THỰC TRẠNG VÀ GIẢI PHÁP AN TOÀN THÔNG TIN TRONG LĨNH VỰC NGÂN HÀNG

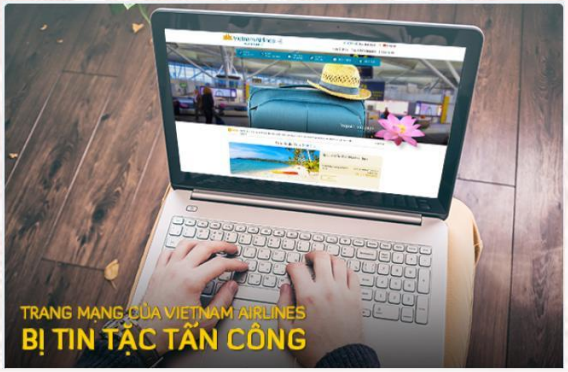
Nội dung trình bày

- Các nguy cơ mất ATTT trong ngân hàng
- Quản lý nhà nước về ATTT ngành Ngân hàng
- Thực trạng sử dụng sản phẩm ATTT trong hệ thống ngân hàng
- Các giải pháp đảm bảo ATTT hệ thống ngân hàng trong thời gian tới
- Kiến nghị, đề xuất

Các nguy cơ mất ATTT trong ngân hàng

1) **Tấn công mạng có tổ chức:**

Những diễn biến phức tạp, bất ổn về vấn đề an ninh trên thế giới, khu vực cũng hiện nay làm gia tăng nguy cơ tấn công mạng xuyên biên giới, gia tăng tội phạm mạng có tổ chức và được tài trợ bởi các chính phủ và có mục tiêu tấn công rõ ràng.



Các nguy cơ mất ATTT trong ngân hàng

2) **Sự gia tăng mã độc:**

Năm 2016, theo ghi nhận của các hãng bảo mật, số lượng mã độc mới đã gia tăng 36%, trong đó mã độc tấn công vào ngành tài chính ngân hàng cũng gia tăng tương ứng.

Đầu năm 2017, hơn 140 ngân hàng ở 40 nước bị dính malware có khả năng ẩn mình trong bộ nhớ máy tính điều khiển các hệ thống ATM nhả tiền.

Tháng 5/2017, mã độc WannaCry lan rộng hơn 150 quốc gia trong đó có Việt Nam, ảnh hưởng tới 10.000 tổ chức, 200.000 cá nhân.

Các nguy cơ mất ATTT trong ngân hàng

3) **Tấn công vào Automated Banking System:**

Xu hướng phát triển, cung cấp dịch vụ ngân hàng số với nhiều kênh dịch vụ trên môi trường mạng Internet làm xuất hiện thêm nhiều rủi ro, thách thức mới. Dự đoán trong 1-2 năm tới tin tặc sẽ tập trung các hoạt động vào việc lấy trộm tiền thông qua hệ thống ngân hàng tự động (ABS Automated Banking System)

Năm 2016, hai Ngân hàng Quốc tế Nga và Ngân hàng Metallinvestbank gánh chịu các cuộc tấn công nghiêm trọng vào hệ thống ngân hàng tự động, thiệt hại đến 1 tỷ rúp

Trong 2 năm gần đây, C50 - Bộ Công an đã phát hiện, bắt giữ hàng chục vụ trộm tiền trong tài khoản ngân hàng với thủ đoạn ăn cắp thông tin thẻ ATM, làm thẻ giả để rút tiền.

Các nguy cơ mất ATTT trong ngân hàng

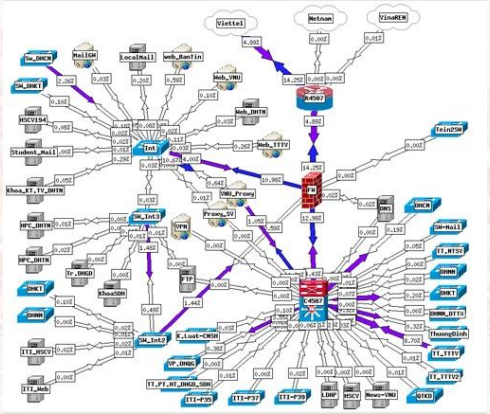
4) **Con người là điểm yếu nhất trong hệ thống:**

Hiện nay tội phạm chuyển hướng tấn công thông qua nhân viên, khách hàng sử dụng dịch vụ là những đối tượng mà nhận thức, khả năng phòng vệ kém.

Theo báo cáo khảo sát 2016 VNISA, về đối tượng đe dọa tới an toàn thông tin, ngoài tội phạm máy tính bất hợp pháp chiếm 65,3%; thì các nguy cơ mất an toàn từ cán bộ đang làm việc chiếm 9,2%; cán bộ đã nghỉ việc chiếm 5,8% và các nguy cơ khác.

Các nguy cơ mất ATTT trong ngân hàng

5) Xu hướng tập trung hóa tài nguyên, điện toán đám mây, hệ thống công nghệ ngày càng kết nối nhiều và phức tạp làm tăng nguy cơ mức độ rủi ro



Quản lý nhà nước về ATTT ngành Ngân hàng

Các VBQPPL của Nhà nước:

- *Luật Giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005;*
- *Luật an toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;*
- *Nghị định số 35/2007/NĐ-CP ngày 08/3/2007 của Chính phủ về giao dịch điện tử trong hoạt động ngân hàng;*
- *Nghị định số 26/2007/NĐ-CP ngày 15/02/2007 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số; và các nghị định sửa đổi bổ sung Nghị định 26.*
- *Thông tư 161/2016/TT-BQP ngày 21/10/2016 của Bộ Quốc phòng về việc ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng.*

Quản lý nhà nước về ATTT ngành Ngân hàng

Các VBQPPL do NHNN ban hành:

- **Thông tư số 31/2015/TT-NHNN** ngày 28/12/2015 quy định việc đảm bảo an toàn, bảo mật hệ thống CNTT trong hoạt động ngân hàng
- **Thông tư số 47/2014/TT-NHNN** ngày 31/12/2014 quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng
- **Thông tư số 35/2016/TT-NHNN** ngày 29/12/2016 ban hành quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet

Quản lý nhà nước về ATTT ngành Ngân hàng

- **Chỉ thị 03/CT-NHNN** ngày 10/01/2017 về tăng cường đảm bảo an ninh, an toàn trong thanh toán điện tử và thanh toán thẻ
- **Quyết định 630/QĐ-NHNN** ngày 31/3/2017 về ban hành Kế hoạch áp dụng các giải pháp về an toàn bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng
- **Quyết định 488/QĐ-NHNN** ngày 27/3/2017 ban hành Kế hoạch ứng dụng CNTT của các tổ chức tín dụng giai đoạn 2017-2020

Quản lý nhà nước về ATTT ngành Ngân hàng

Kiểm tra tuân thủ các VBQPPL về an ninh, bảo mật tại các TCTD

Từ 2010 đến nay, NHNN đã tiến hành hơn 80 đợt kiểm tra tuân thủ các văn bản quy phạm pháp luật về CNTT tại 62 TCTD

Thực trạng sử dụng sản phẩm ATTT trong hệ thống ngân hàng

Theo số liệu khảo sát đến cuối năm 2016:

- 100% TCTD trang thiết bị an ninh bảo mật cơ bản như hệ thống tường lửa (firewall); hệ thống phát hiện xâm nhập (IDS/IPS); hệ thống phòng chống virus; xác thực đa thành tố đối với các giao dịch điện tử.
- Trên 90% TCTD triển khai Hệ thống quản lý truy cập Internet, hệ thống phòng chống thư rác.
- Khoảng 70% TCTD định kỳ thường xuyên đánh giá các điểm yếu, lỗ hổng an ninh bảo mật của hệ thống CNTT.
- Khoảng 55% TCTD đã sử dụng giải pháp hệ thống chữ ký số dựa trên nền tảng PKI (qua hình thức thuê, tự triển khai hoặc mua) tích hợp với các hệ thống ứng dụng nghiệp vụ của ngân hàng.
- Khoảng 35% TCTD đầu tư các giải pháp an ninh bảo mật khác như: hệ thống quản lý sự kiện an ninh (SIEM); hệ thống phòng chống tấn công từ chối dịch vụ; hệ thống firewall lớp ứng dụng.

Thực trạng sử dụng sản phẩm ATTT trong hệ thống ngân hàng

Theo số liệu khảo sát đến cuối năm 2016 (*tiếp theo*):

- 20% TCTD lấy chứng chỉ đạt tiêu chuẩn PCI DSS và tiêu chuẩn ISO 27001.
- Hệ thống thẻ thanh toán chủ yếu phần lớn sử dụng thẻ từ.
- Trên 95% khách hàng sử dụng SMS OTP để xác thực các giao dịch ngân hàng điện tử. Các công nghệ xác thực mạnh như sử dụng OTP Token, ký xác thực giao dịch, chữ ký điện tử có độ an toàn cao hơn chưa được triển khai áp dụng nhiều.

Các giải pháp đảm bảo ATTT hệ thống ngân hàng trong thời gian tới

Đối với NHNN:

- Nghiên cứu, áp dụng các bộ tiêu chuẩn quốc tế trong quá trình xây dựng, ban hành VBQPPL điều chỉnh hoạt động ứng dụng CNTT của các TCTD.
- Ban hành các chính sách đẩy mạnh ứng dụng chữ ký số và các giải pháp xác thực mạnh trong các loại hình dịch vụ điện tử.
- Tổ chức triển khai hoạt động có hiệu quả mạng lưới ứng cứu sự cố an ninh CNTT; ban hành quy chế, cơ chế chia sẻ thông tin, phối hợp và chia sẻ nguồn nhân lực có trình độ chuyên môn cao.
- Tăng cường công tác kiểm tra tuân thủ các quy định về an toàn bảo mật tại các TCTD, tổ chức trung gian thanh toán để đánh giá, phát hiện, cảnh báo và xử lý sớm các rủi ro, sai phạm.

Các giải pháp đảm bảo ATTT hệ thống ngân hàng trong thời gian tới

Đối với NHNN (tiếp theo):

- Xây dựng kế hoạch truyền thông tổng thể về việc đảm bảo an toàn, bảo mật trong thanh toán điện tử và thanh toán thẻ để người dân hiểu rõ và yên tâm khi sử dụng dịch vụ thanh toán.

- Phối hợp với các cơ quan chức năng Bộ Thông tin và truyền thông, Bộ Công an, Ban Cơ yếu Chính phủ và các tổ chức cung cấp dịch vụ hạ tầng CNTT... để chia sẻ thông tin và hỗ trợ hoạt động đảm bảo an toàn, an ninh mạng của ngành Ngân hàng.

Các giải pháp đảm bảo ATTT hệ thống ngân hàng trong thời gian tới

Đối với các TCTD:

- Xây dựng và tổ chức triển khai Khung Kiến trúc CNTT, Chính sách về an ninh bảo mật CNTT, Chính sách về quản lý rủi ro CNTT tuân thủ các văn bản pháp luật của Nhà nước và các quy định của Ngân hàng Nhà nước Việt Nam.
- Thường xuyên rà soát, đánh giá rủi ro đối với toàn bộ cơ sở hạ tầng kỹ thuật CNTT và triển khai các giải pháp phù hợp để giảm thiểu rủi ro, đảm bảo an toàn hệ thống cũng như an toàn tài sản cho khách hàng.
- Nghiên cứu áp dụng các nguyên tắc, tiêu chuẩn quốc tế đối với hệ thống CNTT cũng như các ứng dụng nghiệp vụ như tiêu chuẩn ISO 27001, PCI DSS; các công nghệ xác thực mạnh, đa nhân tố mới cho các giao dịch ngân hàng.

Các giải pháp đảm bảo ATTT hệ thống ngân hàng trong thời gian tới

Đối với các TCTD (tiếp theo):

- Đẩy mạnh công tác đào tạo nâng cao nhận thức về an toàn thông tin; huấn luyện nâng cao kỹ năng nhận diện, tiếp nhận và xử lý rủi ro cho cán bộ nhân viên ngân hàng.

- Làm tốt công tác truyền thông đến khách hàng: thường xuyên, kịp thời đưa ra những cảnh báo, hướng dẫn, thông tin đầy đủ đến khách hàng để khách hàng nắm rõ các rủi ro, thủ đoạn gian lận trong hoạt động thanh toán và cách sử dụng các dịch vụ ngân hàng điện tử an toàn, bảo mật.

Các đề xuất, kiến nghị

1. Mật mã (xác thực, bảo mật, toàn vẹn, chống chối bỏ) có vai trò quyết định, đảm bảo an toàn cho giao dịch điện tử, đề nghị Ban Cơ yếu chính phủ hỗ trợ nghiên cứu ban hành đầy đủ các tiêu chuẩn về mật mã dân sự, nhất là các tiêu chuẩn áp dụng đối với các lĩnh vực cần độ an toàn cao như tài chính, ngân hàng để thống nhất tổ chức triển khai.

Các đề xuất, kiến nghị

2. Bộ TT&TT, Bộ Công an, Ban Cơ yếu Chính phủ phối hợp nghiên cứu, trình Chính phủ ban hành một số chính sách, tiêu chuẩn:

+ Chính sách quốc gia về hỗ trợ cung cấp, chia sẻ thông tin, ứng cứu sự cố an toàn thông tin; quy định việc chia sẻ trách nhiệm của các nhà cung cấp dịch vụ mạng, trang thiết bị mạng, an toàn bảo mật trong việc đào tạo nguồn nhân lực, hỗ trợ nghiên cứu chuyên sâu về an ninh bảo mật, chia sẻ thông tin và hỗ trợ ứng cứu sự cố an ninh mạng.

+ Tiêu chuẩn, hướng dẫn về công tác đảm bảo an toàn thông tin của tổ chức, cá nhân, cũng như chế tài xử phạt các vi phạm trong lĩnh vực này.

+ Chính sách đào tạo, phát triển nguồn nhân lực an ninh mạng để hình thành đội ngũ chuyên gia an ninh thông tin của Việt Nam có đủ trình độ, kinh nghiệm thực thi công tác đảm bảo an toàn, an ninh thông tin quốc gia; có chương trình, kế hoạch tuyên truyền, phổ biến kiến thức an ninh mạng cho mọi người dân.

+ Chính sách ưu tiên đầu tư, thúc đẩy các dự án nghiên cứu, sản xuất các trang thiết bị an ninh bảo mật thương hiệu Việt Nam có các tính năng kỹ thuật tương tự như các sản phẩm nhập ngoại.

XIN CẢM ƠN!