BẢNG SO SÁNH VÀ THUYẾT MINH NHỮNG ĐIỂM KHÁC NHAU GIỮA **DỰ THẢO THÔNG TƯ SỬA ĐỔI, BỔ SUNG** VÀ **Thông tư số 47/2014/TT-NHNN ngày 31/12/2014 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng**

**Ghi chú:** Bảng này trích dẫn những điều khoản sửa đổi, bổ sung. Phần chữ được gạch chân là phần sửa đổi, bổ sung.

| **STT** | **Thông tư 47/2014/TT-NHNN** | **Dự thảo Thông tư sửa đổi, bổ sung** | **Giải thích** |
| --- | --- | --- | --- |
|  | **Điều 2. Giải thích từ ngữ** |  |  |
| **1** | **Khoản 9**  9. Mã hóa mạnh là phương pháp mã hóa dựa trên các thuật toán đã được kiểm tra, chấp nhận rộng rãi trên thế giới cùng với độ dài khóa tối thiểu 112 (một trăm mười hai) bit và kỹ thuật quản lý khóa phù hợp. Các thuật toán tối thiểu bao gồm: AES (128 bit); TDES (112 bit); RSA (2048 bit); ECC (160 bit); ElGamal (2048 bit). | **Sửa đổi khoản 9 Điều 2**  9. Mã hóa mạnh là phương pháp mã hóa dựa trên các thuật toán đã được kiểm tra, chấp nhận rộng rãi trên thế giới cùng với độ dài khóa tối thiểu 112 (một trăm mười hai) bit và kỹ thuật quản lý khóa phù hợp. Các thuật toán tối thiểu bao gồm: AES (128 bit); TDES (168 bit); RSA (2048 bit); ECC (224 bit); ElGamal (2048 bit). | Cập nhật, điều chỉnh độ dài khóa đối với thuật toán TDES và ECC nhằm tăng tính bảo mật của các thuật toán này. |
|  | **Điều 3. Thiết lập và quản lý cấu hình thiết bị an ninh mạng** |  |  |
| **2** | **Điểm d khoản 1**  d) Không cung cấp địa chỉ mạng (địa chỉ IP) nội bộ và thông tin định tuyến cho các tổ chức khác khi chưa được người có thẩm quyền phê duyệt; | **Sửa đổi điểm d khoản 1 Điều 3**  d) Không cung cấp địa chỉ mạng (địa chỉ IP) nội bộ và thông tin định tuyến cho các tổ chức khác khi chưa được người có thẩm quyền phê duyệt. Có biện pháp che giấu địa chỉ mạng nội bộ và các thông tin về bảng định tuyến nội bộ khi kết nối với các bên thứ ba; | Bổ sung quy định về việc che giấu địa chỉ mạng nội bộ và thông tin về bảng định tuyến nội bộ nhằm giảm thiểu rủi ro an ninh mạng. |
| **3** | **Điểm a Khoản 2**  a) Giới hạn các truy cập đến môi trường dữ liệu chủ thẻ, chỉ chấp nhận các truy cập thực sự cần thiết và kiểm soát được; | **Sửa đổi điểm a khoản 2 Điều 3**  a) Giới hạn các truy cập đến môi trường dữ liệu chủ thẻ, chỉ chấp nhận các truy cập thực sự cần thiết theo thiết kế hệ thống và chặn toàn bộ các truy cập khác. Ngăn chặn kết nối Internet của các máy trạm có quyền truy cập vào dữ liệu thẻ dạng rõ (chưa che dấu, mã hóa); | Bổ sung quy định về ngăn chặn kết nối Internet của các máy trạm có quyền truy cập vào dữ liệu thẻ dạng rõ nhằm giảm thiểu rủi ro an ninh mạng liên quan đến lộ lọt dữ liệu thẻ. |
|  | **Điều 4. Thay đổi, loại bỏ hoặc vô hiệu hóa các tham số, chức năng mặc định trong hệ thống trang thiết bị phục vụ thanh toán thẻ** |  |  |
| **4** |  | **Bổ sung khoản 5 Điều 4**  5. Mã hóa tất cả các kết nối truy cập quản trị từ xa bằng phương pháp mã hóa mạnh. | Bổ sung quy định về mã hóa kết nối truy cập quản trị từ xa nhằm giảm thiểu rủi ro an ninh mạng. |
|  | **Điều 5. An toàn bảo mật trong phát triển, duy trì các trang thiết bị phục vụ thanh toán thẻ** |  |  |
| **5** |  | **Bổ sung khoản 8 Điều 5**  8. Xem xét công nghệ phần mềm ít nhất một năm một lần để xác định chúng vẫn được hỗ trợ bởi nhà sản xuất và có thể đáp ứng các yêu cầu bảo mật. Nếu phát hiện không còn được nhà cung cấp hỗ trợ hoặc không đáp ứng nhu cầu bảo mật cần lên kế hoạch khắc phục và thay thế. | Bổ sung quy định về đánh giá công nghệ phần mềm nhằm giảm thiểu rủi ro an ninh mạng. |
|  | **Điều 6. Yêu cầu cấp phát và kiểm soát tài khoản truy cập vào hệ thống thanh toán thẻ** |  |  |
| **6** | **Khoản 1 Điều 6**  1. Việc truy cập vào ứng dụng thanh toán thẻ phải được xác thực bằng ít nhất một trong các phương thức sau: mã khóa bí mật, thiết bị, thẻ xác thực và sinh trắc học. | **Sửa đổi khoản 1 Điều 6**  1. Việc truy cập vào tất cả thành phần hệ thống thanh toán thẻ phải được xác thực bằng ít nhất một trong các phương thức sau: mã khóa bí mật, thiết bị, thẻ xác thực và sinh trắc học. | Sửa đổi yêu cầu về truy cập vào hệ thống thanh toán thẻ nhằm giảm thiểu rủi ro an ninh mạng. |
| **7** | **Điểm e khoản 4 Điều 6**  e) Quy định và thực hiện việc thu hồi, loại bỏ hoặc vô hiệu hóa các tài khoản không sử dụng, hết hạn sử dụng hoặc các tài khoản trong trạng thái không kích hoạt trong một khoảng thời gian; | **Sửa đổi điểm e khoản 4 Điều 6**  e) Quy định và thực hiện việc thu hồi, loại bỏ hoặc vô hiệu hóa các tài khoản không sử dụng, hết hạn sử dụng, không hoạt động trong khoảng thời gian tối đa 90 ngày hoặc các tài khoản trong trạng thái không kích hoạt trong một khoảng thời gian; | Bổ sung nội dung về tài khoản không hoạt động trong khoảng thời gian dài nhằm giảm thiểu rủi ro an ninh mạng. |
|  | **Điều 14. Bảo vệ vùng lưu trữ dữ liệu thẻ** |  |  |
| **8** | **Điểm c khoản 1 Điều 14**  c) Số thẻ phải được che giấu khi hiển thị và chỉ được hiển thị đầy đủ khi có yêu cầu của cơ quan có thẩm quyền hoặc chủ sở hữu hợp pháp của thẻ; số thẻ phải đảm bảo không đọc được tại các nơi lưu trữ; | **Sửa đổi điểm c khoản 1 Điều 14**  c) Số thẻ phải được che giấu phù hợp khi hiển thị (chỉ hiển thị tối đa 6 số đầu và 4 số cuối) và chỉ được hiển thị đầy đủ cho một số hạn chế nhân viên có thẩm quyền để thao tác nghiệp vụ hoặc khi có yêu cầu của cơ quan có thẩm quyền hoặc chủ sở hữu hợp pháp của thẻ. Tổ chức phải lập danh sách các nhân viên có quyền xem số thẻ đầy đủ và thu hồi quyền xem số thẻ đầy đủ ngay khi nhân viên thay đổi vị trí công việc; | Bổ sung yêu cầu cụ thể về che giấu thông tin thẻ và kiểm soát nhân sự có quyền khai thác thông tin thẻ nhằm giảm thiểu rủi ro an ninh mạng. |
|  | **Điều 15. Mã hóa dữ liệu thẻ trên đường truyền qua mạng bên ngoài** |  |  |
| **9** | **Khoản 1 Điều 15**  1. Sử dụng các phương thức mã hóa và các giao thức bảo mật thích hợp (tối thiểu các giao thức SSL/TLS, SSH, IPSEC) để bảo vệ dữ liệu xác thực thẻ trong quá trình truyền thông tin qua mạng kết nối với bên ngoài (mạng Internet, mạng không dây, mạng truyền thông di động và các mạng khác). | **Sửa đổi khoản 1 Điều 15**  1. Sử dụng các phương thức mã hóa mạnh và các giao thức bảo mật an toàn để bảo vệ dữ liệu xác thực thẻ trong quá trình truyền thông tin qua mạng kết nối với bên ngoài (mạng Internet, mạng không dây, mạng truyền thông di động và các mạng khác). | Sửa đổi để phù hợp với sự thay đổi của quy định về mã hóa mạnh. |
|  | **Điều 17. Hạn chế quyền truy cập vật lý tới dữ liệu thẻ** |  |  |
| **10** | **Điểm b khoản 1 Điều 17**  b) Sử dụng camera hoặc có biện pháp khác để giám sát truy cập vật lý tới khu vực phòng máy chủ, khu vực in ấn phát hành, nơi lưu trữ, xử lý dữ liệu chủ thẻ. Các dữ liệu giám sát phải được lưu trữ tối thiểu 03 tháng. | **Sửa đổi điểm b khoản 1 Điều 17**  b) Sử dụng camera hoặc có biện pháp khác để giám sát truy cập vật lý tới khu vực phòng máy chủ, khu vực in ấn phát hành, nơi lưu trữ, xử lý dữ liệu chủ thẻ. Camera hoặc biện pháp giám sát khác phải được bảo vệ khỏi việc phá hoại hoặc vô hiệu hóa. Các dữ liệu giám sát phải được lưu trữ tối thiểu 03 tháng. | Bổ sung quy định về bảo vệ các biện pháp giám sát vật lý |
|  | **Điều 18. Giám sát, bảo vệ và kiểm tra các trang thiết bị phục vụ thanh toán thẻ** |  |  |
| **11** |  | **Bổ sung điểm i khoản 1 Điều 18**  i) Ban hành chính sách, quy trình thực hiện giám sát tất cả các truy cập tới tài nguyên mạng, dữ liệu chủ thẻ và phổ biến cho các bên liên quan. | Bổ sung yêu cầu về giám sát truy cập tới tài nguyên mạng và dữ liệu chủ thẻ của hệ thống thanh toán thẻ nhằm giảm thiểu rủi ro an ninh mạng. |