Đánh giá tuân thủ bảo mật cho hệ thống SWIFT

1. Tổng quan

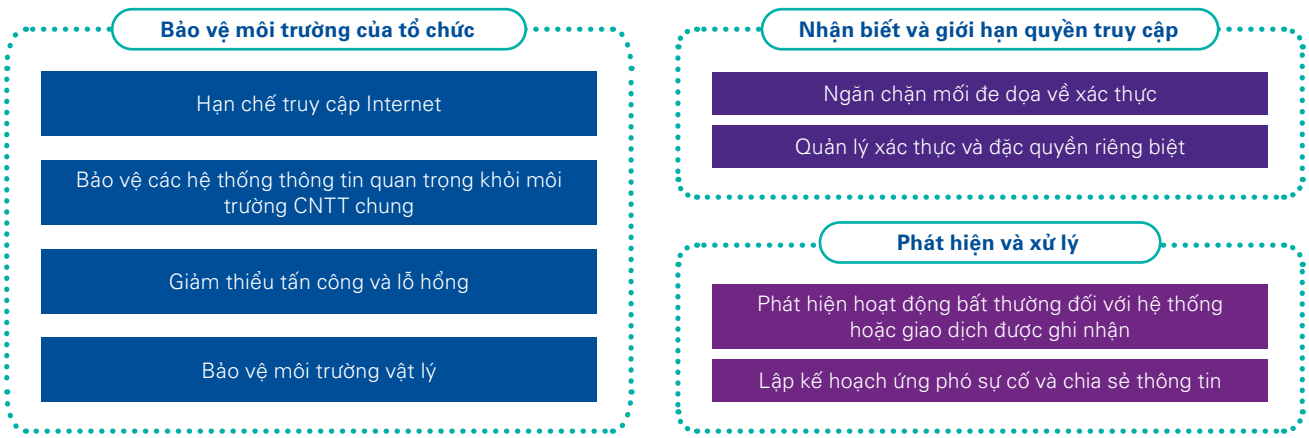
SWIFT (Hiệp hội Viễn thông Tài chính Liên ngân hàng toàn cầu) là một mạng lưới điện tín rộng lớn được nhiều ngân hàng và các tổ chức tài chính khác nhau tin tưởng và sử dụng để trao đổi các thông tin nhạy cảm cần đảm bảo độ chính xác và an toàn, chẳng hạn như lệnh chuyển tiền nhanh giữa các ngân hàng liên quốc gia, thông qua hệ thống mã chuẩn hóa được quy ước sẵn. Hệ thống SWIFT đóng vai trò cực kỳ quan trọng trong các giao dịch tiền tệ quốc tế, tuy nhiên SWIFT chỉ là một hệ thống điện tín trao đổi thông tin giao dịch - SWIFT không nắm giữ bất kỳ khoản tiền hoặc cổ phiếu chứng khoán nào, cũng như không quản lý tài khoản khách hàng.

Tại Việt Nam, chúng tôi đã có cơ hội thực hiện nhiều dự án đánh giá lỗ hổng bảo mật của hệ thống SWIFT cho các ngân hàng bản địa. Qua bài viết này, chúng tôi muốn giới thiệu với Quý khách hàng tổng quan về yêu cầu bảo mật an ninh của SWIFT, cũng như chia sẻ các kinh nghiệm thực tiễn mà chúng tôi nhận thấy được trong quá trình thực hiện các dự án đánh giá để Quý khách hàng hiểu thêm về hệ thống SWIFT cũng như các lưu ý cần thiết để triển khai và sử dụng hệ thống an toàn và bảo mật.

2. Giới thiệu Khung Kiểm soát và Rủi ro Bảo mật Thông tin của hệ thống SWIFT

Khung Kiểm soát Bảo mật Khách hàng (CSP – Customer Security Programme) của SWIFT mô tả một tập hợp các kiểm soát bảo mật bắt buộc và các kiểm soát mang tính tư vấn (kiểm soát khuyến nghị) cho các thành viên của SWIFT. Các biện pháp kiểm soát an ninh bắt buộc thiết lập một số điều kiện bảo mật tối thiểu của cơ sở hạ tầng hệ thống cần đạt được mà toàn bộ đơn vị sử dụng SWIFT phải tuân thủ. SWIFT đã chọn ưu tiên các biện pháp kiểm soát bắt buộc này để đạt được mục tiêu thực tế trong việc tăng cường bảo mật ngắn hạn, tăng bảo mật hữu hình và giảm thiểu rủi ro có thể xảy ra. SWIFT khuyến nghị người dùng thực hiện các biện pháp kiểm soát tư vấn dựa trên những kinh nghiệm đúc kết từ thực tiễn cho cả hệ sinh thái của hệ thống SWIFT. Theo thời gian, các biện pháp kiểm soát bắt buộc có thể thay đổi do bối cảnh mối đe dọa đang phát triển và một số biện pháp kiểm soát tư vấn có thể trở thành bắt buộc.

Tất cả các biện pháp kiểm soát được gắn kết xoay quanh ba mục tiêu chính: "Bảo vệ môi trường hệ thống", "Nhận biết và giới hạn quyền truy cập" và "Phát hiện và Xử lý". Các biện pháp kiểm soát được phát triển dựa trên phân tích của SWIFT về báo cáo mối đe dọa tấn công mạng, kết hợp với các khuyến nghị của các chuyên gia trong ngành và phản hồi của người dùng. Các định nghĩa kiểm soát của SWIFT được thiết kế dựa theo các tiêu chuẩn hiện có của ngành an toàn thông tin.



Hình 1: Các mục tiêu và nguyên tắc bảo mật SWIFT

SWIFT CSP 2021 ban hành 31 biện pháp kiểm soát an ninh (22 biện pháp kiểm soát bắt buộc và 9 biện pháp kiểm soát tư vấn) là cơ sở cho các mục tiêu và nguyên tắc trên. Trong mỗi biện pháp kiểm soát an ninh, SWIFT đã ghi nhận các rủi ro phổ biến nhất mà biện pháp kiểm soát sẽ giúp giảm thiểu được. Những rủi ro này cần được giải quyết nhằm mục đích ngăn ngừa hoặc giảm thiểu các hậu quả kinh doanh gian lận không mong muốn và có khả năng xảy ra, chẳng hạn như:

- Gửi hoặc sửa đổi trái phép các giao dịch tài chính
- Xử lý các giao dịch SWIFT đến (điện tín đã nhận) bị thay đổi hoặc giao dịch trái phép
- Giao dịch trái phép với các đối tác kinh doanh khác
- Vi phạm tính bảo mật (của dữ liệu kinh doanh, hệ thống máy tính Vi phạm tính toàn vẹn (của dữ liệu kinh doanh, hệ thống máy tính hoặc thông tin vận hành)

Cuối cùng, những hậu quả này có thể dẫn tới những rủi ro cấp doanh nghiệp, bao gồm:

- Rủi ro tài chính.
- Rủi ro pháp lý.
- Rủi ro tuân thủ.
- Rủi ro ảnh hưởng danh tiếng.

3. Các điểm yếu phổ biến trong Kiểm soát bảo mật SWIFT

Trong quá trình đánh giá lỗ hổng cho hệ thống SWIFT, chúng tôi đã ghi nhận một số vấn đề phổ biến mà các tổ chức tài chính thường vi phạm so với các yêu cầu bảo mật của SWIFT:

- Việc phân tách mạng cho các ứng dụng và hệ thống SWIFT chưa được thực hiện rõ ràng và đầy đủ. Ví dụ, các ứng dụng email hoặc AD vẫn có các kết nối chung với hệ thống SWIFT.
- Các chính sách và quy trình bảo mật (ví dụ: quy trình quản lý lỗ hổng bảo mật, quy trình phòng chống phần mềm độc hại, v.v.) chưa cập nhật chi tiết, chính xác và phù hợp với tình hình hiện tại của hệ thống.
- Các hướng dẫn / tiêu chuẩn nâng cao tính bảo mật cho hệ thống (security hardening) chưa được phát triển đầy đủ và hoàn thiện, đồng thời cũng không được đánh giá và cập nhật định kỳ.
- Việc dò quét lỗ hổng bảo mật chỉ được thực hiện trên các ứng dụng và máy chủ quan trọng. Đối với các thiết bị mạng hoặc cơ sở dữ liệu, việc dò quét lỗ thổng hệ thống gần như bị bỏ qua.
- Chính sách mật khẩu (độ dài mật khẩu, độ phức tạp, thời gian khóa (lockout), thời hạn thay đổi, v.v.) chỉ được áp dụng cho máy chủ Windows và chưa áp dụng trên thiết bị mạng, thiết bị bảo mật hoặc nền tảng Unix / Linux.

4. Lưu ý khi đánh giá Kiểm soát bảo mật SWIFT

Để đánh giá đầy đủ các biện pháp kiểm soát an ninh của hệ thống SWIFT, cần lưu ý những điểm quan trọng sau:

- **Hiểu biết về kiến trúc SWIFT của khách hàng:** Kiến trúc hiện tại của SWIFT được chia thành 4 loại - A1, A2, A3 và B. Mỗi kiến trúc có sự khác biệt về các thành phần và kết nối từ máy trạm đến hệ thống SWIFT. Vì vậy việc hiểu rõ từng loại kiến trúc sẽ giúp xác định được phạm vi cần đánh giá và các hệ thống liên quan có thể ảnh hưởng đến tính bảo mật của hệ thống SWIFT.
- **Hiểu biết về phạm vi kiểm soát an ninh được đánh giá:** Kiểm soát an ninh của SWIFT chỉ được áp dụng cho một phạm vi nhất định - hệ thống SWIFT và cơ sở hạ tầng gián tiếp liên quan đến SWIFT. Cần nắm rõ về các kết nối và xác định phạm vi nào sẽ áp dụng các biện pháp kiểm soát bảo mật SWIFT, tránh đánh giá các thành phần nằm ngoài phạm vi không cần thiết.

- **Nắm rõ về kiểm soát "Bắt buộc" và "Tư vấn":** Kiểm soát an ninh của SWIFT được chia thành hai loại: (1) Kiểm soát bắt buộc và (2) Kiểm soát tư vấn. Tùy thuộc vào yêu cầu của khách hàng và phạm vi đánh giá, khách hàng nên quyết định các biện pháp kiểm soát nào cần được xem xét và đánh giá theo cách phù hợp nhất.
- **Nắm rõ mục tiêu mấu chốt cần đạt được của mỗi kiểm soát:** SWIFT CSP 2021 bao gồm tổng cộng 31 kiểm soát an ninh (22 kiểm soát bắt buộc và 9 kiểm soát tư vấn) được chia thành 8 nhóm. Việc hiểu rõ mục tiêu của mỗi biện pháp kiểm soát giúp dễ dàng xác định các biện pháp kiểm soát thay thế nếu có, tránh đánh giá sai mức độ bảo mật hiện tại của khách hàng. Trong quá trình đánh giá, chúng tôi nhận thấy rằng một vài khách hàng có thể sử dụng các biện pháp kiểm soát bảo mật khác với yêu cầu của SWIFT nhưng vẫn đáp ứng được mục tiêu mấu chốt và vẫn đảm bảo sự an toàn của hệ thống SWIFT.
- **Hiểu biết về mục đích và vai trò của các thành phần trong hệ thống SWIFT:** SWIFT bao gồm nhiều thành phần với các vai trò khác nhau như: Giao thức điện tín, Giao thức truyền thông, GUI, SWIFTNet Link, HSM, Connector, v.v. Các thành phần này kết nối, tương tác và có các mối quan hệ bảo mật lẫn nhau. Do đó, việc hiểu rõ vai trò và chức năng của từng thành phần giúp xác định các biện pháp kiểm soát an ninh phù hợp với thành phần nào, từ đó đánh giá chính xác và hiệu quả nhất các rủi ro tiềm ẩn.

5. Kết luận

Trong thời đại công nghệ hiện nay, khi các giao dịch và thương mại quốc tế ngày càng trở nên phổ biến, SWIFT hiển nhiên trở thành một trong những thành phần đặc biệt quan trọng của các tổ chức tài chính và đặc biệt là các ngân hàng. Do đó, việc bảo mật SWIFT cần được quan tâm đúng mức để giảm thiểu gian lận trong giao dịch quốc tế, bảo vệ dữ liệu người dùng và uy tín của tổ chức.

Nếu Quý khách hàng cần bất cứ hỗ trợ của chúng tôi trong việc tư vấn và đánh giá bảo mật hệ thống SWIFT, xin vui lòng để lại thông tin liên lạc và yêu cầu cụ thể. Chuyên gia của chúng tôi sẽ liên lạc với Quý khách hàng sớm nhất trong vòng 24 tiếng để làm rõ thêm yêu cầu dịch vụ.

Liên hệ với chúng tôi

Trần Phương Hồng
Giám đốc tư vấn dịch vụ CNTT,
Phòng Tư vấn CNTT
T: +84 90 9988 753
E: hptran@kpmg.com.vn

Đỗ Kim Hiển
Chuyên viên tư vấn cấp cao,
Phòng Tư vấn CNTT
T: +84 94 5417 791
E: hiendo@kpmg.com.vn

Hà Nội
Tầng 46, Tòa tháp Keangnam, Hanoi Landmark Tower,
Tòa nhà 72 tầng, Lô E6, Đường Phạm Hùng, Khu đô thị mới Cầu Giấy,
Phường Mễ Trì, Quận Nam Từ Liêm, Hà Nội, Việt Nam
T: +84 (24) 3946 1600
F: +84 (24) 3946 1601
E: kpmghanoi@kpmg.com.vn

Tp. Hồ Chí Minh
Tầng 10, Tòa nhà Sunwah,
Số 115, Đường Nguyễn Huệ, Phường Bến Nghé,
Quận 1, Tp. Hồ Chí Minh, Việt Nam
T: +84 (28) 3821 9266
F: +84 (28) 3821 9267
E: kpmghcmc@kpmg.com.vn

Đà Nẵng
Lô D3, Tầng 5, Tòa nhà Indochina Riverside,
Số 74, Đường Bạch Đằng, Phường Hải Châu 1,
Quận Hải Châu, Đà Nẵng, Việt Nam
T: +84 (236) 351 9051
F: +84 (28) 3821 9267
E: kpmgdanang@kpmg.com.vn

Theo dõi chúng tôi trên:

© 2021 Công ty TNHH KPMG, Công ty TNHH Thuế và Tư vấn KPMG, Công ty Luật TNHH KPMG, đều là công ty trách nhiệm hữu hạn một thành viên được thành lập tại Việt Nam và là công ty thành viên trong tổ chức toàn cầu của các công ty KPMG độc lập, liên kết với KPMG International Limited, một công ty trách nhiệm hữu hạn theo bảo lãnh được thành lập tại Vương Quốc Anh. Tất cả các quyền được bảo hộ.

Mọi thông tin trong tài liệu này đều là thông tin chung và không nhằm mục đích cung cấp tư vấn cho trường hợp cụ thể của bất kỳ tổ chức hay cá nhân nào. Mặc dù chúng tôi cố gắng cung cấp thông tin chính xác và cập nhật nhất một cách có thể, chúng tôi không thể đảm bảo rằng những thông tin này còn chính xác lúc người đọc nhận được hoặc sẽ duy trì tính chính xác này trong tương lai. Bất cứ ai cũng không nên quyết định hành động dựa trên những thông tin trong tài liệu này nếu không có sự tư vấn phù hợp từ các chuyên gia sau khi xem xét từng tình huống cụ thể.

Tên và biểu tượng KPMG là nhãn hiệu thương mại được cấp phép sử dụng cho các công ty thành viên độc lập của tổ chức các công ty KPMG toàn cầu.

kpmg.com.vn