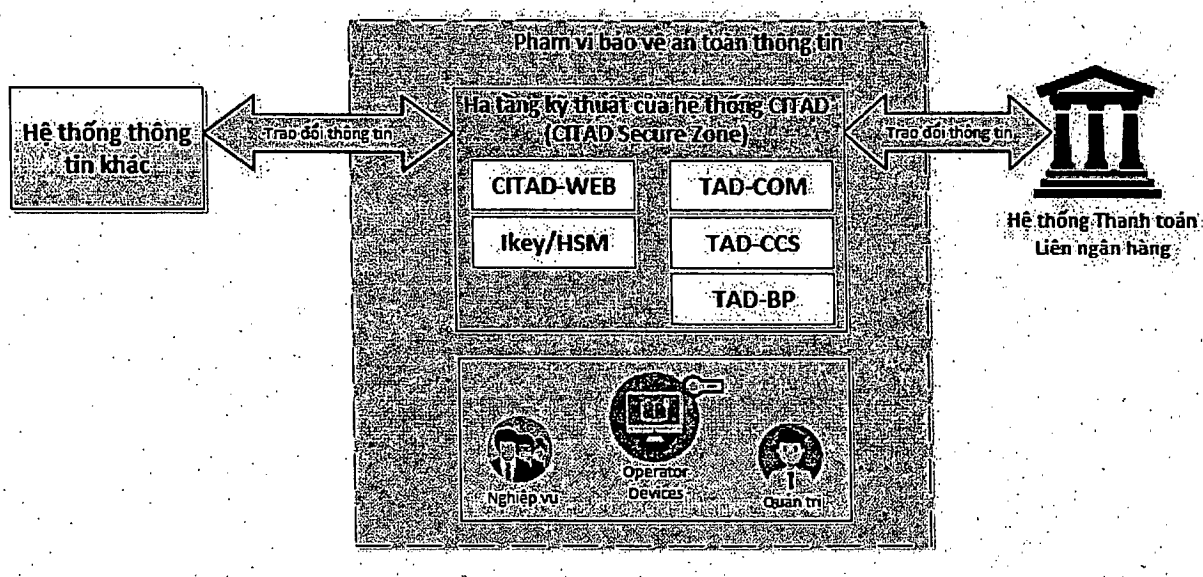
– Ứng phó sự cố an ninh mạng:

+ Lập kế hoạch ứng phó sự cố an ninh mạng.

III. PHẠM VI KIỂM SOÁT AN TOÀN THÔNG TIN



Hình 2: Mô hình kết nối tổng quát Hệ thống CITAD tại thành viên



Hình 3: Phạm vi bảo vệ an toàn thông tin Hệ thống CITAD

Phạm vi bảo vệ an toàn thông tin Hệ thống CITAD gồm:

– Hạ tầng kỹ thuật của Hệ thống CITAD (được gọi là vùng an toàn CITAD: CITAD Secure Zone - CSZ) bao gồm: các hệ thống máy chủ, thiết bị mạng (tường lửa, thiết bị chuyển mạch, bộ định tuyến,...), phần mềm ứng dụng, Ikey/HSM,... phục vụ cho việc vận hành hệ thống CITAD tại thành viên. Trong đó:

+ CITAD-WEB: phần mềm ứng dụng cung cấp giao diện xử lý lệnh tại thành viên;

+ TAD-COM: phần mềm ứng dụng truyền nhận lệnh thanh toán giữa thành viên với Trung tâm xử lý của Hệ thống TTĐTLNH;

+ TAD-CCS: phần mềm xử lý ký duyệt tự động, xử lý lưu lượng lệnh thanh toán lớn tại thành viên;

+ TAD-BP: phần mềm xử lý dịch vụ quyết toán kết quả bù trừ dành cho tổ chức bù trừ điện tử;

+ Ikey/HSM: thiết bị lưu trữ chứng thư số của thành viên.

– Các kết nối trao đổi thông tin liên quan đến Hệ thống CITAD tại thành viên.

+ Giữa Hệ thống CITAD với Hệ thống TTĐTLNH: sử dụng kết nối mạng WAN giữa thành viên và NHNN; giao thức truyền tin điện đồng bộ (Sending Synchronous Messages) và gửi nhận tập tin bảo mật (Secure File Transfer Protocol); tiêu chuẩn dữ liệu IBPS2.5;

+ Giữa Hệ thống CITAD với các hệ thống thông tin nội bộ khác của thành viên: sử dụng kết nối mạng LAN nội bộ của thành viên hoặc kết nối mạng giữa thành viên và bên thứ ba trong trường hợp thành viên sử dụng nền tảng ảo hóa từ xa (được cài đặt và/hoặc vận hành bởi bên thứ ba) để thiết lập các máy chủ ảo để cài đặt Hệ thống CITAD, thành viên nên mã hóa dữ liệu; trao đổi thông tin qua gửi nhận tập tin (File Transfer Protocol) hoặc gửi nhận tập tin bảo mật (Secure File Transfer Protocol), Webservice/API hoặc kết nối cơ sở dữ liệu (ODBC, OLE DB, DB Library,...); tiêu chuẩn dữ liệu IBPS2.5;

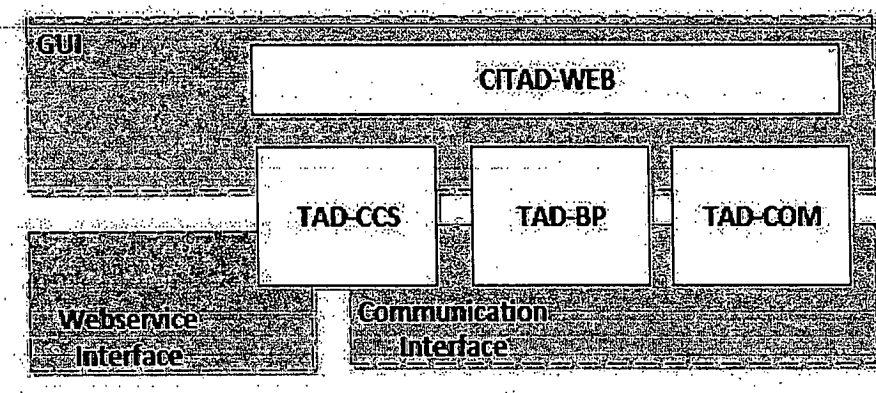
– Người vận hành (Operators): bao gồm người dùng nghiệp vụ và người dùng quản trị hệ thống, có tương tác với CSZ thông qua các phần mềm ứng dụng hoặc tương tác trực tiếp mức hệ điều hành.

– Máy vận hành (Operator Devices): là thiết bị máy tính để bàn hoặc xách tay của người vận hành, được sử dụng để thực hiện các nhiệm vụ của người vận hành liên quan đến Hệ thống CITAD. Thiết bị đầu cuối này gồm 02 loại như sau:

+ Máy vận hành dùng chung (General Purpose Operator Device): được đặt trong môi trường CNTT dùng chung của thành viên, được sử dụng cho nhiều hoạt động nghiệp vụ hằng ngày tại thành viên (trong đó có nghiệp vụ liên quan đến Hệ thống CITAD);

+ Máy vận hành chuyên dùng (Dedicated Operator Device): được đặt trong vùng an toàn và chỉ sử dụng cho các hoạt động liên quan đến Hệ thống CITAD, tương tác với các thành phần trong CSZ.

– Máy chủ trung gian (Jump server): là thiết bị máy tính được được đặt trong vùng an toàn, cho phép cung cấp kết nối đến CSZ từ môi trường mạng của người dùng (ví dụ: sử dụng giải pháp ảo hóa VDI - Virtual Desktop Infrastructure hoặc giải pháp Remote Desktop).



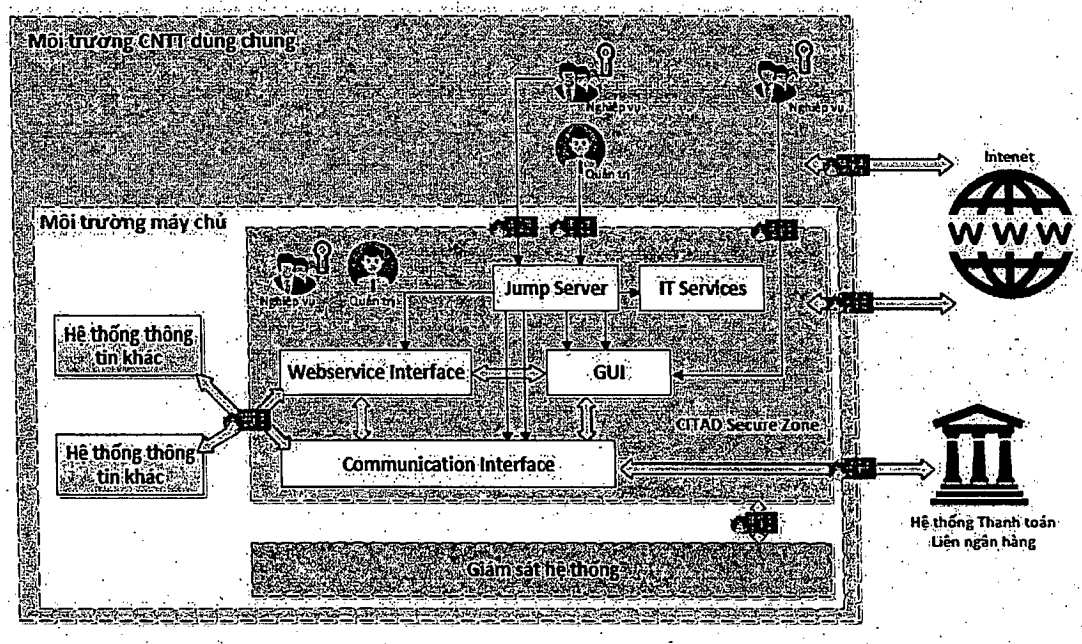
Hình 4: Mô hình tham chiếu giao diện các phần mềm ứng dụng Hệ thống CITAD

– Phân loại giao diện các phần mềm ứng dụng Hệ thống CITAD như sau:

+ CITAD-WEB: phần mềm ứng dụng cung cấp Giao diện đồ họa người dùng (GUI);

+ TAD-COM, TAD-BP: phần mềm ứng dụng cung cấp Giao diện đồ họa người dùng và Giao diện truyền thông (Communication Interface);

+ TAD-CCS: phần mềm ứng dụng cung cấp Giao diện đồ họa người dùng và Giao diện Webservice (Webservice Interface).



Hình 5: Mô hình tham chiếu an toàn thông tin Hệ thống CITAD

IV. TỔNG QUAN CÁC KIỂM SOÁT AN TOÀN THÔNG TIN

Bảng 1: Bảng tổng hợp các yêu cầu kiểm soát an toàn thông tin

STT	Các yêu cầu kiểm soát an toàn thông tin	Yêu cầu	
		Bắt buộc	**Khuyến nghị**
1. Bảo vệ an toàn môi trường hoạt động			
1.1	Kiểm soát truy cập Internet		
1.1.1	*Hạn chế truy cập Internet*	•	
1.2	Bảo vệ các hệ thống thông tin quan trọng khỏi môi trường CNTT dùng chung		
1.2.1	*Bảo mật môi trường CITAD*	•	
1.2.2	*Kiểm soát tài khoản đặc quyền của hệ điều hành*	•	
1.2.3	*Bảo mật môi trường ảo hóa*	•	
1.3	Giảm bề mặt tấn công và lỗ hổng		
1.3.1	*Cập nhật bảo mật*	•	
1.3.2	*Nâng cao bảo mật hệ thống*	•	
1.3.3	*Bảo mật luồng dữ liệu truyền bên ngoài*		•
1.3.4	*Kiểm soát giao dịch*		•
1.3.5	*Nâng cao bảo mật ứng dụng*	•	
1.4	Bảo vệ vật lý môi trường hoạt động		
1.4.1	*An toàn vật lý*	•	
2. Kiểm soát và giới hạn truy cập			
2.1	Ngăn chặn xâm phạm thông tin đăng nhập		
2.1.1	*Xác thực đa thành tố*		•
2.2	Quản trị định danh và đặc quyền		
2.2.1	*Thẩm tra nhân sự*	•	
2.2.2	*Lưu trữ mật khẩu vật lý và logic*	•	
3. Ứng phó sự cố an ninh mạng			
3.1	Kế hoạch ứng phó sự cố an ninh mạng		
3.1.1	*Lập kế hoạch ứng phó sự cố an ninh mạng*	•	

(• cho biết đây là các yêu cầu bắt buộc hay khuyến nghị)

V. CHI TIẾT CÁC YÊU CẦU

1. Bảo vệ an toàn môi trường hoạt động

1.1. Kiểm soát truy cập Internet

1.1.1. Hạn chế truy cập Internet

Các yếu tố rủi ro: Các cuộc tấn công từ Internet.

Mục tiêu kiểm soát: Kiểm soát/bảo vệ hạn chế truy cập Internet từ các máy vận hành và hệ thống trong vùng an toàn .

Phạm vi kiểm soát:

– Các máy vận hành chuyên dùng và máy vận hành dùng chung;

– Máy chủ trung gian;

– Giao diện Webservice;

– Giao diện truyền thông;

– Giao diện đồ họa người dùng;

– Nền tảng ảo hóa (còn được gọi là phần mềm ảo hóa) nội bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba) thiết lập các máy ảo hóa liên quan đến Hệ thống CITAD và các máy tính quản trị của bên thứ ba.

Yêu cầu kiểm soát: Các thành phần trong vùng an toàn phải được kiểm soát truy cập Internet.

Lý do kiểm soát: Truy cập trực tiếp vào Internet làm tăng nguy cơ bị tấn công từ Internet. Rủi ro sẽ tăng cao khi người dùng có các hoạt động tương tác (duyệt web, email hoặc các hoạt động tại các trang mạng xã hội). Sau khi bị xâm nhập, những hệ thống này có thể trở thành điểm truy cập cho phép xâm nhập, thực thi các câu lệnh nguy hiểm và chiếm quyền điều khiển. Việc hạn chế truy cập Internet đóng vai trò quan trọng trong việc giảm bề mặt tấn công và các điểm yếu của các hệ thống.

Hướng dẫn thực hiện:

a) Truy cập Internet từ vùng an toàn

– Hạn chế tối đa (hoặc chặn) truy cập email (Web Mail) trên trình duyệt từ các hệ thống thuộc vùng an toàn CITAD.

– Chặn truy cập Internet từ các hệ thống trong vùng an toàn (ví dụ: các máy vận hành chuyên dùng, các máy chủ trung gian hoặc các thành phần có liên quan đến CITAD):

+ Các hoạt động cần truy cập Internet (ví dụ: tải các bản vá an ninh bảo mật, bản nâng cấp/cập nhật của CITAD,...) nên tiến hành bên ngoài vùng an toàn rồi sau đó chuyển tiếp vào vùng an toàn bằng các phương thức an toàn;

+ Trường hợp cần thiết phải truy cập Internet từ bên trong vùng an toàn thì thiết lập chỉ khởi tạo kết nối Internet theo chiều truy cập từ bên trong ra ngoài và cấp quyền truy cập cho các địa chỉ URLs thuộc danh sách địa chỉ an toàn (white-list) thông qua proxy, có kiểm tra nội dung và các biện pháp kiểm soát chặn/lọc thích hợp. Sau khi hoàn thành công việc liên quan đến yêu cầu phải truy cập Internet, thực hiện khôi phục chính sách chặn truy cập Internet.

b) Truy cập Internet từ các máy vận hành chung

– Kiểm soát truy cập Internet đối với các máy vận hành dùng chung được được sử dụng để truy cập và xử lý giao dịch thanh toán thông qua giao diện đồ họa người dùng với một trong các tùy chọn sau:

+ Truy cập Internet thông qua một máy tính được truy cập từ xa hoặc sử dụng giải pháp máy ảo[8];

+ Chỉ cho phép truy cập các địa chỉ URL thuộc danh sách địa chỉ an toàn (white-list) thông qua proxy, có kiểm tra nội dung và các biện pháp kiểm soát chặn/lọc thích hợp. Kết nối chỉ được phép nếu khởi tạo theo chiều truy cập từ bên trong ra ngoài;

+ Truy cập Internet thông qua Web Gateway (có kiểm tra nội dung và các biện pháp kiểm soát chặn/lọc thích hợp) có sử dụng danh sách đen.

1.2. Bảo vệ các hệ thống thông tin quan trọng với môi trường CNTT dùng chung

1.2.1. Bảo vệ môi trường CITAD

Các yếu tố rủi ro:

– Xâm phạm hệ thống xác thực của thành viên;

– Xâm phạm các thông tin đăng nhập;

– Tấn công phát lại thông tin xác thực;

– Các cuộc tấn công từ Internet ;

– Truy cập trái phép;

– Xâm phạm các thông tin mật.

Mục tiêu kiểm soát: Bảo vệ hạ tầng hệ thống CITAD của thành viên khỏi sự xâm phạm từ môi trường CNTT dùng chung và môi trường bên ngoài.

Phạm vi kiểm soát:

– Giao diện Webservice;

– Giao diện truyền thông;

– Giao diện đồ họa người dùng;

[8] Ví dụ: giải pháp Virtual Desktop Infrastructure - VDI

– Các máy vận hành chuyên dùng và máy vận hành dùng chung;

– Máy chủ trung gian;

– Ikey/HSM.

Yêu cầu kiểm soát: Phân tách hạ tầng[9] hệ thống CITAD với các môi trường bên ngoài.

Lý do kiểm soát: Sự phân tách hạ tầng hệ thống CITAD với các môi trường mạng khác làm giảm bề mặt tấn công và đây là một cách hiệu quả để bảo vệ chống lại các cuộc tấn công mạng gây hại đến môi trường CNTT dùng chung. Sự phân tách hiệu quả bao gồm phân tách cấp độ mạng, hạn chế truy cập và hạn chế kết nối.

Hướng dẫn thực hiện:

a) Chiến lược tổng thể để phân tách môi trường

– Thiết lập một vùng an toàn để phân tách và bảo vệ hạ tầng hệ thống CITAD khỏi sự gây hại từ các hệ thống và dịch vụ nằm bên ngoài vùng an toàn.

– Mật khẩu và các dịch vụ xác thực được sử dụng trong vùng an toàn (đặc biệt là các tài khoản đặc quyền) không được lưu trữ hoặc sử dụng trong bất kỳ hình thức nào (băm, mã hóa hay dạng rõ) trong các hệ thống bên ngoài vùng an toàn (không áp dụng yêu cầu này đối với những tập tin sao lưu đã được mã hóa). Nếu sử dụng dịch vụ xác thực từ các hệ thống xác thực nằm ngoài vùng an toàn CITAD (CSZ), cần phải đáp ứng:

+ Hệ thống xác thực được thiết lập trong một vùng an toàn khác, có áp dụng các biện pháp kiểm soát tương tự.

+ Hoặc nếu hệ thống xác thực chỉ được sử dụng để lọc các kết nối đến các thành phần của hạ tầng CITAD (kiểm soát kết nối tại các vị trí ranh giới của vùng an toàn). Trong trường hợp này, quyền truy cập logic vào các thành phần của hạ tầng CITAD được đảm bảo bởi một cơ chế xác thực khác nằm trong vùng an toàn (sử dụng giải pháp quản lý cấp phát, quản lý định danh người dùng truy cập ứng dụng – Identity & Access Management - IAM khác hoặc sử dụng giải pháp xác thực bởi chính thành phần được truy cập).

– Phạm vi của vùng an toàn được xác định phù hợp với môi trường của từng thành viên, và có thể sử dụng lại các vùng an toàn hiện có của thành viên để chứa hạ tầng CITAD.

– Áp dụng biện pháp quản lý, bảo vệ phù hợp với từng thành phần trong vùng an toàn.

b) Phạm vi của vùng an toàn

– Vùng an toàn chứa, nhưng không giới hạn, tất cả các thành phần của cơ sở hạ tầng CITAD tại thành viên, gồm: giao diện Webservice; giao diện truyền thông; giao diện đồ họa người dùng; Ikey/HSM; các máy vận hành chuyên dùng dành riêng

[9] Thực hiện phân tách về mặt vật lý hoặc logic

cho hoạt động nghiệp vụ hoặc quản trị của cơ sở hạ tầng CITAD; máy chủ trung gian.

+ Các máy tính với mục đích dùng chung không được đặt trong vùng an toàn;

+ Các phần mềm vận hành có giao diện đồ họa người dùng của hệ thống CITAD cần được cài đặt trên các máy vận hành chuyên dùng đặt trong vùng an toàn hoặc được cài đặt trên các máy chủ trung gian và các máy vận hành dùng chung đặt ngoài vùng an toàn truy cập đến các máy chủ trung gian này;

+ Các hệ thống nghiệp vụ nội bộ của thành viên, có trao đổi thông tin với hệ thống CITAD không nhất thiết phải được đưa vào vùng an toàn;

+ Hệ thống kiểm thử (Test systems) phải tách biệt hoàn toàn với hệ thống chạy chính (Production systems) và được cấu hình chỉ để phục vụ cho việc kiểm thử. Trường hợp không tách biệt hoàn toàn giữa hệ thống kiểm thử và hệ thống chạy chính, thì hệ thống kiểm thử phải được bảo vệ với cùng một cấp độ an ninh bảo mật như đối với hệ thống chính. Hệ thống phát triển (Development systems) không nằm trong vùng an toàn và không kết nối đến hệ thống TTĐTLNH (bao gồm môi trường chạy chính và môi trường thử nghiệm).

– Giới hạn và phạm vi vùng an toàn được xác định phù hợp nhất với môi trường của thành viên. Các tùy chọn có thể bao gồm, nhưng không giới hạn:

+ Thiết lập một vùng an toàn CITAD dành riêng cho cơ sở hạ tầng CITAD;

+ Mở rộng vùng an toàn hiện có để bảo vệ cơ sở hạ tầng CITAD. Quy mô và phạm vi của khu vực này có thể thay đổi đáng kể tùy thuộc vào môi trường hiện có.

– Các phần mềm, hệ thống và dịch vụ trong vùng an toàn cần được đánh giá về sự cần thiết và loại bỏ khỏi vùng nếu không hỗ trợ cho việc vận hành hoạt động hoặc đảm bảo an toàn bảo mật của vùng (ví dụ: đánh giá nhu cầu truy cập email).

c) Bảo vệ vùng an toàn (bảo vệ vùng biên)

– Các tường lửa được sử dụng để tách biệt lôgic tại vùng biên của vùng an toàn.

+ Sử dụng thiết bị tường lửa lớp truyền tải dạng vật lý hoặc ảo hóa dùng riêng cho việc tách biệt lôgic tại vùng biên của vùng an toàn. Trường hợp chia sẻ tường lửa với các vùng mạng khác, phải quản trị tường lửa để đảm bảo việc chia sẻ không ảnh hưởng đến việc bảo vệ vùng an toàn;

+ Danh sách truy cập (ACLs) và tường lửa ứng dụng (application firewalls) có thể được sử dụng để cung cấp các biện pháp bảo vệ bổ sung cho vùng an toàn.

– Các thiết bị lớp 2 (ví dụ: switch) có thể được dùng chung giữa vùng an toàn và những vùng khác (phân chia mạng VLAN).

– Bảo vệ việc truy cập quản trị tới các thiết bị mạng khi sử dụng kênh truyền tín hiệu riêng (out-of-band)[10] hoặc kênh truyền dữ liệu thông thường (in-band)[11] (ví dụ: quản trị qua VLAN). Quản trị truy cập vào các thiết bị tường lửa không dựa vào hệ thống xác thực dùng chung mà sử dụng một hệ thống nằm trong vùng an toàn được áp dụng các biện pháp bảo vệ tương tự cho vùng an toàn CITAD.

– Kết nối vào ra vùng an toàn nên hạn chế tới mức tối đa có thể. Thực hiện tiến trình để phân tích, soát xét và thực thi các chính sách tường lửa để điều chỉnh các kết nối:

+ Không cho phép luật "cho phép tất cả", tất cả các luồng mạng phải được cấp quyền một cách rõ ràng. Để thực hiện điều này, có thể sử dụng một máy chủ dùng chung để lọc truy cập kết nối hợp pháp hướng tới vùng an toàn mà không làm mất khả năng truy xuất nguồn gốc của các kết nối đó;

+ Thiết lập giới hạn đối với kết nối qua vùng biên của vùng an toàn, gồm: giao diện chiều vào (inbound) từ các máy vận hành dùng chung tới máy chủ trung gian, giao diện chiều ra đối với dữ liệu quản trị (dữ liệu nhật ký, dữ liệu sao lưu);

+ Rà soát các chính sách tường lửa tối thiểu 01 lần/01 năm.

d) Truy cập vào các hệ thống thuộc vùng an toàn

– Triển khai một số mô hình sau cho vùng an toàn để hạn chế truy cập của người vận hành vào vùng an toàn (thông qua giao diện hoặc dòng lệnh)

+ Người vận hành kết nối từ các máy vận hành chuyên dùng cho việc vận hành CITAD và các máy tính này đặt trong vùng an toàn;

+ Người vận hành kết nối từ các máy vận hành dùng chung tới vùng an toàn thông qua một máy chủ trung gian đặt trong vùng an toàn CITAD hoặc trong vùng an toàn khác được thiết lập các chính sách kiểm soát tương tự. Máy chủ trung gian được áp dụng các phương pháp bảo mật gồm:

• Đảm bảo tất cả các biện pháp kiểm soát an ninh thuộc phạm vi tài liệu này được thiết lập (ví dụ: cập nhật bản vá bảo mật, nâng cao bảo mật hệ thống);

• Tách biệt máy chủ trung gian dành cho người quản trị hệ thống (administrators) với máy chủ trung gian dành người dùng cuối (end users). Một hình thức khác để tách biệt máy chủ trung gian nếu dùng chung máy chủ trung gian là phê duyệt cho phép chỉ truy cập tạm thời vào hệ thống quản trị và ghi nhật ký phiên truy cập đối với người quản trị hệ thống;

• Hạn chế truy cập, chỉ cho người vận hành được cấp quyền;

• Loại bỏ các phần mềm không cần thiết;

---

[10] Out-of-band: cách truy cập vào các thiết bị mạng thông qua một kênh truyền tín hiệu riêng biệt (các cổng console, các thiết bị chuyển đổi hoặc cổng dịch vụ riêng biệt được thiết kế trên từng thiết bị); phương pháp truy cập này cho phép giám sát, điều khiển các thiết bị mạng bất cứ lúc nào.

[11] In-bank: cách truy cập vào các thiết bị mạng thông qua cổng Ethernet, sử dụng các giao thức như Telnet, VNC, RDP hoặc SSH.

- Hạn chế hoặc cấm các hoạt động nguy hại (ví dụ, việc gửi/nhận email).

– Hạn chế quyền quản trị vào hệ thống CITAD, chỉ cho phép truy cập theo một số cổng (ports), giao thức truy cập và địa chỉ IP cụ thể.

e) Phân tách khỏi dịch vụ xác thực dùng chung

– Để bảo vệ vùng an toàn khỏi sự đánh cắp thông tin xác thực và/hoặc sự thỏa hiệp của các dịch vụ xác thực (ví dụ: LDAP, Radius[12], multi-factor), vùng an toàn nên sử dụng một giải pháp hoặc hệ thống xác thực phân tách với hệ thống xác thực dùng chung của thành viên hoặc sử dụng dịch vụ xác thực riêng biệt từ hệ thống xác thực dùng chung (ví dụ: sử dụng miền - domain riêng trong hệ thống dịch vụ thư mục dùng chung của thành viên cho Hệ thống CITAD).

Tùy chọn nâng cao

– Lập danh sách các ứng dụng được cài đặt, thực thi trong vùng an toàn.

– Hạn chế giao tiếp giữa các thành phần trong vùng an toàn:

+ Sử dụng danh sách kiểm soát truy cập mạng (ACL) hoặc phần mềm tường lửa (host-based firewall) để hạn chế truy cập trực tiếp giữa các máy chủ (host – to – host) trong vùng an toàn;

+ Sử dụng tường lửa phần cứng hoặc tường lửa lớp mạng (network-based firewall) riêng biệt giữa các thành phần trong vùng an toàn.

1.2.2. Kiểm soát tài khoản đặc quyền của hệ điều hành

Các yếu tố rủi ro:

– Xóa nhật ký và bằng chứng pháp lý;

– Đặc quyền hoặc quyền truy cập vượt quá mức cho phép;

– Thiếu khả năng xác minh lịch sử, nguồn gốc;

– Thay đổi hệ thống trái phép;

Mục tiêu kiểm soát: Hạn chế và kiểm soát việc phân quyền và sử dụng các tài khoản quản trị hệ điều hành.

Phạm vi kiểm soát:

– Vùng an toàn: tài khoản quản trị hệ điều hành (trên máy vật lý hoặc máy ảo).

– Nền tảng ảo hóa (còn được gọi là phần mềm ảo hóa) nội bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba) thiết lập các máy ảo hóa liên quan đến Hệ thống CITAD: các tài khoản cấp quản trị của nền tảng.

[12] Remote Authentication Dial-In User Service: Dịch vụ người dùng quay số xác thực từ xa

Yêu cầu kiểm soát: Hạn chế truy cập bằng các tài khoản quản trị hệ điều hành. Việc sử dụng tài khoản quản trị hệ điều hành cần được kiểm soát, giám sát, và chỉ sử dụng để cài đặt phần mềm, cấu hình.

Lý do kiểm soát: Việc bảo vệ chặt chẽ các tài khoản quản trị trong hệ điều hành làm giảm cơ hội sử dụng các tài khoản đặc quyền để tấn công của tin tặc (ví dụ: thực thi câu lệnh, xóa bằng chứng).

Hướng dẫn thực hiện:

– Tài khoản quản trị hệ thống được xác định như sau:

+ Windows: tài khoản Administrator được thiết lập sẵn và các tài khoản thành viên trong nhóm có quyền quản trị (ví dụ: các tài khoản có quyền sửa lỗi – debug hoặc các quyền thao tác với tập tin hệ thống). Các nhóm có quyền quản trị gồm: Enterprise Admins, Domain Admins và Local Administrator;

+ Linux/Unix: tài khoản root (User ID = 0) và các thành viên của nhóm root;

+ Mainframe: tài khoản có vai trò quản trị hệ thống (system administrator) hoặc người lập trình hệ thống (system programmer).

– Truy cập bằng tài khoản quản trị hệ thống phải được hạn chế tối đa, trừ trường hợp cần thiết phải sử dụng để cài đăt, cấu hình, bảo trì và hỗ trợ trong những tình huống khẩn cấp. Phải giới hạn khoảng thời gian sử dụng tài khoản quản trị hệ thống (ví dụ: hoạt động bảo trì hệ điều hành Windows).

– Không được đăng nhập (Log-in) với các tài khoản quản trị được thiết lập sẵn, ngoại trừ trường hợp thực thi các hoạt động đặc biệt cần thiết (ví dụ, cấu hình hệ thống) hoặc trong các tình huống khẩn cấp. Thực hiện sử dụng thay thế bằng các tài khoản cá nhân với quyền tương đương tài khoản quản trị hoặc các tài khoản có thể chuyển sang quyền truy cập cấp quản trị (ví dụ quyền 'sudo').

– Việc truy cập và sử dụng tài khoản quản trị cá nhân phải được ghi nhật ký sao cho các hành động trên tài khoản có thể được tái lập lại để xác định lý do chính của những sự cố.

– Nếu lưu trữ mật khẩu của tài khoản quản trị ra các phương tiện vật lý thì phải kiểm soát việc truy cập vào các phương tiện lưu trữ vật lý này.

– Thực hiện đổi mật khẩu tài khoản đăc quyền định kỳ hoặc khi có dấu hiệu lộ lọt.

– Xây dựng, ban hành quy chế, quy trình hướng dẫn thực hiện sử dụng tài khoản đặc quyền truy cập hệ thống.

Tùy chọn nâng cao

– Hệ thống phải được cấu hình để: (i) không cho phép đăng nhập (log-in) với các tài khoản quản trị được thiết lập sẵn, ngoại trừ việc đăng nhập qua chế độ bảo trì (ví dụ: chế độ đơn người dùng -single user mode trong Linux/Unix hoặc safe mode trong Windows); (ii) vô hiệu hóa (disable) hoặc xóa (delete) các tài khoản mặc định hoặc không có mục đích sử dụng (ví dụ tài khoản Guest,...). Điều này

ngăn chặn hiệu quả việc đăng nhập vào tài khoản dưới dạng một dịch vụ, nhóm tác vụ (batch job) thông qua các dịch vụ truy cập từ xa hoặc leo thang đặc quyền từ tài khoản khác.

1.2.3. Bảo vệ môi trường ảo hóa

Các yếu tố rủi ro:

– Truy cập trái phép;;

– Không kiểm soát được sự gia tăng các hệ thống và dữ liệu.

Mục tiêu kiểm soát: Nền tảng ảo hóa và các máy chủ ảo (Virtual Machines - VMs) cài đặt các hệ thống liên quan đến CITAD được bảo vệ với cấp độ tương tự như các hệ thống vật lý.

Phạm vi kiểm soát: Nền tảng ảo hóa (còn đươc gọi là phần mềm ảo hóa) nội bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba) và các máy chủ ảo được sử dụng để cài đặt các thành phần liên quan đến Hệ thống CITAD gồm:

– Giao diện Webservice;

– Giao diện truyền thông;

– Giao diện đồ họa người dùng;

– Các máy vận hành chuyên dùng và vận hành dùng chung;

– Máy chủ trung gian;

– Tường lửa.

Yêu cầu kiểm soát: Nền tảng ảo hóa, các máy chủ ảo và hạ tầng ảo hóa phụ trợ (ví dụ: tường lửa) được bảo vệ với cấp độ tương tự như các hệ thống vật lý

Lý do kiểm soát:

– Các biện pháp kiểm soát bảo mật áp dụng cho các hệ thống vật lý cũng được áp dụng cho các hệ thống ảo. Lớp ảo hóa bổ sung cần được chú ý thêm về bảo mật. Việc gia tăng không kiểm soát các máy chủ ảo có thể dẫn đến các máy chủ không được kiểm soát với nguy cơ rủi ro, không được cập nhật các bản vá hệ thống và tạo lỗ hổng cho việc truy cập trái phép vào dữ liệu.

– NHNN không giới hạn việc sử dụng các công nghệ ảo hóa để thiết lập các thành phần của hệ thống CITAD tại thành viên.

Hướng dẫn thực hiện:

– Nền tảng ảo hóa, các máy chủ ảo và hạ tầng ảo hóa phụ trợ được áp dụng các yêu cầu bảo mật tương tự như đối với các hệ thống và thành phần cơ sở hạ tầng khác (ví dụ: đặt trong vùng an toàn, các hạn chế truy cập đặc quyền, chính sách đăng nhập, chính sách mật khẩu, cài đặt các bản vá bảo mật, hạn chế truy cập Internet,...).

– Quét lỗ hổng bảo mật các nền tảng ảo hóa, các máy chủ ảo cài đặt các hệ thống liên quan đến CITAD.

– Các máy chủ nền tảng ảo hóa phải được bảo vệ vật lý để ngăn chặn truy cập vật lý trái phép.

– Tính cách ly của VM được đảm bảo trên nền tảng ảo hóa để ngăn: (i) di chuyển ngang ra khỏi máy ảo để truy cập hoặc tương tác với VM khác hoặc nền tảng ảo hóa; (ii) bỏ qua các điều khiển mạng thông thường lọc và/hoặc kiểm tra các kết nối với môi trường CITAD.

+ Việc lọc và kiểm tra dự kiến các luồng mạng đến các máy ảo liên quan đến CITAD được thực hiện tốt hơn bằng cách sử dụng các tài nguyên (chẳng hạn như tường lửa, kiểm tra gói hoặc lọc nội dung) bên ngoài nền tảng ảo hóa hoặc phải được thực thi ở phần mềm ảo hóa (Hypervisor);

+ Với điều kiện sự cô lập được đảm bảo trên nền tảng ảo hóa, máy ảo được lưu trữ có thể giữ phân loại (bảo mật) của chúng và được bảo mật riêng cho phù hợp (như vậy, chúng sẽ không kế thừa phân loại của máy ảo liên quan đến CITAD và phải tuân theo tất cả các kiểm soát liên quan đến CITAD) .

– Nếu xác thực đa yếu tố được triển khai để truy cập tương tác vào hệ điều hành máy ảo liên quan đến CITAD, phù hợp với yêu cầu kiểm soát 2.1.2 Xác thực đa thành tố, ngăn chặn truy cập trực tiếp vào máy ảo đó từ lớp giám sát máy ảo, xác thực đa yếu tố không được yêu cầu ở cấp quản lý nền tảng ảo hóa.

1.3. Giảm bề mặt tấn công và các lỗ hổng

1.3.1. Cập nhật bảo mật

Các yếu tố rủi ro: Khai thác các điểm yếu bảo mật đã biết.

Mục tiêu kiểm soát: Giảm thiểu sự xuất hiện của các điểm yếu kỹ thuật đã biết trên các máy tính của người vận hành và trong hạ tầng hệ thống CITAD thông qua sự hỗ trợ của nhà cung cấp, cập nhật các bản vá bắt buộc.

Phạm vi kiểm soát:

– Các máy vận hành chuyên dùng, vận hành dùng chung, máy chủ trung gian: phần cứng và phần mềm.

– Nền tảng ảo hóa (còn được gọi là phần mềm ảo hóa) nội bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba) thiết lập các máy ảo hóa liên quan đến Hệ thống CITAD và các máy quản trị tương ứng.

– Vùng an toàn: thiết bị phần cứng (gồm cả thiết bị mạng) và phần mềm.

Yêu cầu kiểm soát: Tất cả phần cứng và phần mềm bên trong vùng an toàn và máy tính của người vận hành phải trong giai đoạn hỗ trợ của nhà cung cấp, đã thực hiện nâng cấp các bản cập nhật bắt buộc và áp dụng các bản cập nhật an ninh cần thiết.

Lý do kiểm soát: Việc khoanh vùng các điểm yếu bảo mật đã biết góp phần giảm thiểu các cuộc tấn công. Quy trình cập nhật bản vá bảo mật phải toàn diện, có

thể lặp lại và được thực hiện kịp thời khi có các bản vá bảo mật để liên tục đóng các điểm yếu đã biết.

Hướng dẫn thực hiện:

– Triển khai cập nhật bảo mật:

+ Quá trình đánh giá rủi ro được thực hiện để xác định sự xử lý thích hợp nhất đối với những cập nhật/bản vá bảo mật của nhà sản xuất. Các cân nhắc về đánh giá rủi ro có thể bao gồm: báo cáo sự cần thiết của bản vá, sự giảm thiểu các kiểm soát và tác động;

+ Thành viên xác định và thiết lập lộ trình triển khai trên cơ sở sự cần thiết, loại hệ thống cần cập nhật và kiểm thử bản vá trước khi cập nhật cho hệ thống chạy chính;

+ Lưu ý: Thông thường, các bản cập nhật/vá lỗi bảo mật của hệ điều hành thường được tự động tải xuống và áp dụng trên các máy vận hành ngay sau khi nhà sản xuất công bố.

– Thực hiện cập nhật phiên bản các phần mềm của hệ thống CITAD theo lộ trình và kế hoạch của Ngân hàng Nhà nước công bố.

– Kiểm tra tính hợp lệ nguồn gốc và tính toàn vẹn của các bản cập nhật phần mềm và bảo mật.

– Trước khi áp dụng các bản cập nhật phần mềm và bảo mật, phải xác thực nguồn gốc và kiểm tra tính toàn vẹn (ví dụ: kiểm tra hợp lệ tổng thể – checksum validation) nếu có thể.

1.3.2. Nâng cao bảo mật hệ thống

Các yếu tố rủi ro:

– Tấn công bề mặt dư thừa;

– Khai thác cấu hình hệ thống không an toàn.

Mục tiêu kiểm soát: Giảm bề mặt tấn công mạng của các thành phần liên quan đến Hệ thống CITAD bằng cách nâng cao bảo mật hệ thống.

Phạm vi kiểm soát:

– Hệ điều hành của các máy vận hành chuyên dùng, máy vận hành dùng chung, máy chủ trung gian.

– Hệ điều hành của các ứng dụng liên quan đến CITAD (bao gồm cả VM)

– Nền tảng ảo hóa (còn đươc gọi là phần mềm ảo hóa) nội bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba) thiết lập các máy ảo hóa liên quan đến Hệ thống CITAD và các máy quản trị tương ứng

– Cơ sở hạ tầng phụ trợ trong vùng an toàn (ví dụ: tường lửa, bộ định tuyến).

Yêu cầu kiểm soát: Bảo mật nâng cao được tiến hành và duy trì trên tất cả các thành phần thuộc phạm vi.

Lý do kiểm soát: Nâng cao bảo mật hệ thống áp dụng nguyên tắc "đặc quyền tối thiểu – least privilege"[13] bằng cách vô hiệu hóa các tính năng và dịch vụ không cần thiết cho các hoạt động bình thường của hệ thống. Quá trình này làm giảm khả năng, đặc tính và các giao thức của hệ thống mà tin tặc có thể sử dụng để tấn công.

Hướng dẫn thực hiện:

– Tất cả các hệ thống nằm trong phạm vi được cân nhắc tối ưu theo một hoặc nhiều chỉ dẫn sau:

+ Hướng dẫn bảo mật của nhà sản xuất;

+ Hướng dẫn bảo mật đã được tiêu chuẩn hóa (ví dụ CIS, DISA STIG, NIST);

+ Theo tiêu chuẩn bảo mật nội bộ hoặc cơ quan quản lý hoặc tiêu chuẩn tương đương hướng dẫn của ngành, nhà sản xuất.

– Cấu hình nâng cao (bộ quy tắc) đã lựa chọn có thể được thay thế bởi các yêu cầu cấu hình của một ứng dụng cụ thể để duy trì hoạt động bình thường cho các hệ thống liên quan đến CITAD

– Quá trình nâng cao bảo mật tối thiểu gồm:

+ Thay đổi những mật khẩu mặc định;

+ Vô hiệu hóa hoặc loại bỏ những tài khoản người dùng không cần thiết;

+ Vô hiệu hóa hoặc hạn chế những dịch vụ, cổng hoặc giao thức không cần thiết;

+ Loại bỏ những phần mềm không cần thiết;

+ Hạn chế sử dụng các cổng vật lý (ví dụ: USB);

+ Thiết lập tùy chọn tự động khóa (ví dụ: kích hoạt chương trình bảo vệ màn hình máy tính của người dùng; tự động khóa tài khoản nếu đăng nhập tài khoản sai 5 lần trong 30 phút; yêu cầu đăng nhập lại sau 15 phút không phát sinh thao tác);

+ Điều chỉnh các cấu hình mặc định có điểm yếu.

– Các sai lệch từ các cấu hình tối ưu hệ thống phải được tài liệu hóa để làm căn cứ và xây dựng các biện pháp giảm thiểu.

– Duy trì an toàn bảo mật cho hệ thống:

+ Kiểm tra định kỳ (ít nhất hai lần một năm) các thiết lập bảo mật đối với hệ thống để khắc phục điểm yếu;

---

[13] Đặc quyền tối thiểu (least privilege): Chỉ cung cấp các chức năng cần thiết cho người dùng được ủy quyền, sao cho không ai có thể sử dụng các chức năng không cần thiết.

+ Hoặc thường xuyên áp dụng các thiết lập bảo mật cho hệ thống.

1.3.3. Bảo vệ luồng dữ liệu truyền bên ngoài

Các yếu tố rủi ro:

– Xâm phạm dữ liệu sao lưu;

– Mất tính bí mật của dữ liệu nhạy cảm.

Mục tiêu kiểm soát: Bảo vệ tính bí mật dữ liệu của hệ thống CITAD trong khi truyền nhận hoặc lưu trữ ngoài vùng an toàn.

Phạm vi kiểm soát: Dữ liệu nhạy cảm của hệ thống CITAD (ví dụ: dữ liệu sao lưu, chi tiết giao dịch, thông tin đăng nhập).

Yêu cầu kiểm soát: Dữ liệu nhạy cảm liên quan đến hệ thống CITAD khi mang ra ngoài vùng an toàn (gồm: (i) bản sao lưu hệ điều hành/ứng dụng, sao chép dữ liệu giao dịch với mục đích lưu trữ hoặc khôi phục; (ii) dữ liệu trích xuất để xử lý ngoài hệ thống) phải được bảo vệ khi lưu trữ ngoài vùng an toàn mật hoặc được mã hóa khi trao đổi.

Lý do kiểm soát:

– Thực hiện kiểm soát dữ liệu liên quan đến hệ thống CITAD trong đám mây hoặc được trích xuất từ vùng an toàn và được thao tác bởi các hoạt động vận hành (ví dụ lưu hoặc trích xuất/sao chép dữ liệu tự động/thủ công).

– Các bản sao lưu hệ điều hành, ứng dụng và dữ liệu đồng bộ các giao dịch có thể cung cấp thông tin hữu ích cho các giao dịch gian lận. Do đó, việc truyền tải, xử lý và lưu trữ bên ngoài vùng an toàn (ví dụ: giải pháp lưu trữ mạng SAN/NAS), phải được bảo vệ để ngăn chặn truy cập trái phép. Thực hiện mã hóa luồng trao đổi dữ liệu hoặc dữ liệu để bảo vệ dữ liệu trong quá trình truyền tải. Bảo vệ dữ liệu lưu trữ bằng việc mã hóa dữ liệu sao lưu, mã hóa dữ liệu trên các thiết bị lưu trữ hoặc kiểm soát truy cập và phân quyền phù hợp.

– Kiểm soát xử lý dữ liệu ngoài hệ thống gồm các hoạt động hỗ trợ, phân tích dữ liệu, báo cáo số liệu.

– Kiểm tra tính sẵn sàng của dữ liệu sao lưu.

Hướng dẫn thực hiện:

– Sao chép hoặc trích xuất dữ liệu nhạy cảm của hệ thống CITAD (gồm các thông tin chi tiết của giao dịch như người gửi, người thụ hưởng, số tài khoản, số tiền, nội dung giao dịch), phải thực hiện:

+ Mã hóa hoặc có biện pháp bảo vệ khi lưu trữ bên ngoài vùng an toàn CITAD hoặc vùng an toàn khác có các kiểm soát tương tự như vùng an toàn CITAD để đảm bảo không bị truy cập trái phép. Việc mã hóa có thể ở mức dữ liệu, tập tin, ứng dụng hoặc hệ thống;

+ Mã hóa khi trao đổi thông tin giữa các vùng an toàn (ví dụ: trao đổi dữ liệu giữa các trung tâm dữ liệu của thành viên). Có thể thực hiện mã dữ liệu hoặc mã hóa đường truyền.

– Khi sử dụng nền tảng ảo hóa từ xa (được cài đặt và/hoặc vận hành bởi bên thứ ba), thành viên nên mã hóa dữ liệu.

– Sử dụng các thuật toán mật mã đã được kiểm tra, chấp nhận rộng rãi trên thế giới (ví dụ AES, ECDHE) với độ dài khóa phù hợp theo từng trường hợp cụ thể.

– Nếu mật mã bảo vệ dữ liệu nhạy cảm liên quan đến CITAD bị xâm phạm, cần thiếp lập áp dụng mật mã và bảo vệ hoặc hủy bỏ các bản sao dữ liệu bị xâm phạm.

– Định kỳ khôi phục dữ liệu sao lưu liên quan đến hệ thống CITAD tối thiểu 1 lần trong năm để kiểm tra tính sẵn sàng sử dụng, ứng phó với sự cố khi xảy ra.

Lưu ý: Các bản sao lưu phục vụ khôi phục hệ thống hoặc hoạt động nghiệp vụ nên được duy trì trong vùng an toàn tương tự vùng an toàn CITAD.

1.3.4. Kiểm soát giao dịch

Các yếu tố rủi ro:

– Thực hiện giao dịch với một đối tác trái phép;

– Không phát hiện được bất thường hoặc hoạt động đáng ngờ;

Mục tiêu kiểm soát: Hạn chế các giao dịch bất thường.

Phạm vi kiểm soát:

– Giao diện đồ họa người dùng;

– Vùng an toàn: giao diện truyền thông, giao diện Webservice.

Yêu cầu kiểm soát: Thực hiện các biện pháp kiểm soát phát hiện, ngăn chặn và kiểm tra tính hợp lệ giao dịch để hạn chế các giao dịch bất thường.

Lý do kiểm soát: Việc thực hiện các biện pháp kiểm soát nghiệp vụ để hạn chế giao dịch đáng ngờ, phòng chống rửa tiền. Những thiết lập kiểm soát này được xác định thông qua phân tích hoạt động nghiệp vụ tại thành viên.

Hướng dẫn thực hiện:

– Thực hiện các biện pháp kiểm soát để phát hiện, ngăn chặn giao dịch đáng ngờ:

+ Hạn chế truy cập hệ thống CITAD ngoài giờ làm việc;

+ Giám sát những giao dịch bất thường (ví dụ, giá trị giao dịch lớn, thông tin người gửi, người thụ hưởng thuộc danh sách đáng ngờ,...).

– Đối chiếu giao dịch cuối ngày.

1.3.5. Nâng cao bảo mật ứng dụng

Các yếu tố rủi ro:

– Bề mặt tấn công dư thừa;

– Khai thác cấu hình ứng dụng không an toàn;

– Dễ dàng tấn công trái phép.

Mục tiêu kiểm soát: Giảm bề mặt tấn công của các thành phần liên quan đến CITAD bằng cách thực hiện nâng cao bảo mật ứng dụng cho giao diện truyền thông và các ứng dụng liên quan khác.

Phạm vi kiểm soát:

– Giao diện truyền thông;

– Giao diện đồ họa người dùng.

Yêu cầu kiểm soát: Tăng cường bảo mật ứng dụng cho các thành phần thuộc giao diện truyền thông và giao diện đồ họa người dùng.

Lý do kiểm soát: Nâng cao bảo mật ứng dụng áp dụng nguyên tắc "đặc quyền tối thiểu – least privilege" bằng cách vô hiệu hóa các tính năng và dịch vụ không cần thiết cho các hoạt động bình thường của ứng dụng. Quá trình này làm giảm khả năng, đặc tính và các giao thức của ứng dụng mà tin tặc có thể sử dụng để tấn công, đảm bảo các thông tin đăng nhập mặc định được thay đổi.

Hướng dẫn thực hiện:

– Thực hiện nâng cao bảo mật ứng dụng tối thiểu như sau:

+ Thay đổi các mật khẩu truy cập mặc định;

+ Vô hiệu hóa hoặc xóa các tài khoản người dùng không cần thiết;

+ Vô hiệu hóa hoặc hạn chế các thành phần hoặc phương thức kết nối không cần thiết

+ Cấu hình an toàn các kết nối từ xa;

+ Loại bỏ các gói, chương trình hoặc ứng dụng không cần thiết;

+ Tinh chỉnh các cấu hình mặc định được cho là dễ bị tấn công.

1.4. Bảo mật vật lý môi trường hoạt động

1.4.1. An toàn vật lý

Các yếu tố rủi ro:

– Thiếu khả năng xác minh lịch sử, nguồn gốc;

– Truy cập vật lý trái phép.

Mục tiêu kiểm soát: Ngăn chặn truy cập trái phép vào môi trường làm việc, thiết bị lưu trữ, máy chủ cài đặt ứng dụng CITAD, thiết bị chứa thông tin nhạy cảm.

Phạm vi kiểm soát:

– Máy vận hành chuyên dùng, máy vận hành dùng chung, máy trung gian và các thiết bị có thể tháo rời khác.

– Vùng an toàn: tất cả phần cứng.

– Phần cứng hỗ trợ nền tảng ảo hóa (còn được gọi là phần mềm ảo hóa) cục bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba), được dùng để thiết lập các máy ảo hóa để cài đặt các thành phần liên quan đến Hệ thống CITAD.

Yêu cầu kiểm soát: Các biện pháp kiểm soát an ninh vật lý được áp dụng để bảo vệ truy cập vào thiết bị chứa thông tin nhạy cảm, thiết bị lưu trữ, máy chủ cài đặt ứng dụng CITAD.

Lý do kiểm soát: Việc triển khai các biện pháp kiểm soát bảo mật vật lý sẽ bảo vệ chống lại các mối đe dọa từ bên trong và bên ngoài, đồng thời giảm các cuộc tấn công cơ hội được kích hoạt bằng cách truy cập vào các hệ thống vật lý.

Hướng dẫn thực hiện:

– Bảo mật thiết bị có thể tháo rời:

+ Thiết bị tháo rời nhạy cảm (ví dụ: USB token, Thiết bị mật khẩu theo thời gian Time-Based One-Time Password TOTP) phải được kiểm soát, hay lưu giữ một cách an toàn khi không sử dụng;

+ Thiết bị tháo rời nhạy cảm cần thiết để vận hành hệ thống hoạt động liên tục bình thường (ví dụ: thiết bị HSM, ổ đĩa thay thế nóng[14]- hot swappable disks) được lưu trữ trong trung tâm dữ liệu hoặc tối thiểu là trong phòng có khóa;

+ Phương tiện sao lưu (ví dụ: băng từ) được bảo vệ về mặt vật lý.

– Bảo mật môi trường làm việc:

+ Các máy vận hành được đặt trong một môi trường làm việc an toàn, truy cập được kiểm soát và cấp quyền chỉ cho các nhân viên vận hành/quản trị và những người được cấp quyền. Không phải thiết lập một khu vực vật lý riêng cho các máy vận hành truy cập vào hệ thống CITAD;

+ Các máy in sử dụng cho giao dịch CITAD phải được đặt trong môi trường làm việc an toàn và hạn chế truy cập;

+ Truy cập USB và các điểm truy cập ngoại vi trên máy vận hành phải được vô hiệu hóa ở mức tối đa có thể, trong khi vẫn hỗ trợ vận hành (ví dụ: thiết bị Ikey để xác thực giao dịch).

---

[14] Các ổ đĩa có khả năng thay thế khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

– Bảo mật đối với nhân viên làm việc từ xa:

+ Bảo mật trong khi sử dụng ở môi trường công cộng;

+ Thiết lập chính sách sử dụng các thiết bị cá nhân (ví dụ: không được sử dụng máy tính cá nhân để truy cập cơ sở hạ tầng CTIAD, tuy nhiên, thiết bị di động cá nhân có thể được sử dụng làm yếu tố xác thực thứ hai);

+ Hạn chế truy cập bất hợp pháp tới các thiết bị được sử dụng để truy cập hệ thống CITAD (ví dụ, hạn chế người thân trong gia đình hoặc bạn bè sử dụng, truy cập vào các thiết bị được sử dụng làm việc từ xa);

+ Yêu cầu truy cập từ xa (khuyến nghị xác thực đa thành tố khi sử dụng VPN);

+ Bảo vệ các thiết bị di động được sử dụng để xác thực, ví dụ OTP (khuyến nghị đặt mật khẩu và tự động khóa thiết bị di động);

+ Báo cáo các sự cố bảo mật (ví dụ: trộm cắp) trong quá trình làm việc từ xa.

2. Kiểm soát và giới hạn các truy cập

2.1. Ngăn chặn xâm phạm thông tin đăng nhập

2.1.1. Xác thực đa thành tố

Các yếu tố rủi ro:

– Tấn công phát lại thông tin xác thực[15];

– Bẻ khóa, đoán mật khẩu hoặc xâm phạm khác;

– Đánh cắp mật khẩu.

Mục tiêu kiểm soát: Ngăn chặn sự xâm phạm vào hệ thống hoặc ứng dụng CITAD bằng cách triển khai xác thực đa thành tố.

Phạm vi kiểm soát:

– Truy cập vào máy vận hành chuyên dùng;

– Truy cập vào máy trung gian;

– Truy cập vào máy chủ cài đặt giao diện truyền thông, giao diện Webservice;

– Truy cập vào cơ sở hạ tầng CITAD từ xa (cài đặt hoặc/và vận hành bởi bên thứ ba).

Yêu cầu kiểm soát: Xác thực đa yếu tố được áp dụng cho người dùng tương tác truy cập đến Hệ thống CITAD.

---

[15] Hình thức tin tặc nghe trộm quá trình giao tiếp qua mạng bảo mật, chặn giao tiếp, trì hoãn, lấy thông tin xác thực để tấn công hệ thống.

Lý do kiểm soát: Xác thực đa yếu tố yêu cầu trình bày hai hoặc nhiều yếu tố xác thực phổ biến được đề cập dưới đây:

– Yếu tố đã biết (điều mà người vận hành biết): điển hình là mật khẩu.

– Yếu tố sở hữu (thứ mà người vận hành có), thường là:

+ Mã thông báo có kết nối (ví dụ: USB token, thẻ thông minh);

+ Mã thông báo không có kết nối (ví dụ: trình tạo mật khẩu một lần sử dụng trên điện thoại di động, mã thông báo RSA hoặc thiết bị xác thực Digipass).

– Yếu tố sinh học (đặc điểm của người vận hành), ví dụ: vân tay, quét võng mạc hoặc nhận dạng giọng nói.

Việc triển khai xác thực đa yếu tố cung cấp một lớp bảo vệ bổ sung chống lại các cuộc tấn công xác thực thông thường (ví dụ: tấn công qua vai – shoulder surfing, sử dụng lại mật khẩu, hoặc mật khẩu yếu) và cung cấp khả năng bảo vệ cao hơn khỏi sự xâm nhập tài khoản để xử lý giao dịch độc hại. Tin tặc thường sử dụng các đặc quyền của một tài khoản bị xâm nhập để di chuyển theo bên trong một môi trường và tiến hành một cuộc tấn công.

Hướng dẫn thực hiện:

– Phải thực hiện xác thực đa thành tố ít nhất 01 lần trong quá trình người dùng quản trị hệ thống truy cập các máy chủ cài đặt Hệ thống CITAD hoặc người dùng cuối truy cập Hệ thống CITAD.

+ Đối với người dùng quản trị hệ thống:

- Tại vùng biên của vùng an toàn (truy cập vào máy chủ trung gian);
- Tại vùng an toàn (truy cập vào máy vận hành chuyên dùng; máy chủ cài đặt giao diện truyền thông, giao diện Webservice).

+ Đối với người dùng cuối (thứ tự ưu tiên áp dụng xác thực đa thành tố giảm dần):

- Tại vùng biên của vùng an toàn (truy cập vào máy chủ trung gian);
- Tại vùng an toàn (truy cập vào máy vận hành chuyên dùng).

– Xác thực đa yếu tố được thiết lập đối với truy cập quản trị của người dùng từ xa (VPN Authentication).

– Hệ thống xác thực đa yếu tố bị lộ nhiều hơn nếu thông tin xác thực được lưu trữ bên ngoài vùng an toàn (ví dụ: lưu trữ trong dịch vụ thư mục dùng chung – Enterprise Active Directory). Nếu có thể, hệ thống xác thực đa thành tố phải được đặt trong vùng an toàn.

– Những yếu tố xác thực phải gắn với cá nhân và đảm bảo trách nhiệm cá nhân khi truy cập dịch vụ, hệ điều hành và ứng dụng.

– Nếu triển khai hệ thống Single Sign-On (ví dụ: SAML) thì yếu tố xác thực thứ hai vẫn phải được yêu cầu tại Single Sign-On, hay tại các giai đoạn xác thực sau đó.

2.2. Quản trị định danh và các đặc quyền

2.2.1. Thẩm tra nhân sự

Các yếu tố rủi ro: Nhân viên vận hành không đáng tin cậy.

Mục tiêu kiểm soát: Đảm bảo độ tin cậy của nhân viên vận hành hệ thống CITAD bằng cách thực hiện việc thẩm tra nhân sự phù hợp với luật và quy định hiện hành của thành viên.

Phạm vi kiểm soát: Tất cả nhân sự (ví dụ: nhân viên, nhà tư vấn và nhà thầu) có quyền truy cập vận hành (bảo trì hoặc quản trị) vào các hệ thống liên quan đến CITAD, nền tảng ảo hóa cục bộ hoặc từ xa thiết lập các máy ảo cho hệ thống CITAD.

Yêu cầu kiểm soát: Thẩm tra nhân viên vận hành cơ sở hạ tầng CITAD trước khi giao nhiệm vụ lần đầu và thẩm tra định kỳ sau khi giao nhiệm vụ.

Lý do kiểm soát: Quá trình thẩm tra nhân sự thông qua nội bộ hoặc thuê ngoài, góp phần đảm bảo rằng các nhân viên vận hành hoặc quản trị của cơ sở hạ tầng CITAD đáng tin cậy và giảm nguy cơ bị đe dọa từ nội bộ.

Hướng dẫn thực hiện: Trong phạm vi được phép theo luật và quy định hiện hành và trong phạm vi thông tin có sẵn, các hướng dẫn được khuyến nghị gồm:

– Xác minh lý lịch các nhân viên thuộc phạm vi tối thiểu 05 năm/lần. Đối với nhân viên đã giao nhiệm vụ nhưng chưa được xác minh, thực hiện xác minh lại.

– Quy trình xác minh lý lịch tuyển dụng nhân sự gồm các nội dung sau (được tiến hành theo luật và quy định hiện hành của thành viên):

+ Xác minh danh tính;

+ Xác nhận đầy đủ thông tin chi tiết về bằng cấp;

+ Xác nhận quá trình làm việc trước đây;

+ Làm rõ các tố tụng dân sự hoặc hình sự trong quá khứ hoặc đang trong quá trình xử lý đối với người lao động;

+ Kiểm tra sự tham gia vào các tổ chức, doanh nghiệp khác có thể dẫn đến xung đột lợi ích;

+ Xác minh tín dụng tài chính.

– Quy trình thẩm tra định kỳ bao gồm các xác minh sau (được tiến hành theo quy định của pháp luật và quy định của thành viên):

+ Làm rõ các tố tụng dân sự hoặc hình sự trong quá khứ hoặc đang trong quá trình xử lý đối với người lao động;

+ Kiểm tra sự tham gia vào các tổ chức, doanh nghiệp khác có thể dẫn đến xung đột lợi ích;

+ Xác minh tín dụng tài chính.

2.2.2. Lưu trữ mật khẩu theo hình thức vật lý hoặc logic

Các yếu tố rủi ro: Đánh cắp mật khẩu.

Mục tiêu kiểm soát: Bảo vệ về mặt vật lý và logic các phiên bản mật khẩu được ghi lại.

Phạm vi kiểm soát: Tài khoản và mật khẩu được xác định trong các trường hợp sau:

– Máy vận hành chuyên dùng, máy vận hành dùng chung, máy trung gian: để truy cập hệ điều hành.

– Máy vận hành chuyên dùng, máy vận hành dùng chung, máy trung gian: phiên làm việc của người dùng.

– Vùng an toàn: tất cả các ứng dụng, hệ điều hành, HSM và thiết bị token liên quan, các thành phần mạng.

– Nền tảng ảo hóa (còn được gọi là phần mềm ảo hóa) nội bộ hoặc từ xa (thuê đặt và/hoặc vận hành bởi bên thứ ba) thiết lập các máy ảo hóa liên quan đến Hệ thống CITAD.

Yêu cầu kiểm soát: Bảo vệ với quyền truy cập bị hạn chế trên cơ sở nguyên tắc cần biết (need-to-know) các mật khẩu được ghi lại lưu trữ ở một vị trí vật lý hoặc logic.

Lý do kiểm soát:

– Việc lưu trữ an toàn các mật khẩu đã được ghi lại (kho lưu trữ) đảm bảo rằng mật khẩu không dễ bị người khác truy cập, bảo vệ chống lại việc đánh cắp mật khẩu đơn giản. Các phương pháp lưu trữ mật khẩu an toàn phổ biến gồm (danh sách không đầy đủ): ghi lại mật khẩu vào tập tin và lưu trữ trên máy tính hoặc thư mục chia sẻ trên máy chủ hoặc điện thoại di động; viết/in ra giấy ghi chú hoặc tờ rơi.

– Kiểm soát này bao gồm việc lưu trữ các mật khẩu khẩn cấp, đặc quyền hoặc bất kỳ mật khẩu nào khác. Tất cả các tài khoản phải được xem xét vì (i) sự kết hợp của các tài khoản không đặc quyền bị xâm phạm có thể gây hại, ví dụ tài khoản tạo giao dịch và tài khoản phê duyệt (ii) các tài khoản giám sát cũng cung cấp thông tin có giá trị trong thời gian thu thập thông tin.

Hướng dẫn thực hiện:

– Bảo vệ mật khẩu được ghi ra các phương tiện vật lý:

+ Lưu trữ trong một phong bì đảm bảo chống giả mạo, được niêm phong;

+ Lưu trữ trong két sắt an toàn;

+ Ghi nhật ký khi truy cập vị trí lưu trữ và các mật khẩu được sử dụng.

– Bảo vệ mật khẩu được lưu trữ logic (hình thức số hóa):

+ Mã hóa một phần hoặc toàn bộ (nghĩa là không lưu trữ dạng rõ);

+ Xác thực khi truy cập vào nơi lưu trữ và ghi nhật ký truy cập.

– Không ghi mật khẩu vào sổ tay hướng dẫn sử dụng hoặc tài liệu vận hành (nếu ghi ra các phương tiện này thì phải lưu trữ theo các hướng dẫn trên).

– Nếu sử dụng mật khẩu trong trường hợp khẩn cấp cho người vận hành (không được phân quyền sử dụng trong hoạt động bình thường) thì phải thay đổi mật khẩu sau khi sử dụng.

– Không lưu trữ (hardcode) mật khẩu trong tập tin kịch bản hoặc mã nguồn chương trình.

3. Ứng phó sự cố an ninh mạng

3.1. Kế hoạch ứng phó sự cố an ninh mạng

3.1.1. Lập kế hoạch ứng phó sự cố an ninh mạng

Các yếu tố rủi ro: Thiệt hại tăng thêm do thiếu khả năng sẵn sàng trước các sự cố an ninh mạng.

Mục tiêu kiểm soát: Đảm bảo việc quản lý các sự cố an ninh mạng theo cách thống nhất và hiệu quả.

Phạm vi kiểm soát: Kiểm soát mức tổ chức.

Yêu cầu kiểm soát: Người dùng có kế hoạch ứng phó đối với sự cố mạng đã được xác định và thử nghiệm trước đó.

Lý do kiểm soát: Sự sẵn sàng và khả năng phục hồi thích hợp là điều quan trọng hàng đầu đối với tổ chức. Xác định và thử nghiệm kế hoạch ứng phó sự cố mạng là một cách hiệu quả cao để giảm tác động và thời gian ảnh hưởng của một sự cố an ninh mạng.

Hướng dẫn thực hiện:

– Xây dựng và cập nhật hàng năm Kế hoạch phản ứng sự cố an ninh mạng cho Hệ thống CITAD, gồm các nội dung tối thiểu như sau[16]:

+ Phạm vi và đối tượng của kế hoạch; thông tin liên hệ, chức năng, nhiệm vụ của các lực lượng tham gia ứng phó sự cố;

+ Đánh giá các nguy cơ, sự cố an toàn thông tin mạng;

+ Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể;

+ Công tác triển khai điều phối, xử lý, ứng cứu sự cố tại thành viên;

[16] Tham khảo Đề cương kế hoạch ứng phó sự cố an toàn thông tin mạng ban hành kèm theo Thông tư 20/2017/TT-BTTT ngày 12/9/2017

+ Công tác triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố;

+ Các giải pháp đảm bảo, tổ chức triển khai kế hoạch và kinh phí.

VI. MA TRẬN KIỂM SOÁT RỦI RO

Bảng 2: Ma trận kiểm soát rủi ro

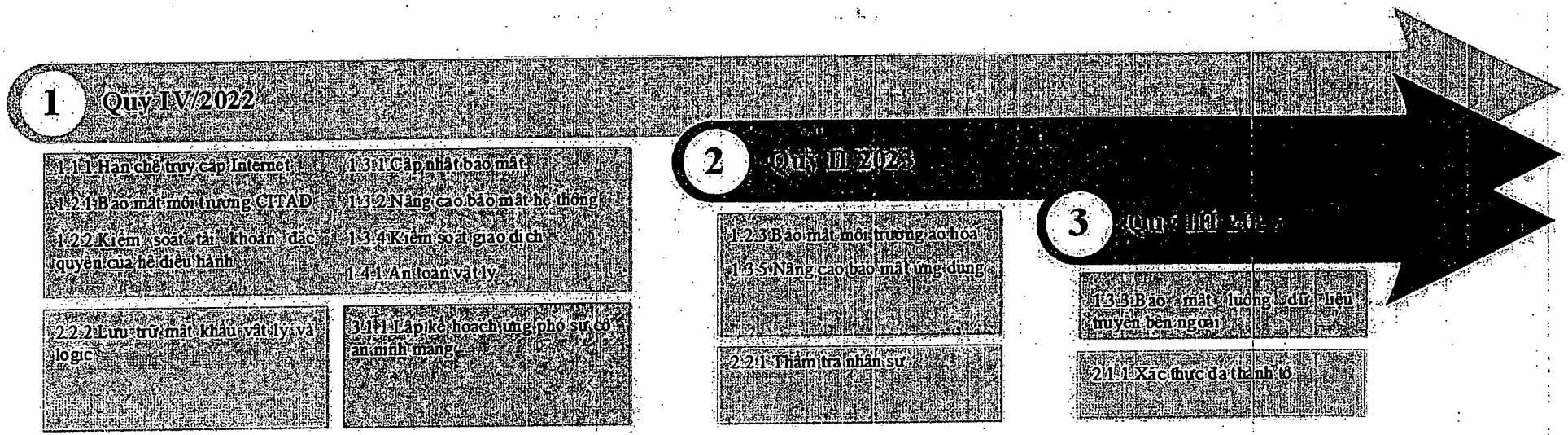
		1.1.1	1.2.1	1.2.2	1.2.3	1.3.1	1.3.2	1.3.3	1.3.4	1.3.5	1.4	2.1.1	2.2	2.2.1	3.1.1
1	Thực hiện giao dịch với một đối tác trái phép								●						
2	Xâm phạm hệ thống xác thực của thành viên		●												
3	Xâm phạm dữ liệu sao lưu							●							
4	Xâm phạm các thông tin đăng nhập		●												
5	Tấn công phát lại thông tin xác thực		●									●			
6	Xóa nhật ký và bằng chứng pháp lý			●											
7	Tấn công bề mặt dư thừa						●			●					
8	Thiệt hại tăng thêm do thiếu khả năng sẵn sàng trước các sự cố an ninh mạng														●
9	Đặc quyền hoặc quyền truy cập vượt quá mức cho phép			●											
10	Khai thác cấu hình hệ thống không an toàn						●			●					
11	Khai thác các điểm yếu bảo mật đã biết					●									
12	Các cuộc tấn công từ Internet	●	●												
13	Thiếu khả năng xác minh lịch sử, nguồn gốc			●							●				
14	Mất tính bí mật của dữ liệu nhạy cảm							●							
15	Bẻ khóa mật khẩu, đoán hoặc xâm phạm khác											●			
16	Đánh cắp mật khẩu											●		●	

		1.1.1	1.2.1	1.2.2	1.2.3	1.3.1	1.3.2	1.3.3	1.3.4	1.3.5	1.4.1	2.1.1	2.2.1	2.2.2	3.1.1
17	Truy cập trái phép		•		•										
18	Truy cập vật lý trái phép										•				
19	Thay đổi hệ thống trái phép			•											
20	Không kiểm soát được sự gia tăng các hệ thống và dữ liệu.				•										
21	Không phát hiện được bất thường hoặc hoạt động đáng ngờ								•						
22	Nhân viên vận hành không đáng tin cậy												•		
23	Dễ dàng tấn công trái phép									•					
24	Xâm phạm các thông tin mật		•												

14 yêu cầu kiểm soát của Hướng dẫn ATTT đưa ra các biện pháp cần thực hiện tại thành viên để kiểm soát, giảm thiểu 24 rủi ro an toàn thông tin có thể xảy ra. Ma trận kiểm soát rủi ro là bảng tổng hợp ánh xạ các rủi ro an toàn thông tin (hàng dọc) với yêu cầu kiểm soát (hàng ngang).

- cho biết rủi ro an toàn thông tin (hàng ngang) sẽ được giảm thiểu khi thực hiện biện pháp kiểm soát tương ứng (hàng dọc).

VII. LỘ TRÌNH ÁP DỤNG



Hình 6: Lộ trình áp dụng các yêu cầu

Thành viên rà soát hiện trạng triển khai, vận hành, khai thác Hệ thống CITAD tại thành viên để áp dụng được nhiều yêu cầu kiểm soát, thời điểm áp dụng sớm nhất, đảm bảo an toàn hoạt động của hệ thống. Đến hết quý III/2023 (theo lộ trình áp dụng nêu trên), các yêu cầu bắt buộc tại Hướng dẫn ATTT cần phải được áp dụng. Trường hợp vướng mắc, thành viên cần giải trình lý do, đề xuất phương án, lộ trình cụ thể gửi NHNN (Cục Công nghệ thông tin) để phối hợp thực hiện, đảm bảo an toàn thông tin chung cho toàn hệ thống TTĐTLNH.

VIII. SO SÁNH VỚI CÁC TIÊU CHUẨN VÀ QUY ĐỊNH HIỆN HÀNH

TT	Các yêu cầu kiểm soát của Hướng dẫn ATTT	Tiêu chuẩn TCVN ISO/IEC 27002:2020	Các quy định hiện hành của NHNN về an toàn thông tin đối với hoạt động của Hệ thống CITAD
1	1.1.1. Hạn chế truy cập Internet	13.1.3 Phân tách mạng	Điều 31 Thông tư 09/2020 /TT-NHNN ngày 21/10/2020 Điều 13, Điều 14 Quyết định số 1820/QĐ-NHNN ngày 26/10/2020
2	1.2.1. Bảo vệ môi trường CITAD	13.1.3 Phân tách mạng	Điều 23 Thông tư 09/2020/TT-NHNN ngày 21/10/2020 Điều 4, Điều 5, Điều 12 Thông tư 35/2016/TT-NHNN ngày 29/12/2016 Điều 12 Quyết định số 1820/QĐ-NHNN ngày 26/10/2020
3	1.2.2. Kiểm soát tài khoản đặc quyền của hệ điều hành	9.2.3 Kiểm soát đặc quyền truy cập	Điều 28 Thông tư 09/2020/TT-NHNN ngày 21/10/2020 Điều 7 Quyết định số 1820/QĐ-NHNN ngày 26/10/2020
4	1.2.3. Bảo vệ môi trường ảo hóa		
5	1.3.1. Cập nhật bảo mật	12.6.1 Quản lý các lỗ hổng kỹ thuật	Điều 42, Điều 43 Thông tư 09/2020/TT-NHNN ngày 21/10/2020 Điều 19 Quyết định số 1820/QĐ-NHNN ngày 26/10/2020
6	1.3.2. Nâng cao bảo mật hệ thống	14.1.1 Phân tích và đặc tả các yêu cầu về an toàn thông tin	

TT	Các yêu cầu kiểm soát của Hướng dẫn ATTT	Tiêu chuẩn TCVN ISO/IEC 27002:2020	Các quy định hiện hành của NHNN về an toàn thông tin đối với hoạt động của Hệ thống CITAD
7	1.3.3. Bảo vệ luồng dữ liệu truyền bên ngoài	13.2.1 Các chính sách và thủ tục truyền tải thông tin	Điều 24 Thông tư 09/2020/TT-NHNN ngày 21/10/2020
8	1.3.4. Kiểm soát giao dịch	13.2.2 Các thỏa thuận truyền tải thông tin	Điều 16, Điều 17 Thông tư số 37/2016/TT-NHNN ngày 30/12/2016
9	1.3.5. Nâng cao bảo mật ứng dụng	14.1.1 Phân tích và đặt tả các yêu cầu về an toàn thông tin	
10	1.4.1. An toàn vật lý	11.1.1 Vành đai an toàn vật lý 11.1.2 Kiểm soát lối vào vật lý 11.1.3 Bảo vệ các văn phòng, phòng làm việc và vật dụng 11.1.4 Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường 11.1.5 Làm việc trong các khu vực an toàn	
11	2.1.1. Xác thực đa thành tố	9.4.2 Các thủ tục đăng nhập an toàn	
12	2.2.1. Thẩm tra nhân sự	7.1.1 Thẩm tra	Điều 14, Điều 15 Thông tư số 09/2020/TT-NHNN ngày 21/10/2020 Điều 11 Quyết định số 1820/QĐ-NHNN ngày 26/10/2020
13	2.2.2. Lưu trữ mật khẩu vật lý và logic	9.4.3 Hệ thống quản lý mật khẩu	

TT	Các yêu cầu kiểm soát của Hướng dẫn ATTT	Tiêu chuẩn TCVN ISO/IEC 27002:2020	Các quy định hiện hành của NHNN về an toàn thông tin đối với hoạt động của Hệ thống CITAD
14	3.2.1. Lập kế hoạch ứng phó sự cố mạng	16.1.1 Trách nhiệm và thủ tục	

PHỤ LỤC 1: DANH MỤC TÀI LIỆU THAM KHẢO

[1]. SWIFT Customer Security Controls Framework v20201 (Customer Security Programme)

[2]. Thông tư số 09/2020/TT-NHNN ngày 21/10/2020 của Ngân hàng Nhà nước Việt Nam quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng

[3]. Thông tư số 37/2016/TT-NHNN ngày 30/12/2016 của Ngân hàng Nhà nước Việt Nam quy định về việc quản lý, vận hành và sử dụng Hệ thống Thanh toán điện tử liên ngân hàng Quốc gia

[4]. Thông tư số 35/2016/TT-NHNN ngày 29/12/2016 của Ngân hàng Nhà nước quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet

[5]. Quyết định số 1820/QĐ-NHNN ngày 26/10/2020 Ngân hàng Nhà nước ban hành Quy chế an toàn bảo mật hệ thống thông tin của Ngân hàng Nhà nước

[6]. TCVN 11238:2015 (ISO/IEC 27000:2014) "Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng" (Information technology – Security techniques – Information security management systems – Overview and vocabulary)

[7]. TCVN 12480:2019 (ISO/IEC 17788:2014) "Công nghệ thông tin - Tính toán đám mây - Tổng quan và từ vựng" (Information technology – Cloud Computinig – Overview and vocabulary)

[8]. TCVN 27002:2020 (ISO/IEC 27002:2013) "Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành biện pháp kiểm soát an toàn thông tin" (Information technology - Security techniques - Code of practice for information security controls)

[9]. TCVN 27001:2019 (ISO/IEC 27001:2013) "Công nghệ thông tin - Các kỹ thuật an toàn – Hệ thống quản lý an toàn thôn gtin – Các yêu cầu" (Information technology - Security techniques – Information security management systems - Requirements)

[10]. TCVN 11780:2017 (ISO/IEC 27032:2012) "Công nghệ thông tin - Các kỹ thuật an toàn – Hướng dẫn về an toàn không gian mạng" (Information technology - Security techniques – Guidelines for cybersecurity)

PHỤ LỤC 2: MẪU BÁO CÁO DÀNH CHO THÀNH VIÊN

STT	Các yêu cầu kiểm soát an toàn thông tin	Yêu cầu		Hiện trạng tuân thủ tại thành viên
		Bắt buộc	Khuyến nghị	
1. Bảo vệ an toàn môi trường hoạt động				
1.1	Hạn chế truy cập Internet			
1.1.1	*Hạn chế truy cập Internet*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
1.2	Bảo vệ các hệ thống thông tin quan trọng với môi trường CNTT dùng chung			
1.2.1	*Bảo mật môi trường CITAD*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
1.2.2	*Kiểm soát tài khoản đặc quyền của hệ điều hành*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: ....

STT	Các yêu cầu kiểm soát an toàn thông tin	Yêu cầu		Hiện trạng tuân thủ tại thành viên
		Bắt buộc	Khuyến nghị	
				☐ Khác Mô tả: ....
1.2.3	*Bảo vệ môi trường ảo hóa*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
1.3	Giảm bề mặt tấn công và các lỗ hổng			
1.3.1	*Cập nhật bảo mật*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
1.3.2	*Nâng cao bảo mật hệ thống*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác

STT	Các yêu cầu kiểm soát an toàn thông tin	Yêu cầu		Hiện trạng tuân thủ tại thành viên
		Bắt buộc	Khuyến nghị	
				Mô tả: ....
1.3.3	*Bảo vệ luồng dữ liệu truyền bên ngoài*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
1.3.4	*Kiểm soát giao dịch*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
1.3.5	*Nâng cao bảo mật ứng dụng*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....

STT	Các yêu cầu kiểm soát an toàn thông tin	Yêu cầu		Hiện trạng tuân thủ tại thành viên
		Bắt buộc	Khuyến nghị	
1.4	Bảo mật vật lý môi trường hoạt động			
1.4.1	*An toàn vật lý*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
2. Kiểm soát và giới hạn các truy cập				
2.1	Ngăn chặn xâm phạm thông tin đăng nhập			
2.1.1	*Xác thực đa thành tố*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
2.2	Quản trị định danh và các đặc quyền			
2.2.1	*Thẩm tra nhân sự*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác

STT	Các yêu cầu kiểm soát an toàn thông tin	Yêu cầu		Hiện trạng tuân thủ tại thành viên
		Bắt buộc	Khuyến nghị	
				Mô tả: ....
2.2.2	*Lưu trữ mật khẩu theo hình thức vật lý hoặc logic*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....
3. Ứng phó sự cố an ninh mạng				
3.1	Kế hoạch ứng phó sự cố an ninh mạng			
3.2.1	*Lập kế hoạch ứng phó sự cố an ninh mạng*			☐ Tuân thủ hoàn toàn ☐ Chưa tuân thủ Hiện trạng: .... Kế hoạch thực hiện: .... ☐ Khác Mô tả: ....