AN TOÀN BẢO MẬT TRONG HOẠT ĐỘNG NGÂN HÀNG THƯƠNG MẠI VIỆT NAM

PGS., TS. HẠ THỊ THIỀU DAO
Đại học Ngân hàng TP. Hồ Chí Minh
ThS. LẠI VĂN TÀI
Đại học Bách khoa, ĐHQG TP. Hồ Chí Minh

1. Đặt vấn đề

Đại dịch Covid-19 dù đã gây ra nhiều khó khăn, thách thức với nền kinh tế nhưng cũng tạo ra nhiều cơ hội mới, đặc biệt là thúc đẩy quá trình số hóa hệ thống ngân hàng. Thực tế thời gian qua, số lượng giao dịch qua kênh Internet và điện thoại di động liên tục tăng. Đa phần các dịch vụ cơ bản của cá nhân như gửi tiền tiết kiệm online, thanh toán hóa đơn... gần như đã được các ngân hàng triển khai hiệu quả, đáng lưu ý nhất là thay đổi tích cực trong việc cung cấp dịch vụ cho doanh nghiệp (Bảng 1). Có thể nói, hoạt động của các ngân hàng thương mại (NHTM) đã có bước tiến đáng kể cả về chất lượng lẫn số lượng. Tuy nhiên, theo khảo sát của Hiệp hội An toàn thông tin Việt Nam, hơn 50% các cuộc tấn công mạng thời gian qua nhắm vào các tổ chức tài chính, ngân hàng. Những thách thức về an toàn thông tin mạng đòi hỏi các nhà quản lý ngân hàng phải nắm được các hình thức tấn công của tội phạm công nghệ cao hiện nay, hiện trạng phòng, chống và cách thức phòng, chống để có thể chuyển đổi số an toàn và bền vững.

2. Cơ sở lý luận

2.1. Các chỉ tiêu đo lường mức độ bảo mật, an toàn cấp độ doanh nghiệp

Các phương thức tấn công của tội phạm sử dụng công nghệ cao thường sử dụng bao gồm: (1) Các hành vi lừa

Bảng 1: Một số dịch vụ trực tuyến phục vụ khách hàng phổ biến của các NHTM

Đơn vị tính: %

STT	Chỉ tiêu	2015	2016	2017	2018	2019
1	Mobile Banking	*	93,1	100,0	93,8	93,3
2	SMS Banking	-	96,6	93,8	90,6	80,0
3	Phone Banking	82,6	34,5	34,4	31,3	30,0
4	Chuyển khoản trong hệ thống của doanh nghiệp	-	89,7	96,9	96,9	96,7
5	Chuyển khoản ngoài hệ thống của doanh nghiệp	-	93,1	93,8	93,8	96,7
6	Chi trả lương nhân viên	-	82,8	87,5	84,4	87,5
7	Giao dịch tín dụng thư	-	44,8	53,1	50,0	60,0
8	Tiết kiệm điện tử cá nhân	-	89,7	90,6	93,8	96,7
9	Thanh toán hóa đơn cá nhân	-	93,1	93,8	93,8	93,3
10	Nạp tiền điện tử cá nhân	-	89,7	90,6	90,6	93,3
11	Tra cứu (số dư, giao dịch)	-	100,0	100,0	100,0	96,7
12	Chuyển khoản trong hệ thống	-	100,0	100,0	96,9	96,7
13	Chuyển khoản ngoài hệ thống	-	96,6	96,9	96,9	96,7
14	Mua thẻ trả trước	-	75,9	78,1	87,5	90,0

** - : Không có thông tin*

Nguồn: Bộ Thông tin và Truyền thông; Hội Tin học Việt Nam (2017, 2018, 2020)

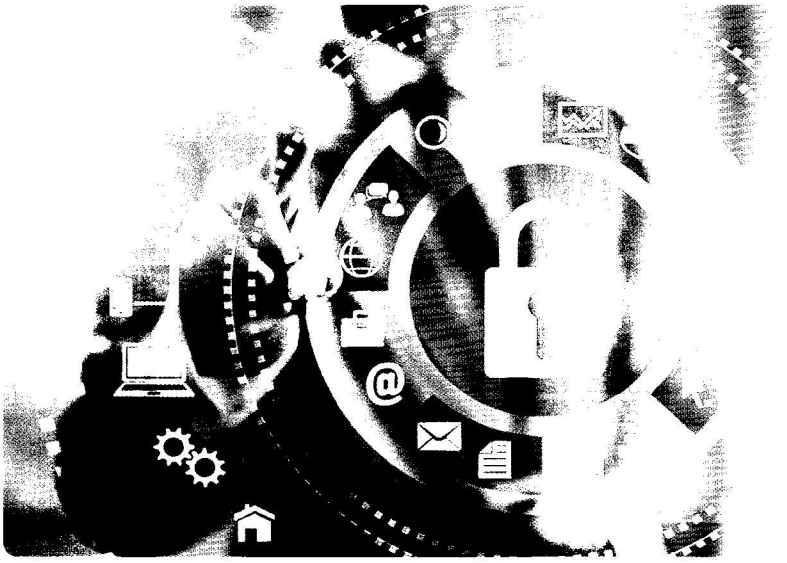
đảo trực tuyến hay tấn công giả mạo (Phishing); (2) Tấn công từ chối dịch vụ (DoS và DDos); (3) Tấn công xen giữa (Man-in-the-middle) và tấn công khai thác lỗ hổng (điểm yếu kỹ thuật); (4) Tấn công kiểu thầm lặng (gián điệp mạng); (5) Kỹ thuật xã hội (Social Engineering). Để đánh giá mức độ an toàn và bảo mật công nghệ thông tin (CNTT), các chỉ tiêu quản lý hiệu quả thường được sử dụng. Mỗi một tổ chức khác nhau thiết lập các chỉ tiêu khác nhau.

Bài viết sẽ đánh giá mức độ an toàn bảo mật trong hoạt động của các NHTM dựa trên các tiêu chí đánh giá chỉ số sẵn sàng phát triển và ứng dụng CNTT (ICT Index) của Việt Nam.

2.2. Khung tổng thể an toàn mạng

Để đảm bảo an toàn mạng đòi hỏi có sự phối hợp của tất cả các bên liên quan. Bài viết giới thiệu sơ lược khung tổng thể an toàn mạng được tổng hợp từ kinh nghiệm của Ngân hàng Trung ương Bangladesh với nghiên cứu của Karim (2016), các nước khối Ả Rập với nghiên cứu của Brahim & Ali (2016), các nước châu Phi với nghiên cứu của Kritzinger & Von Solms (2012) và một số nước phát triển khác. Các mô hình này có thể áp dụng cho Việt Nam vì khá tương đồng về tình trạng an ninh mạng, về thu nhập trung bình thấp, dân số đông, nhiều doanh nghiệp nhỏ lẻ, sử dụng chung tài nguyên, đặc biệt là tài nguyên mạng.

Kritzinger & Von Solms (2012) đề xuất bốn nội dung cần được đáp ứng đảm bảo một không gian mạng an toàn để xây dựng văn hóa mạng, cũng như để có một hệ thống thông tin an toàn cho hoạt động ngân hàng: (1) Sự quan tâm, nhận thức của các bên liên quan; (2) Sự cam kết thực hiện nghiên cứu sâu, đầy đủ về an ninh mạng của nhà nghiên cứu, nhà nước và doanh nghiệp;



(3) Sự hiểu biết về an ninh thông tin của người sử dụng mạng và nhà cung cấp dịch vụ Internet; (4) Hành động của các bên liên quan để phòng ngừa tội phạm sử dụng công nghệ cao. Theo khung tổng thể này, các hành động thực tế để phòng, chống tội phạm sử dụng công nghệ cao bao gồm: (1) Hoạt động xây dựng khung pháp lý và chính sách phù hợp; (2) Hoạt động hợp tác và kết nối giữa cơ quan quản lý, ngân hàng, các bên liên quan; (3) Hoạt động nâng cao nhận thức của cộng đồng về an ninh mạng; (4) Giải pháp kỹ thuật bảo mật và nhân lực phòng, chống tội phạm mạng.

Trong giới hạn bài viết này, nội dung thứ tư sẽ được chú trọng và chủ thể đảm nhận nhiệm vụ chính của hoạt động này là ngân hàng sẽ được phân tích cụ thể.

3. Thực trạng an toàn thông tin và đảm bảo an toàn thông tin trong lĩnh vực ngân hàng

3.1. Thực trạng tội phạm sử dụng công nghệ cao qua các hình thức tấn công

Tấn công từ chối dịch vụ và tấn công xen giữa

Tấn công từ chối dịch vụ trong lĩnh vực ngân hàng mới chỉ thấy một vụ việc. Đó là trường hợp của Ngân hàng Hợp tác xã bị tin tặc tấn công và dọa bán 275.000 dữ liệu (Trung Hiền, 2018). Bên cạnh đó, tấn công xen giữa cũng ít phổ biến ở Việt Nam (PwC, 2018; SWIFT, 2018).

Gián điệp mạng (tấn công kiểu thầm lặng)

Tháng 5/2016, TPBank đã ngăn chặn một vụ việc với kỹ thuật tương tự vụ trộm vào giữa tháng 2/2016 từ Ngân hàng Trung ương Bangladesh. TPBank đã xác định các yêu cầu đáng ngờ thông qua các tin nhắn lừa đảo trên hệ thống nhắn tin SWIFT để chuyển hơn 1 triệu USD. TPBank đã nỗ lực để ngăn chặn việc di chuyển tiền của tội phạm bằng cách liên hệ ngay với các bên liên quan. Chính vì vậy, các cuộc tấn công đã không gây ra bất kỳ tổn thất nào và nó cũng đã không có tác động đến hệ thống SWIFT nói riêng và hệ thống giao dịch giữa ngân hàng và khách hàng nói chung. TPBank cho biết, việc chuyển tiền được thực hiện bằng cơ sở hạ tầng của một nhà cung cấp bên ngoài được thuê để kết nối nó với hệ thống nhắn tin ngân hàng SWIFT. TPBank không nêu tên nhà cung cấp dịch vụ nhưng

sau đó đã ngừng làm việc với nhà cung cấp này, chuyển sang sử dụng một hệ thống mới có mức bảo mật cao hơn và cho phép kết nối trực tiếp với SWIFT.

Tấn công giả mạo

Tấn công giả mạo là hình thức tấn công phổ biến nhằm lấy được các thông tin nhạy cảm từ người dùng như: Tài khoản email, tài khoản mạng xã hội, thông tin tài khoản thẻ tín dụng ngân hàng. Một số vụ việc nổi cộm bao gồm:

+ Tấn công qua tạo email giả email ngân hàng: Ví dụ như trường hợp chị H (sống tại Q.9, TP.HCM) sở hữu thẻ visa của VPBank bất ngờ nhận được email từ địa chỉ ebank@ebank.vpbank.com.vn, yêu cầu nhập lại thông tin cá nhân kể cả số thẻ, ngày hết hạn, mã xác minh thẻ (còn gọi là mã CVV, là 3 chữ số in ở mặt dưới thẻ). Phía gửi thư nhân danh "gần đây, ngân hàng nhận được một báo cáo an ninh công cộng địa phương và thấy rằng nhiều thẻ tín dụng đã bị người lạ đánh cắp" nên khách hàng cần mở website http://ebank.vpbank.com.vn/security.html và điền chi tiết về thẻ để bảo mật tốt hơn. Nhận thấy tên website trên không giống như website của VPBank mà mình thường truy cập (https://www.vpbank.com.vn), chị H. gọi đến tổng đài ngân hàng này thì được biết đã bị kẻ xấu dùng email giả để đánh cắp thông tin thẻ tín dụng.

+ Đầu năm 2018, rộ lên thủ đoạn hacker yêu cầu nạn nhân đăng ký dịch vụ Internet Banking bằng số điện thoại do chúng cung cấp.

+ Giao dịch lừa đảo qua email: Vào đầu tháng 7/2018, Agribank cũng cảnh báo về việc xuất hiện giao dịch lừa đảo qua email. Cụ thể, đã có một số khách hàng thông báo họ chuyển tiền nhưng không đến đúng người nhận do đã bị "hack" email. Kẻ lừa đảo đã xâm nhập vào hệ thống email của khách hàng và đối tác để thay đổi thông tin về người hưởng trên hợp đồng hoặc bổ sung phụ lục hợp đồng, các chứng từ liên quan.

Phần mềm độc hại

Cuối tháng 12/2017, nhiều người dùng sử dụng ứng dụng Facebook Messenger tại Việt Nam đã trở thành nạn nhân của một loại mã độc được cho là sử dụng để đào tiền ảo. Số liệu thống kê từ hệ thống giám sát virus của Bkav cho thấy, kể từ thời điểm bắt đầu bùng phát vào sáng 19/12/2017, số lượng máy tính tại Việt Nam bị nhiễm mã độc đào tiền ảo phát tán qua Facebook Messenger đã liên tục tăng nhanh, từ con số 12.600 máy tính bị lây nhiễm tại thời điểm 14h ngày 21/12/2017 lên hơn 23.000 máy tính bị nhiễm vào chiều ngày 26/12/2017 và số máy tính bị hệ thống của Bkav ghi nhận nhiễm mã độc đào tiền ảo tính đến thời điểm ngày 2/1/2018 là 36.000 máy tính. Theo phân tích của Cục An toàn thông tin - Bộ Thông tin và Truyền thông, mã độc này lây lan bằng cách gửi đi một tập tin tên là video_xxx.zip. Đây là một tập tin nén trong đó có chứa tập tin với định dạng mp4.exe, thực chất là tập tin của hệ điều hành Windows. Tuy nhiên, người dùng thông thường lại nhầm tưởng là tập tin Video (mp4) nên dễ dàng tin tưởng mở tập tin. Mã độc này khi lây nhiễm vào máy tính đã thực hiện các bước: Tự động tải và cài đặt một số tập tin độc hại 7za.exe, files.g7z từ website độc hại có tên miền yumuy.johetbid (với các mẫu mã độc khác nhau, tên miền này có thể thay đổi). Mã độc sử dụng tập tin 7za.exe để giải nén tập tin tiles.7z, sau đó lấy tiện ích mở rộng (extension) độc hại và tự động cài đặt tiện ích mở rộng này vào trình duyệt Chrome. Đồng thời, mã độc này không cho người dùng truy cập vào phần quản lý tiện ích mở rộng của trình duyệt. Trong tập tin được giải nén có chứa các tập tin thực thi nhằm lợi dụng tài nguyên máy tính người dùng để đào tiền ảo. Cục An toàn thông tin cho biết, thông qua các biện pháp kỹ thuật, xác định được tác giả của mẫu mã độc này có thể đang sử dụng địa chỉ email có tên miền là kadirgun.com.

Năm 2020, lợi dụng điểm yếu công nghệ trong phương thức gửi OTP qua tin nhắn truyền thống trên điện thoại di động (SMS OTP), kẻ xấu đã lợi dụng để tấn công lừa đảo. Bkav phát hiện phần mềm gián điệp VN84App có máy chủ ở Trung Quốc đã thu thập hơn 300 mã OTP từ điện thoại là những giao dịch ngân hàng có số tiền lớn, lên tới hàng tỷ đồng (Mai Phương, Anh Vũ, 2020).

Thực trạng tội phạm sử dụng công nghệ cao nêu trên cho thấy ngành Ngân hàng đang đối mặt với nguy cơ rủi ro từ tất cả chủ thể chính: Ngân hàng, khách hàng, đối tác liên kết của ngân hàng. Do vậy, các biện pháp phòng, chống rủi ro không phải chỉ áp dụng cho ngân hàng mà còn cho cả các bên liên quan.

3.2. Thực trạng đảm bảo an toàn, bảo mật thông tin trong ngành Ngân hàng

Sẵn sàng phát triển và ứng dụng CNTT

Để đánh giá về thực trạng đảm bảo an toàn bảo mật thông tin, bài viết sử dụng chỉ số ICT Index. Dù xu hướng chung cho thấy các ngân hàng đang thực hiện chuyển đổi số và đầu tư nhiều cho CNTT, số liệu Bảng 2 cho thấy, năm 2019 chỉ có 11/29 NHTM Việt Nam có chỉ số sẵn sàng phát triển và ứng dụng CNTT trên mức trung bình. Các ngân hàng khác có điểm dao động 0,26 đến

Bảng 2: Xếp hạng mức sẵn lòng phát triển và ứng dụng CNTT của ngân hàng

STT	Tên ngân hàng	ICT Index					Xếp hạng				
		2015	2016	2017	2018	2019	2015	2016	2017	2018	2019
1	Đầu tư và Phát triển Việt Nam	0,81	0,56	0,78	0,76	0,76	1	1	1	1	1
2	Nam Á	0,57	0,52	0,71	0,68	0,74	11	5	2	2	2
3	Kỹ thương Việt Nam	0,54	0,49	0,49	0,63	0,70	15	10	8	3	3
4	Tiên Phong		0,46	0,39	0,42	0,45	-	16	21	6	19
5	Quân đội	0,57	0,52	0,54	0,50	0,63	10	4	4	7	5
6	Bảo Việt	0,51	0,55	0,57	0,49	0,44	17	2	3	8	20
7	An Bình	0,60	0,40	0,52	0,49	0,43	6	22	6	9	23
8	Sài Gòn - Hà Nội	0,72	0,49	0,53	0,49	0,44	3	11	5	10	22
9	Xuất nhập khẩu Việt Nam	0,57	0,47	0,49	0,48	0,55	13	14	9	11	8
10	Bản Việt	0,58	0,51	0,47	0,46	0,38	8	7	10	12	26
11	Đại Dương		0,43	0,35	0,46	0,51	-	17	23	13	10
12	Đại chúng Việt Nam		0,47	0,37	0,45	0,47	-	15	19	14	16
13	Quốc tế Việt Nam		0,37	0,47	0,45	0,60	-	25	13	15	6
14	Hàng hải Việt Nam	0,59	0,48	0,47	0,44	0,49	7	12	11	16	13
15	Sài Gòn - Thương Tín			0,28	0,32	0,44	-	-	18	17	21
16	Bắc Á				0,42	0,48			-	18	14
17	Đông Nam Á	0,75	0,43	0,42	0,41	0,46	2	19	15	19	18
18	Ngoại thương Việt Nam	0,63	0,37	0,47	0,39	0,57	4	24	12	20	7
19	Việt Nam Thịnh Vượng	0,44	0,55	0,34	0,38	0,50	21	3	24	21	12
20	Sài Gòn	0,57	0,33	0,41	0,37	0,48	12	28	17	22	15
21	Xăng dầu			0,31	0,36	0,51	-	-	28	25	11
22	Công thương Việt Nam	0,62	0,40	0,31	0,33	0,39	5	23	27	26	25
23	Phát triển TP. Hồ Chí Minh		0,51	0,34	0,33	0,46	-	6	25	27	17
24	Quốc Dân	0,55	0,37	0,30	0,36	0,53	14	26	30	28	9
25	Nông nghiệp và Phát triển nông thôn Việt Nam			0,27	0,30	0,39	-	-	31	29	24
26	Á Châu			0,15	0,27	0,33	-	-	32	30	28
27	Bưu điện Liên Việt		0,50	0,37	0,25	0,27	-	8	20	31	29
28	Dầu khí toàn cầu			0,50		0,69	-	13	-	-	4
29	Phương Đông					0,36			-	-	27

Nguồn: Bộ Thông tin và Truyền thông; Hội Tin học Việt Nam (2015, 2017, 2018, 2020).

0,49. Nếu tính riêng hạ tầng kỹ thuật và hạ tầng nhân lực thì có lần lượt 10 và 12 ngân hàng đạt mức trung bình. Bên cạnh đó, có sự phân hóa trong mức độ ứng dụng CNTT giữa các ngân hàng. Ngoại trừ BIDV (liên tục đứng đầu từ năm 2016) và Nam A Bank (liên tục đứng thứ hai từ năm 2017), các vị trí khác liên tục đổi chỗ giữa các ngân hàng.

An toàn thông tin tại Việt Nam đang tiềm ẩn nhiều nguy cơ, một số ngân hàng vẫn chưa tuân thủ triệt để các quy định, tiêu chuẩn về an toàn thông tin trên cơ sở các quy định, tiêu chuẩn an toàn thông tin của quốc tế và Việt Nam (Bộ Tiêu chuẩn ISO/IEC 27000 và các tiêu chuẩn liên quan). Bảng 3 cho thấy 46,7% ngân hàng đã được cấp chứng chỉ an toàn thông tin và bảo mật trong thanh toán. Số liệu này được cải thiện đáng kể trong các năm (trừ năm 2018), tuy nhiên chỉ có một số ngân hàng khẳng định về tính an toàn bảo

Bảng 3: Tỷ lệ triển khai các giải pháp an ninh, an toàn thông tin, an toàn dữ liệu của các NHTM

Đơn vị tính: %

STT	Chỉ tiêu	2015	2016	2017	2018	2019
1	Tỷ lệ triển khai giải pháp IPS/IDS					
	- Trung tâm dữ liệu chính	-	96,6	90,6	90,6	90,0
	- Các chi nhánh, đơn vị trực thuộc	-	24,1	21,9	21,9	26,7
2	Tỷ lệ triển khai kiểm soát truy cập Internet					
	- Trung tâm dữ liệu chính	-	100,0	100,0	100,0	100,0
	- Các chi nhánh, đơn vị trực thuộc	-	44,8	50,0	56,3	56,7
3	Tỷ lệ triển khai bảo mật thư điện tử					
	- Trung tâm dữ liệu chính	-	82,8	84,4	84,4	90,0
	- Các chi nhánh, đơn vị trực thuộc	-	41,4	50,0	56,3	33,3
4	Tỷ lệ cài đặt hệ thống phân tích, cảnh báo an toàn thông tin (SOC)					
	- Trung tâm dữ liệu chính	-	37,9	21,9	34,4	50,0
	- Các chi nhánh, đơn vị trực thuộc	-	3,4	3,1	9,4	6,7
5	Tỷ lệ cài đặt giải pháp phòng, chống tấn công (APT)					
	- Trung tâm dữ liệu chính	-	34,5	37,5	46,9	50,0
	- Các chi nhánh, đơn vị trực thuộc	-	3,4	18,8	12,5	23,3
6	Tỷ lệ cài đặt sử dụng trên tủ đĩa SAN	-	91.1	93	97.1	94
7	Tỷ lệ cài đặt sử dụng tại trung tâm dự phòng thảm họa	-	84	84.5	79.6	81
8	Tỷ lệ sao lưu ra đĩa cứng	-	87,9	85,3	94,3	89,8
9	Tỷ lệ sao lưu ra băng từ	-	78,2	77,9	76,9	66,4
10	Tỷ lệ ngân hàng đạt chứng chỉ về an toàn thông tin	21,70	27,60	43,80	-	-

** -: Không có thông tin*

Nguồn: Bộ Thông Tin và Truyền thông; Hội Tin học Việt Nam (2017, 2018, 2020)

mật trên website.

Triển khai các giải pháp an ninh, an toàn thông tin, an toàn dữ liệu

Tất cả các NHTM đã triển khai đầy đủ các biện pháp quản lý truy cập mạng, quản lý truy cập hệ thống ứng dụng, quản lý nhân viên truy cập trái phép vào hệ thống thực hiện các giao dịch trái phép hoặc lấy trộm thông tin mật, nhạy cảm như thông tin khách hàng. Tuy nhiên, tại các chi nhánh, hoạt động này chưa được quan tâm đúng mức như chưa có biện pháp quản lý truy cập mạng nội bộ, cho phép máy trạm kết nối trực tiếp Internet khi chưa áp dụng các biện pháp kiểm soát an toàn, chưa khóa tài khoản nhân viên nghỉ việc dài ngày. Khoảng 50% NHTM chưa định kỳ thường xuyên đánh giá các điểm yếu, lỗ hổng an ninh bảo mật của hệ thống CNTT. Một số đơn vị chưa thực hiện đưa các yêu cầu bảo mật trong quá trình phát triển hệ thống. Việc sao lưu dữ liệu đã cơ bản được các đơn vị thực hiện. Tuy nhiên việc kiểm tra, đánh giá phục hồi dữ liệu định kỳ vẫn còn những đơn vị chưa thực hiện đầy đủ. Các ngân hàng đang còn thiếu một hệ thống tổng hợp, ghi nhận lỗi để hệ thống hóa các lỗi phát sinh cũng như đề ra các giải pháp giải quyết vấn đề một cách khoa học, nhanh chóng. Tỷ lệ cài đặt hệ thống phân tích, cảnh báo an toàn thông tin tại hội sở chính dù đã cải thiện nhiều nhưng chỉ mới đạt 50%, các chi nhánh có tỷ lệ rất thấp, đạt 6,7%. Công tác phổ biến quy định nội bộ, nâng cao nhận thức về an toàn bảo mật cho nhân viên và công tác kiểm tra nội bộ việc tuân thủ quy định của nhân viên về an toàn bảo mật thông tin tại một số đơn vị chưa được chú trọng.

Thực trạng hạ tầng kỹ thuật

Các NHTM đã quan tâm đầu tư, đổi mới công nghệ, từng bước hoàn chỉnh hạ tầng CNTT nói chung và hạ tầng an ninh, bảo mật nói riêng. Cụ thể: Tại trung tâm dữ liệu (TTDL) chính, TTDL dự phòng và các hệ thống quan trọng, 100% các NHTM đã đầu tư, trang bị các giải pháp an ninh bảo mật cơ bản như: Tường lửa; hệ thống phát hiện xâm nhập (IPS/IDS); hệ thống phòng, chống virus; xác thực đa thành tố đối với các giao dịch điện tử và mã hóa dữ liệu đối với các hệ thống quan trọng (Bảng 4). Phần lớn các NHTM cũng đã trang bị các giải pháp tăng cường an toàn, an ninh mạng như: Hệ thống quản lý sự kiện an ninh; hệ thống phòng, chống thư rác; hệ thống lọc nội dung web; hệ thống quản lý file nhật ký; hệ thống đánh giá điểm yếu ứng dụng và mạng; công nghệ chữ ký số PKI.

Tuy nhiên, vẫn còn nhiều vấn đề liên quan đến hạ tầng kỹ thuật mà các NHTM chưa tuân thủ:

- Trung tâm dự phòng: Trong khi việc xây dựng quy trình, kịch bản đảm bảo hoạt động liên tục và tổ chức diễn tập chuyển đổi hoạt động từ hệ thống chính sang hệ thống dự phòng là rất cần thiết để đảm bảo hoạt động liên tục hệ thống CNTT thì 6,7% NHTM chưa xây dựng TTDL dự phòng thảm họa hoặc TTDL dự phòng mới chỉ là nơi sao lưu dữ liệu, không đảm bảo khả năng thay thế hoạt động cho TTDL chính. Nhiều NHTM chưa có trang thiết bị dự phòng cho các thiết bị quan trọng tại TTDL chính, tạo ra các điểm lỗi đơn (Single Point of Failure). Bên cạnh đó, do hệ thống CNTT của các ngân hàng tương đối lớn, có những hệ thống hoạt động 24/7 (như hệ thống thẻ, hệ thống Internet Banking và các hệ thống liên quan như Corebank) dẫn đến việc thực hiện chuyển đổi hệ thống phức tạp, tốn nhiều thời gian và nhân lực chuẩn bị. Do đó, vẫn có các đơn vị không tổ chức được diễn tập chuyển đổi hoặc chuyển đổi hệ thống không đáp ứng thời gian quy định.

- Đảm bảo an toàn vật lý cho phòng máy chủ: Công tác phòng cháy, chữa cháy tại một số đơn vị chưa đảm bảo, cụ thể như chưa có hệ thống báo cháy; hệ thống chữa cháy không phù hợp với hệ thống CNTT khi sử dụng nước hoặc bình bột; phòng máy chủ dùng chung với phòng làm việc, lưu trữ nhiều vật liệu dễ cháy.

- Sử dụng phần mềm không cập nhật bản vá: Hiện tại vẫn có NHTM sử dụng máy trạm chạy hệ điều hành Windows XP đã hết hạn hỗ trợ của hãng. Đặc biệt, hệ thống ATM sử dụng hệ điều hành này tại Việt Nam chiếm tỷ lệ tương đối lớn. Việc này là một nguy cơ rất lớn cho an toàn hệ thống vì các hệ điều hành cũ sẽ có nhiều lỗ hổng và hệ điều hành không có bản quyền sẽ không cập nhật bản vá lỗi được cung cấp từ nhà sản xuất.

- Việc đầu tư cho hạ tầng công nghệ của một số ngân hàng còn khá hạn chế do chi phí cho phát triển và thực thi cao. Điều này tác động không nhỏ đến an ninh CNTT trong bối cảnh công nghệ phát triển, kéo theo tội phạm

Bảng 4: Hạ tầng kỹ thuật của các NHTM 2016 - 2019

Đơn vị tính: %

STT	Chỉ tiêu	2015	2016	2017	2018	2019
1	Tỷ lệ máy trạm trong vòng 3 năm gần đây/Tổng số máy trạm	-	0,39	0,37	0,46	0,39
2	Tỷ lệ máy trạm chạy hệ điều hành bản quyền và có hỗ trợ của nhà sản xuất/tổng số máy trạm	-	71,0	74,3	87,3	90,9
3	Tỷ lệ băng thông Internet cung cấp dịch vụ Internet Banking/ Tổng số khách hàng Internet Banking	-	10,96	2,92	0,42	0,66
4	Tỷ lệ băng thông Internet cung cấp cho người dùng nội bộ/Tổng số máy tính được kết nối Internet	-	223,27	314,07	111,46	105,94
5	Tỷ lệ ngân hàng có trung tâm dự phòng	78,3	93,1	93,8	93,8	93,3
6	Tỷ lệ ngân hàng đạt chứng chỉ về an toàn thông tin	-	27,6	43,8	59,4	46,7
7	Tỷ lệ lắp đặt thiết bị tường lửa tại TTDL chính	-	100,00	100,00	100,00	100,00
8	Tỷ lệ lắp đặt tường lửa tại các chi nhánh, đơn vị trực thuộc	-	37,90	34,40	31,3	36,7

Ghi chú: -: Không có thông tin

Nguồn: Bộ Thông Tin và Truyền thông; Hội Tin học Việt Nam (2017, 2018, 2020)

công nghệ cao ngày càng tinh vi, dễ dẫn đến nguy cơ mất quyền kiểm soát hệ thống của các ngân hàng. Trên thế giới, trung bình đầu tư cho an toàn, bảo mật thông tin trong các dự án CNTT của các tổ chức chiếm 15 - 25%, tại Việt Nam chỉ gần 5% (Trường Xuân, 2018). Tỷ lệ đầu tư cho hạ tầng kỹ thuật/số cán bộ, nhân viên trong đơn vị trong một năm có xu hướng tăng đến năm 2018, nhưng lại giảm trong năm 2019, nếu xu hướng này kéo dài sẽ không tốt cho hệ thống, đặc biệt trong bối cảnh đại dịch Covid-19, các giao dịch không tiếp xúc được triển khai mạnh hơn bao giờ hết. Việc đầu tư triển khai các giải pháp an ninh bảo mật nâng cao như hệ thống quản lý sự kiện an ninh (SIEM); hệ thống phòng, chống tấn công từ chối dịch vụ,... chưa được quan tâm thực hiện. (Bảng 5)

Hiện nay, hầu hết các NHTM tại Việt Nam đều có hệ thống Internet Banking/ Mobile Banking được đầu tư bảo mật tương tự nhau với những lớp bảo mật cơ bản mà bất kỳ khách hàng nào cũng có thể nhận biết như sử dụng tên giao dịch và mật khẩu để đăng nhập, thông báo biến động số dư, báo cáo kết quả giao dịch qua email, tin nhắn. Một số ngân hàng sử dụng OTP để thực hiện giao dịch với hai hình thức qua tin nhắn và mã thông báo (Token) hay thông qua phần mềm mã thông báo (Software Token OTP) được cài trên thiết bị di động. Bên cạnh đó, các ngân hàng cũng đã triển khai hoặc đang triển khai chữ ký điện tử cho giao dịch điện tử. Tuy nhiên, hình thức xác thực này chủ yếu chỉ áp dụng cho khách hàng doanh nghiệp, ít hoặc không áp dụng cho khách hàng cá nhân. Nhiều ngân hàng đã sử dụng công nghệ tiên tiến như công nghệ xác thực sinh trắc học qua vân tay, qua mống mắt, qua giọng nói... Một số nước như (Singapore, Anh,...) đã áp dụng thêm các hình thức xác thực nâng cao ví dụ như ký giao dịch Transaction Signing cho các giao dịch rủi ro cao như thêm người thụ hưởng, đổi thông tin cá nhân. Các ngân hàng Việt Nam cần tiếp cận tìm hiểu những công nghệ mới này để tăng cường an toàn bảo mật thêm cho khách hàng của mình.

Tương tự như thanh toán trực tuyến, giao dịch thẻ tín dụng cũng rất cần được quan tâm về vấn đề an ninh an toàn bảo mật. Nếu so sánh với kênh Internet Banking và Mobile Banking, thanh toán trực tuyến qua thẻ tín dụng rủi ro hơn, có nhiều giao dịch gian lận và thất thoát gấp nhiều lần. Hiện nay, mọi thông tin cần thiết để thanh toán bằng thẻ đều được in trên bề mặt thẻ (số thẻ, tên chủ thẻ, ngày hết hạn, CVV/CVC), do vậy, nếu khách hàng để lộ thông tin thẻ hoặc rơi thẻ, thất thoát có thể xảy ra mà không có kiểm soát. Do đó, giao dịch qua thẻ tín dụng cần thiết phải được áp dụng giải pháp bảo mật 3D Secure mà các đối tác Visa, Mastercard, JCB đều cung cấp.

Thực trạng nhân lực và tổ chức

Các NHTM đều đang đứng trước khó khăn thiếu hụt về nhân lực CNTT có trình độ cao. Tất cả các chỉ số về hạ tầng nhân lực CNTT của các NHTM đều có xu hướng giảm. Theo số liệu thu thập từ Báo cáo ICT Index các năm gần đây cho thấy, các NHTM có tỷ lệ cán bộ chuyên trách CNTT tương đối cao so với mặt bằng chung của các đơn vị trong báo cáo, đặc biệt là các tổng công ty. Trừ tỷ lệ cán bộ chuyên trách CNTT có chứng chỉ CNTT/tổng số cán bộ chuyên trách CNTT tăng, các chỉ tiêu khác về chất lượng nguồn nhân lực và mức đầu tư cho nguồn nhân lực đều giảm trong 5 năm gần đây.

Một số đơn vị hiện chưa có bộ phận hoặc cán bộ chuyên trách về an ninh, an toàn thông tin; các dịch vụ CNTT phức tạp phần lớn phải thuê ngoài. Do đó, trong thời gian tới, các NHTM cần tiếp tục đầu tư cho nguồn nhân lực để tăng cường chất lượng và số lượng đội ngũ cán bộ CNTT. Hầu hết các NHTM hiện nay còn thiếu quy định về ưu tiên,

Bảng 5: Đầu tư cho hạ tầng kỹ thuật

Chỉ tiêu	2015	2016	2017	2018	2019
Đầu tư cho hạ tầng kỹ thuật/tổng số cán bộ nhân viên trong 01 năm (triệu đồng)	11,00	17,60	20,40	27,10	20,40
Tỷ lệ đầu tư cho hạ tầng an ninh, an toàn thông tin/tổng số cán bộ nhân viên (%)	3,20	3,90	3,70	4,1	3,0
Đầu tư cho đào tạo CNTT/cán bộ nhân viên trong 01 năm (triệu đồng)	-	0, 70	0,64	0,67	0,61

Nguồn: Bộ Thông tin và Truyền thông; Hội Tin học Việt Nam (2011, 2017, 2018, 2020)

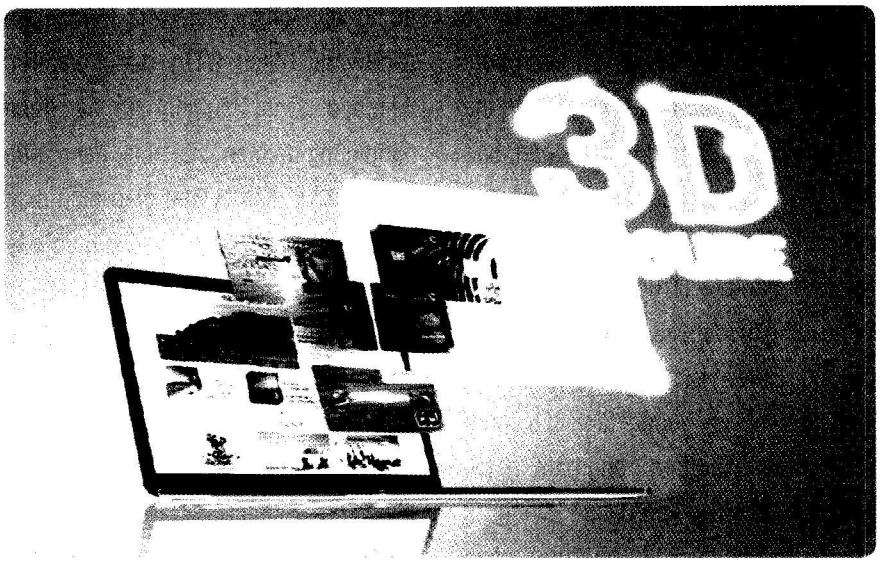
đãi ngộ đối với nhân lực trình độ cao về CNTT nên có nhiều người trong số đó chưa an tâm cống hiến, không có ý định gắn bó lâu dài. (Bảng 6)

4. Một số khuyến nghị cho các NHTM

Đầu tư cho CNTT tốn nhiều chi phí. Điều này đã được khẳng định trong nhiều nghiên cứu trước đây (Solow,1987; Jorgenson & Stiroh, 1995; Beccalli, 2007). Trong bối cảnh công nghệ đang tiến nhanh như vũ bão, kèm theo đó là các mối đe dọa không ngừng tăng lên của tội phạm sử dụng công nghệ cao, thì ngân hàng nào muốn đi nhanh, đi xa nhưng để bền vững thì không có lựa chọn nào khác ngoài việc bảo đảm an toàn, bảo mật cho ngân hàng mình và cho cả khách hàng. Vì thế, các NHTM cần lưu ý một số vấn đề sau đây:

Thứ nhất, tăng cường đầu tư cho công nghệ

Ngoài việc thường xuyên khuyến cáo, hướng dẫn khách hàng sử dụng dịch vụ an toàn và phòng, chống lừa đảo, các NHTM cần tăng cường đầu tư cho các giải pháp bảo mật, đặc biệt là các ứng dụng tự bảo vệ để chủ động ngăn chặn hoặc tắt ứng dụng nếu có



các mối đe dọa từ các phần mềm gián điệp. Nghiên cứu, áp dụng các giải pháp CNTT để chủ động nhận diện, cảnh báo kịp thời các hiểm họa, nguy cơ mất an ninh cho khách hàng như: Công nghệ chống tấn công và công nghệ phát hiện giao dịch gian lận. Triển khai áp dụng sớm và đồng bộ các biện pháp đảm bảo an toàn hoạt động ngân hàng điện tử với các công nghệ bảo mật tiên tiến như xác thực sinh trắc học, công nghệ 3D Secure, khóa công khai PKI; công nghệ chống tấn công, công nghệ phát hiện giao dịch gian lận, hệ thống bảo mật ba lớp... Với dịch vụ 3D-Secure này chủ thẻ sẽ phải nhập mã OTP do ngân hàng cung cấp trước khi hoàn tất giao dịch mua hàng hóa, dịch vụ trực tuyến. Dịch vụ này được đăng ký mặc định và sử dụng miễn phí cho các chủ thẻ quốc tế của ngân hàng.

Thứ hai, quan tâm đến nhân lực CNTT

Các NHTM còn thiếu hụt về nhân lực CNTT trình độ cao. Một số NHTM chưa có chính sách ưu tiên, đãi ngộ, tôn vinh nhân lực trình độ cao. Để có thể đảm bảo an toàn hệ thống thông tin, các NHTM cần hết sức chú trọng về con người. Có nhiều vấn đề cần quan tâm tuy nhiên, các vấn đề sau đây cần chú trọng đặc biệt: (1) Tăng cường công tác tuyên truyền, nâng cao nhận thức, khả năng tự bảo vệ cho cán bộ, nhân

Bảng 6: Số liệu về hạ tầng nhân lực của các NHTM

Năm	2015	2016	2017	2018	2019
Tỷ lệ cán bộ chuyên trách CNTT (%)	3,0	2,6	2,6	2,4	2,4
Tỷ lệ cán bộ chuyên trách an toàn thông tin (%)	0,5	0,1	0,1	0,1	0,1
Tỷ lệ cán bộ chuyên trách CNTT có chứng chỉ CNTT/ tổng số cán bộ chuyên trách CNTT (%)	-	16,9	9,0	8,8	10,3
Chi cho đào tạo cán bộ CNTT/tổng số cán bộ nhân viên trong 01 năm (ngàn đồng)	872	702	635	670	608

Nguồn: Bộ Thông tin và Truyền thông; Hội Tin học Việt Nam (2017, 2018, 2020).

viên ngân hàng hiểu rõ về vị trí, vai trò, trách nhiệm của bản thân trong việc phòng, chống tội phạm sử dụng công nghệ cao trong lĩnh vực ngân hàng vì đây là yếu tố then chốt và đóng vai trò quyết định trong việc đảm bảo an toàn thông tin; (2) Giáo dục, nâng cao đạo đức nghề nghiệp của nhân viên ngân hàng và nhân viên của các đơn vị có liên quan để không bị lợi dụng, mua chuộc. Thực hiện Bộ chuẩn mực đạo đức nghề nghiệp và quy tắc ứng xử của cán bộ ngân hàng theo Quyết định số 11/QĐ-HHNH ngày 25/12/2019, đặc biệt là Điều 6 về ý thức bảo mật thông tin; (3) Cần kịp thời khen thưởng các điển hình có sáng kiến trong đảm bảo an toàn bảo mật và có biện pháp chế tài đối với các trường hợp vi phạm.

Thứ ba, đầu tư cho công nghệ và nhân lực phải được thực hiện thường xuyên

Trong một môi trường thường xuyên thay đổi, ngày càng rủi ro, việc đầu tư và nâng cấp hệ thống ngân hàng lõi, công nghệ bảo mật, hệ thống quản lý rủi ro... không chỉ là yêu cầu bắt buộc mà còn là yêu cầu thường xuyên, liên tục nếu như không muốn bị tụt hậu. Vị thế của các NHTM từ năm 2015 cho đến nay là minh chứng rõ cho vấn đề này.

Thứ tư, tuân thủ các quy định về an toàn hệ thống thông tin

Trong lĩnh vực ngân hàng, Thông tư số 09/2020/TT-NHNN của Ngân hàng Nhà nước Việt Nam quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng, ban hành ngày 21/10/2020 và có hiệu lực ngày 01/01/2021 là văn bản bao quát nhất trong Ngành. Thống kê cho thấy, chỉ khi các cơ quan quản lý có hành lang pháp lý chặt chẽ, có biện pháp chế tài mạnh thì mới buộc tất cả các ngân hàng tăng chi phí đầu tư cho bảo mật, an toàn hệ thống, chấp nhận giảm lợi nhuận để có một không gian mạng an toàn cho tất cả các bên liên quan trong hoạt động ngân hàng.■

TÀI LIỆU THAM KHẢO:

1. Bitsight (2019). 6 Cybersecurity KPI Examples for Your Next Report. https://www.bitsight.com/blog/6-cybersecurity-kpis-examples-for-your-next-report

2. Bộ Thông tin và Truyền thông; Hội Tin học Việt Nam (2011, 2015, 2017, 2018, 2020). Báo cáo chỉ số sẵn sàng cho phát triển và ứng dụng CNTT-TT Việt Nam năm 2011, 2015, 2017, 2018, 2019.

3. Cipher (2018). 10 Cybersecurity Metrics You Should Be Monitoring. http://blog.cipher.com/10-cybersecurity-metrics-you-should-be-monitoring

4. Dangolani, S. K. (2011). The Impact of information technology in banking system (A case study in Bank Keshavarzi IRAN). Procedia-Social and Behavioral Sciences, 30, 13-16.

5. Hà An (2020), Lỗ hổng trong an ninh thông tin ngân hàng số. https://nhandan.com.vn/chuyen-de-cuoi-tuan/lo-hong-trong-an-ninh-thong-tin-ngan-hang-so-616515/

6. Imperva (2019). Social Engineerings. https://www.imperva.com/learn/application-security/social-engineering-attack/.

7. Indusface Blog (2018), 8 cybersecurity kpis track.

https://www.indusface.com/blog/8-cybersecurity-kpis-track/

8. Jorgenson, D. W., Stiroh, K. J., Gordon, R. J., & Sichel, D. E. (2000). Raising the speed limit: US economic growth in the information age. Brookings papers on economic activity, 2000(1), 125-235.

9. Karim, S. S. (2016). Cyber-crime Scenario in Banking Sector of Bangladesh: An Overview. http://www.icmab.org.bd/images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf.

10. KPMG (2016), cyber security dashboard: monitor, analyse and take control of cyber security. http://filestest.smart.pr.s3-eu-west-1.amazonaws.com/60/50f560e98811e4ba43b37df128779b/Cyber-Security-Dashboard_-Monitor_-analyse-and-take-control-of-Cyber-Security.pdf

11. Kritzinger & Von Solms (2012). Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa - Has the CIIP and Cyber Security Rubicon Been Crossed?.Retrrieved from 12. https://pdfs.semanticscholar.org/756d/636848cbac9832cbd4fc79eac22ed89d8956.pdf

12. Linkedin (2019)

13. Mai Phương, Anh Vũ (2020), Rủi ro phần mềm gián điệp. https://thanhnien.vn/tai-chinh-kinh-doanh/rui-ro-phan-mem-gian-diep-1243134.html

14. NetcomLearning (2019). 5 Cybersecurity KPIs You Should Know. https://www.netcomlearning.com/blogs/111/127/5-Cybersecurity-KPIs-You-Should-Know

15. Nguyễn Mạnh Hà & Vũ Duy Thăng (2018). Các hình thức tấn công Social Engineering phổ biến. http://m.antoanthongtin.gov.vn/hacker-malware/cac-hinh-thuc-tan-cong-social-engineering-pho-bien-104856

16. PwC (2018). Global Economic Crime and Fraud Survey – Pulling Fraud out of the Shadows. https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

17. Roger, E. S. (2008). Rogers Communications Inc, 2008 Annual Report.

18. Solow, R. M. (1987). We'd better watch out. New York Times Book Review, 36.

19. SWIFT (2018). 2018 Mid-Year Report: Cybersecurity Stats. https://swiftsystems.com/2018-mid-year-report-cybersecurity-stats/

20. Trung Hiền (2018). Một ngân hàng Việt bị tấn công, hacker "dọa" bán 275.000 dữ liệu, http://soha.vn/mot-ngan-hang-viet-bi-tan-cong-hacker-doa-ban-275000-du-lieu-20181014153013053.htm

21. Trường Xuân (2018). Ngân hàng số và các mối quan ngại bảo mật. https://tinnhanhchungkhoan.vn/fin-tech/ngan-hang-so-va-cac-moi-quan-ngai-bao-mat-245208.html