Bản tin điện tử nội bộ - Số 83 | Tháng 11 - 2018

THẾ GIỚI THẺ

Tổng biên tập: *Bà Phan Thị Quỳnh Hoa - Giám đốc Tập đoàn MK* | **Ý kiến đóng góp vui lòng gửi về:** *marketing@mkgroup.com.vn*

Lưu ý: *Toàn bộ thông tin/hình ảnh trong Bản tin điện tử nội bộ Thế Giới Thẻ MK Group được sưu tầm từ các nguồn tin khác nhau và chỉ sử dụng cho mục đích chia sẻ kiến thức.*

Các tin bài chính

HỘI THẢO "PHÁT HÀNH THẺ NGAY LẬP TỨC – SỨC SỐNG MỚI CHO CÁC CHƯƠNG TRÌNH THẺ TÀI CHÍNH"

HỘI THẢO "PHÁT HÀNH THẺ NGAY LẬP TỨC - SỨC SỐNG MỚI CHO CÁC CHƯƠNG TRÌNH THẺ TÀI CHÍNH"

Vào ngày 23/1/2018, Hội thảo "Phát hành thẻ ngay lập tức - Sức sống mới cho các chương trình thẻ tài chính" đã được MK Group cùng Entrust Datacard phối hợp tổ chức thành công tại Khách sạn Majestic, số 1 Đồng Khởi, thành phố Hồ Chí Minh.

Một trong những vấn đề nóng hiện nay được nhiều tổ chức tài chính ngân hàng quan tâm chính là việc sự xuất hiện của nhiều phương thức thanh toán mới như QR code, ví điện tử, các hình thức thanh toán online… đã tác động không nhỏ vào tính trung thành của người tiêu dùng với các thương hiệu thẻ thanh toán. Mặc dù nhu cầu sở hữu một chiếc thẻ ngân hàng vẫn còn, song khách hàng cũng luôn sẵn sàng thay đổi những hành vi và thói quen thanh toán truyền thống để trải nghiệm những phương thức mới theo xu hướng chung của thế giới.

Trước thách thức này, một câu hỏi quan trọng được đặt ra cho các tổ chức tài chính liệu phương thức phát hành thẻ truyền thống hiện nay của các ngân hàng có còn giúp các Ngân hàng đạt được mục tiêu “Gắn kết khách hàng – Thúc đẩy doanh thu” nữa không? Phải chăng đây là thời điểm các ngân hàng nên chuyển đổi sang hình thức phát hành thẻ ngay lập tức tại thời điểm khách hàng phát sinh nhu cầu sử dụng thẻ, vừa giúp rút ngắn thời gian chờ đợi, vừa có thể hỗ trợ bán chéo sản phẩm hoặc hiện thực hóa chương trình thẻ liên kết giữa ngân hàng và doanh nghiệp chỉ trong một vài phút. Ngoài ra, một trong những vấn đề được nhiều ngân hàng quan tâm và chia sẻ chính là việc thiếu kinh nghiệm triển khai thực tế và vai trò của nhà cung cấp trong các hoạt động tư vấn, tích hợp hệ thống, bảo trì và hỗ trợ kỹ thuật trong quá trình triển khai giải pháp.

Để giải đáp những e ngại của Khách hàng, các chuyên gia của Entrust Datacard là ông Ajay Kumar - *Giám đốc khu vực chuyên về Giải pháp phát hành thẻ ngay lập tức*, ông Jeremy NG - *Giám đốc Marketing khu vực của giải pháp*, ông Hồ Văn Hữu – Trưởng phòng kỹ thuật của MK Group và ông Đỗ Hải Đăng – Giám đốc chi nhánh MK Group tại Tp. Hồ Chí Minh với kinh nghiệm triển khai nhiều chương trình thẻ toàn cầu cùng đội ngũ kỹ thuật được đào tạo chính hãng đã giúp các Ngân hàng phân tích sâu những vấn đề trọng tâm trong việc triển khai giải pháp liên quan đến việc lựa chọn nhà cung cấp, những quy định cần tuân thủ về bảo mật, việc tối ưu hóa ngân sách triển khai và những dịch vụ bảo trì đi kèm (*), bên cạnh việc chứng minh những lợi ích thiết thực liên quan đến gia tăng tỉ lệ kích hoạt thẻ thanh toán, gắn kết khách hàng với mục tiêu “Mang lại sức sống mới cho các chương trình thẻ tài chính”.

Cũng trong khuôn khổ sự kiện, các Khách hàng cũng được trải nghiệm phần mềm phát hành thẻ ngay lập tức CardWizards và thiết bị phát hành thẻ để bàn Datacard® CE875 để hiểu rõ hơn sự linh hoạt, nhanh gọn và dễ quản lý của giải pháp phát hành thẻ ngay lập tức.

Có thể nói, xuất phát từ sự am hiểu thị trường với kinh nghiệm hơn 40 năm trong lĩnh vực phát hành thẻ, Entrust Datacard đã cùng MK Group mang lại một giải pháp phát hành thẻ ngay slập tức toàn diện, được xây dựng để phù hợp các tổ chức tài chính, các mô hình kinh doanh và phương thức phát hành thẻ khác nhau. Thông qua giải pháp phát hành thẻ ngay lập tức, việc giữ chân khách hàng hiện tại và thu hút khách hàng tiềm năng trở nên hiệu quả, từ đó các tổ chức tài chính ngân hàng sẽ giữ được sự trung thành của khách hàng và thúc đẩy phát triển bền vững.

Hà Nội chính thức dùng vé điện tử đi bus nhanh

Hà Nội vừa chính thức triển khai thí điểm vé điện tử trên tuyến buýt nhanh (BRT) 01 Kim Mã-Yên Nghĩa, tiến tới liên thông trên toàn hệ thống xe buýt có trợ giá.

Thẻ vé điện tử được xây dựng đáp ứng tiêu chuẩn khung tại Quyết định số 3978/QĐ-UBND của UBND TP.Hà Nội, đáp ứng khả năng liên thông với các loại hình vận tải hành khách công cộng khác trong tương lai. Thay vì sử dụng vé giấy, hành khách đi lại trên tuyến buýt nhanh BRT 01 Kim Mã-Bến xe Yên Nghĩa sẽ được sử dụng loại Thẻ vé điện tử thông minh làm bằng chất liệu nhựa tổng hợp (NFC) có gắn chíp điện tử.

Theo đại diện Sở Giao thông vận tải Hà Nội, thẻ vé điện tử là phương thức thanh toán hiện đại, tiện lợi cho việc giao dịch và nạp thẻ của hành khách, kiểm soát doanh thu. Đồng thời giúp cơ quan quản lý nhà nước và đơn vị vận hành thu thập thông tin về nhu cầu đi lại phục vụ công tác quy hoạch mạng lưới tuyến, điều chỉnh dịch vụ hợp lý nhằm khuyến khích, thu hút người dân sử dụng phương tiện vận tải hành khách công cộng.

Liên danh Viettel-Transerco-Công ty Nhật Cường đã đầu tư lắp đặt cổng kiểm soát ra vào, hệ thống camera giám sát, thiết bị bán vé và đường truyền Internet tại 23 nhà chờ dọc tuyến; xây dựng phần mềm phát hành thẻ, nạp tiền, quản trị dữ liệu khách hàng tại liên danh và Trung tâm Quản lý và điều hành giao thông đô thị, Sở Giao thông vận tải.

Dự kiến sau thời gian thí điểm sẽ tổng kết đánh giá, hoàn thiện giải pháp công nghệ và trình UBND TP. Hà Nội phê duyệt dự án triển khai nhân rộng trên toàn bộ các tuyến xe buýt có trợ giá./.

(ICTNews)

ĐIỂM TIN VIỆT NAM

- **Công ty CP Thanh toán Quốc gia Việt Nam (Napas)** từ nay đến ngày 16/12 sẽ phối hợp với Ngân hàng TMCP Đầu tư và Phát triển Việt Nam (BIDV) triển khai chương trình ưu đãi dành cho chủ thẻ ghi nợ nội địa thanh toán hàng hóa, dịch vụ trên POS tại tất cả các các đơn vị chấp nhận thẻ trên toàn quốc vào các ngày thứ Bảy, Chủ Nhật hàng tuần nhằm thúc đẩy phát triển thanh toán không dùng tiền mặt theo định hướng của Chính phủ và Ngân hàng Nhà Nước.

- **Ngân hàng TMCP Sài Gòn Thương Tín (Sacombank)** từ ngày 25/10 đến 31/7/2019 triển khai chương trình khuyến mãi "Mở thẻ - có quà" dành cho người đăng ký mở mới thẻ tín dụng quốc tế Sacombank JCB hạng chuẩn và vàng. Theo đó, chủ thẻ sẽ nhận một mũ bảo hiểm thời trang khi rút tiền hoặc thanh toán hàng hóa, dịch vụ lần đầu tiên qua thẻ trị giá từ 500.000 đồng đến một triệu đồng. Khi thanh toán, mua sắm lần đầu qua thẻ với hóa đơn trên một triệu đồng, khách sẽ được hoàn 200.000 đồng.

- **Ngân hàng TMCP Công Thương Việt Nam (VietinBank)** vừa ra mắt sản phẩm thẻ tín dụng dành riêng cho khách hàng doanh nghiệp vừa và nhỏ - SME Business Card. Theo đó, khi dùng SME Business Card, doanh nghiệp không phải tạm ứng cho nhân viên các khoản chi nhỏ, thường xuyên, có thể thanh toán 24/7 mọi lúc, mọi nơi.

(Tổng hợp từ Internet)

5 câu hỏi cần cân nhắc về Giải pháp phát hành thẻ ngay lập tức

Trước khi gặt hái những thành quả từ FII, sẽ sáng suốt hơn nếu xem xét một số câu hỏi quan trọng dưới đây. Từ cách thức chọn lựa nhà cung cấp đảm bảo đáp ứng yêu cầu bảo mật, thì ***việc trả lời 5 câu hỏi dưới đây có thể giúp các tổ chức định hướng con đường chuyển đổi tới FII.***

1. Nhà cung cấp nào tốt nhất?

Cần cân nhắc nhiều yếu tố khi chọn nhà cung cấp hơn là chỉ đơn thuần xem xét yếu tố giá. Mặc dù giá cả hợp lý và khả năng tạo doanh thu luôn phải tính đến, nhưng danh tiếng của nhà cung cấp cũng không kém phần quan trọng. Hãy tận dụng mạng lưới để chọn ra những nhà cung cấp tiềm năng.

Các khía cạnh bên trong – bao gồm các hình thức đào tạo hoặc chất lượng máy in và phôi thẻ - có thể là tiêu chí chính để lựa chọn nhà cung cấp phù hợp nhất cho chương trình FII. Các tổ chức cũng có thể xem xét liệu nhà cung cấp có khả năng tùy chỉnh sản phẩm để phù hợp với những nhu cầu cụ thể. Có càng nhiều lựa chọn cá thể hóa, các tổ chức càng có cơ hội tạo ra chương trình FII lấy khách hàng làm trọng tâm.

2. Tuân thủ quy định như thế nào?

Dù muốn hay không, chúng ta bắt buộc phải tuân thủ các yêu cầu bảo mật. Bảo vệ các thông tin định danh khách hàng bằng cách đảm bảo chương trình FII tuân thủ các quy định liên quan. Tiêu chuẩn an ninh thông tin về bảo mật thông tin thẻ thanh toán PCI-DSS là một trong những tiêu chuẩn giúp bảo mật thông tin nhạy cảm. Tuân thủ tiêu chuẩn này bằng cách lên kế hoạch cho việc xử lý và lưu trữ thông tin thẻ thanh toán.

Tuy nhiên một quy định giá trị khác cần lưu ý là quy định bảo vệ dữ liệu chung. GDPR là một trong những quy định mới nhất và phức tạp nhất trong ngành dịch vụ tài chính, với mục tiêu trao trả quyền nắm giữ dữ liệu cá nhân cho người sở hữu.

Hi vọng các tổ chức luôn cập nhật những quy định mới và tôn trọng mong muốn bảo vệ dữ liệu của chủ sỡ hữu. Nếu khách hàng muốn biết cách thức dữ liệu của họ đang được sử dụng như thế nào, các tổ chức có thể đưa ra những giải thích chi tiết nhằm gia tăng sự minh bạch và nâng cao khả năng tuân thủ các quy định.

3. SFP (Software For Purchase) hay SaaS (Sofware as a Service)?

Khi cân nhắc chương trình FII, các tổ chức nên biết ai là người nắm quyền sở hữu máy chủ, nơi lưu trữ dữ liệu cũng như các thẻ mới của chương trình này. Giải pháp mua phần mềm *(Software For Purchase - SFP)* trao quyền cho các tổ chức tài chính, trong khi lựa chọn phần mềm là dịch vụ *(Software as a Service - SaaS)* - chuyển trách nhiệm sang phần mềm dựa trên điện toán đám mây và máy chủ sang sang nhà cung cấp giải pháp phát hành ngay lập tức.

Đưa ra lựa chọn chính xác cho tổ chức bắt đầu bằng những yếu tố khác nhau – đặc biệt là chi phí và quản lý khóa EMV. Thường được lựa chọn bởi các ngân hàng lớn, SFP có chi phí tích hợp cao hơn. Mặt khác, Saas mang lại khả năng in thẻ thanh toán tại bất kì chi nhánh nào chỉ với một phần nhỏ chi phí trả trước

Trong trường hợp cân nhắc đến production key, cần quyết định thêm một số điểm. Được sử dụng để quyết định sô ghi trên mỗi thẻ thanh toán, những khóa này có thể được xử lý bởi các chuyên viên của tổ chức - SFP hoặc nhà cung cấp – SaaS.

Cân nhắc đến tình nhạy cảm của EMV production key, chọn nhà cung cấp giải pháp phát hành ngay lập tức với kinh nghiệm chuyên gia hoặc đảm bảo tổ chức có thể đối mặt với các thách thức khi lựa chọn giải pháp SFP.

4. Việc bảo trì sẽ được thực hiện như thế nào?

Vấn đề bảo trì chắc chắn sẽ phát sinh. Các tổ chức nên sẵn sàng đối mặt bằng cách chuẩn bị sẵn sàng cho các trường hợp có thể xảy ra và cách thức giải quyết. Trong khi một số vấn đề phần cứng có thể yêu cầu sự can thiệp của kĩ sư, những vấn đề khác có thể xử lý từ xa.

Trong trường hợp máy in không thể sửa được, hãy đảm bảo hợp đồng có đề cập tới thời hạn có thể thay thế máy. Máy càng được thay thế sớm, tổ chức sẽ càng giảm thiểu được thời gian dừng hoạt động.

Tổ chức có thể cân nhắc mua máy dự phòng tại những nơi có khối lượng thẻ phát hành lớn. Khi có vấn đề nghiêm trọng xảy ra như lỗi hệ thống – lên sơ bộ các thủ tục xử lý khẩn cấp và xem xét tổ chức hay nhà cung cấp sẽ chịu trách nhiệm sửa chữa.

Thêm vào đó, nên cân nhắc giải pháp có phần mềm giám sát, trong đó có thể xác định các vấn đề cần bảo trì ngay khi xảy ra. Nhiều ngân hàng hiện nay đang sử dụng dịch vụ này cho máy ATM nhưng vẫn chưa triển khai trên máy in thẻ. Một khi có phần mềm giám sát, các tổ chức có thể hy vọng giảm thời gian chết và nâng cao trải nghiệm của khách hàng.

5. Bảo mật như thế nào?

Việc bảo vệ thông tin nhận dạng cá nhân của khách hàng là rất quan trọng cho cả tổ chức và khách hàng. Có không thiếu các biện pháp an ninh được đề xuất và yêu cầu đối với thẻ thanh toán.

Mỗi tổ chức thẻ quốc tế (ví dụ: Visa, Mastercard, AMEX) đều có các khuyến nghị riêng liên quan đến việc triển khai giải pháp phát hành thẻ ngay lập tức. Một số biện pháp bảo mật liên quan đến máy in bao gồm: giám sát camera; khóa kép đối với máy in; thủ tục kiểm tra thẻ; và báo cáo.

Điều cần đặc biệt chú ý là bảo mật những dữ liệu không thể nhìn thấy được – dữ liệu trong quá trình được truyền giữa máy in và phần mềm – phải được đảm bảo ở mức độ bảo mật cao nhất.

Thêm vào đó, trong khi hầu hết các chương trình phát hành thẻ ngay lập tức đều cung cấp chương trình tuân thủ PCI, chỉ một số ít cung cấp chương trình được chứng nhận bởi PCI. Triển khai chương trình không được PCI chứng nhận đồng nghĩa với việc tổ chức tài chính phải trải qua quy trình kiểm tra bởi chính các tổ chức thẻ quốc tế, việc này yêu cầu nhiều thời gian và công sức để chuẩn bị

Các tổ chức có thể muốn bắt tay vào việc triển khai FII sớm nhất có thể. Sau tất cả, dường như các tổ chức đều đang chuyển mình theo FII. Nhưng hãy chắc chắn dành một chút thời gian để suy nghĩ về những gì đi kèm với quá trình này. Đưa ra các quyết định khó khăn – chẳng hạn như cách chọn nhà cung cấp hay những việc bảo trì cần thiết – trước đó sẽ giúp việc triển khai giải pháp trơn tru hơn.

Juniper Research: Tới năm 2023, sẽ có 1,5 tỷ người sử dụng công nghệ bảo mật sinh trắc

Công ty nghiên cứu thị trường Juniper Research trong báo cáo mới đây dự đoán rằng thay đổi lớn nhất trong ngành bảo mật thanh toán di động (m-payment) là xu hướng sử dụng các phương pháp xác minh bằng phần mềm dựa trên các thành phần tiêu chuẩn của smartphone.

Theo dự báo của Juniper Research, số người sử dụng các phương pháp nói trên sẽ tăng từ 429 triệu (ước tính vào năm nay) lên đến 1,5 tỷ vào năm 2023. Juniper cho biết tương lai này sẽ mở ra một kỷ nguyên xác thực m-payment sử dụng công nghệ sinh trắc dựa trên các mẫu sử dụng thiết bị của các cá nhân.

“Bảo mật m-payment sẽ mở rộng mạnh mẽ nhờ vào việc triển khai các giải pháp phần mềm thuần túy”, theo James Moar - tác giả của báo cáo nhận xét. “Trận chiến quan trọng hiện nay sẽ là thuyết phục người dùng, đặc biệt là ở Châu Âu và Bắc Mỹ, rằng những phương pháp này cũng an toàn và bảo mật như những phương pháp bảo mật trên dựa phần cứng truyền thống.”

Theo Juniper, với iPhone X và các smartphone khác sơ hữu tính năng nhận diện khuôn mặt và mống mắt, cảm biến vân tay sẽ giảm tương ứng theo tỷ lệ phần cứng về sinh trắc trên smartphone, từ hơn 95% năm 2018 xuống còn chưa đến 90% vào năm 2023. Với sự gia tăng của các phương thức xác thực sinh trắc dựa trên phần mềm, việc sử dụng cảm biến vân tay sẽ tùy thuộc vào hoàn cảnh chứ không phải là tùy chọn mặc định./.

(PYMNTS)

Bahrain triển khai hệ thống thanh toán sinh trắc tại nhiều ngân hàng


Nguồn ảnh: Internet

Ngân hàng Ithmaar và Công ty Dịch vụ Tài chính Eazy của Bahrain vừa công bố kế hoạch khởi động mạng lưới thanh toán sinh trắc đầu tiên ở khu vực Trung Đông, nhằm cung cấp giải pháp thay thế mới hiệu quả hơn cho khách hàng khi thực hiện nhiều giao dịch tài chính.

Khi được triển khai, các khách hàng của Ithmaar Bank sẽ không còn phải sử dụng thẻ ngân hàng tại ATM. Thay vào đó, họ sẽ chỉ cần sử dụng vân tay cùng với mã PIN để xử lý các giao dịch tài chính. Công nghệ mới sẽ tạo ra một cách thức đơn giản, an toàn hơn bao giờ hết để xử lý các giao dịch tài chính. Trong tương lai, công nghệ này cũng có thể được triển khai tại các điểm bán hàng./.

(Planet Biometrics)

Dự báo sẽ có 579 triệu thẻ sinh trắc học được lưu hành vào năm 2023

Goode Intelligence dự báo với khả năng xác thực nhanh chóng với các khoản thanh toán không tiếp xúc sẽ khiến cho công nghệ thẻ sinh trắc học được ứng dụng rộng rãi vào năm 2023, và sẽ có gần 579 triệu thẻ thanh toán sinh trắc học được sử dụng trên khắp thế giới trong vòng 5 năm tới.

Giám đốc điều hành Alan Goode cho biêt: "Sau một năm thí điêm thẻ thanh toán sinh trăc học vào năm 2018, chúng tôi sẽ tăng cường thí điểm vào năm tới và có thể sẽ triển khai một số tính chất thương mại trong năm 2019. Năm 2020 sẽ là năm phát hành hàng loạt thẻ thanh toán sinh trắc học trên toàn Thế Giới cho khách hàng."

Nhìn chung, Goode Intelligence dự đoán rằng hơn 2,6 tỷ người sẽ sử dụng sinh trắc học để bảo đảm thanh toán vào năm 2023, do một số nhu cầu chủ yếu từ khách hàng như đảm bảo xác thực liên tục và nhanh chóng trong khi thanh toán không tiếp xúc với các khoản giá trị cao, cũng như đảm bảo an toàn bảo mật."

(NFCWorld)

Thanh toán thẻ chiếm ưu thế trong hoạt động bán lẻ tại Anh

Thanh toán thẻ hiện chiếm hơn 75% tổng lượng giao dịch bán lẻ tại Anh, bởi thanh toán không tiếp xúc (TTKTX) đang dần chiếm lĩnh thị phần của thanh toán tiền mặt.

Theo cuộc khảo sát thanh toán hàng năm mới đây nhất của Hiệp hội Bán lẻ Anh (BRC), ổng giá trị mua hàng thông qua thẻ thanh toán trong năm 2017 là 227,1 tỷ Bảng Anh, chiếm 76% tổng lượng hàng hóa bán lẻ.

Trong khi đó, thanh toán tiền mặt tiếp tục giảm trong cả hoạt động giao dịch bán lẻ (giảm 0,5%) và giá trị bán hàng (giảm 1,2%), và chỉ còn chiếm khoảng 22%.

BRC cho rằng sự tăng trưởng của các khoản thanh toán bằng thẻ đã tác động cả tới các thành viên của hiệp hội này, với việc các nhà bán lẻ phải chi bổ sung 170 triệu Bảng để xử lý các giao dịch thanh toán trong năm 2017. Các khoản phí hiện nay đã lên tới khoảng 1 tỷ Bảng mỗi năm.

BRC chỉ trích các tổ chức thẻ đã gây ra xu hướng gia tăng chi phí nói trên. Theo tổ chức này, các khoản phí đã tăng 37% trong năm 2017, và họ kêu gọi Chính phủ Anh cùng các cơ quan quản lý phải vào cuộc điều tra./.

(Finextra)

Giải pháp Kiểm tra Danh tính để xác minh thanh toán thẻ trực tuyến

MasterCard vừa đưa ra đề xuất về các giải pháp Kiểm tra Danh tính (Identity Check) dành cho các ngân hàng để xác thực danh tính trực tuyến.

MasterCard Labs đã phát triển công nghệ cho phép người dùng sử dụng các yếu tố thông tin sinh trắc cá nhân như vân tay, mống mắt, và khuôn mặt để xác minh danh tính. Phương thức này giúp người dùng xác thực qua thiết bị di động trong quá trình mua sắm trực tuyến, qua đó giảm tỷ lệ hủy bỏ giao dịch và cải thiện khả năng bảo mật cho các hoạt động ngân hàng

Theo MasterCard, 1 đến 2% giao dịch trực tuyến diễn ra tại Cộng hòa Ireland yêu cầu chủ thẻ xác thực thông tin sinh trắc để hoàn tất giao dịch, và các phương thức thông thường thực hiện thanh toán qua mật khẩu. Đến mùa Thu năm 2019, tỷ lệ này dự kiến đạt 25% khi các yêu cầu mới về phương thức xác thực có hiệu lực.

Bên cạnh đó, nghiên cứu đã chỉ ra rằng 95% giao dịch ngoại tuyến được ngân hàng chấp nhận, trong khi đối với giao dịch trực tuyến tỷ lệ đó chỉ là 86%. Sonya Geelon, Giám đốc của MasterCard Ireland cho rằng việc sử dụng mật khẩu để xác thực đã lỗi thời, vì mọi người có xu hướng quên, và do vậy các nhà bán lẻ phải đối mặt với tình trạng hủy bỏ đơn hàng. Cũng theo Sonya Geelon, thực trạng này đã kích thích nhu cầu dịch chuyển từ tiền mặt sang dùng thẻ, từ mật khẩu sang dấu vân tay và thậm chí vượt ra ngoài để đổi mới công nghệ như trí thông minh nhân tạo./.

(Paypers)

Nguồn ảnh: Internet

Những hiểm họa từ không gian mạng (Kỳ 1): Bài học chẳng bao giờ cũ

Phân tích chuyên ngành hết sức sâu sắc của Information Security Media Group, Inc. (iSMC) về những mối đe dọa đến từ không gian mạng đối với các tổ chức kinh doanh dịch vụ tài chính và ngân hàng trong năm 2018.

Trong năm qua, các tổ chức dịch vụ tài chính (FSI) đã chứng kiến sự gia tăng hết sức đáng lo ngại về số vụ việc liên quan đến rò gỉ dữ liệu (87%), số lượng thẻ bị đánh cắp (149%), tấn công mạng (151%), và các tài khoản mạng xã hội giả mạo (48%). Bên cạnh đó, các nhóm tin tặc ATP (Advanced Persistent Threat) được một số chính phủ tài trợ, với động cơ hầu như không phải là tài chính, vẫn tiếp tục nhằm vào các FSI để phát động chiến tranh và reo rắc chủ nghĩa khủng bố trên không gian mạng. Do các nhân tố đe dọa và các chiến thuật không gian mạng ngày một phát triển, nên chiến lược an ninh mạng các FSI cũng bắt buộc phải phát triển theo. Vì vậy, điều tối cần thiết là các tổ chức này cần phải có kiến thức sâu sắc về những công cụ, chiến thuật và quy trình mới nhất mà giới tội phạm mạng sử dụng để nhắm vào chính họ và các khách hàng của tổ chức, cũng như hoạt động mà những tổ chức này cần phải giám sát nhằm chặn trước các cuộc tấn công.

Chạy Box dữ liệu:

Một số thống kê đáng giật mình của iSMC trong "Báo cáo về tình hình gian lận tài chính năm 2018":
• Tăng 151% về số lượng tài sản của các FSI được rao bán và trao đổi trên các trang "web đen", đặc biệt là những trang mạng phục vụ giới tội phạm hoặc hành vi gian lận;
• Tăng 91% số vụ tấn công gian lận (phishing) nhằm vào các FSI;
• Tăng 149% lượng thông tin thẻ tín dụng bị đánh cắp với sự trỗi dậy của một xu thế mà trong đó những cao thủ hacker khai thác các trang web để bán lại thông tin thẻ đánh cắp được cho những tay hacker có trình độ kém hơn;
• Tăng 135% lượng thông tin về ngân hàng trực tuyến và lịch sử giao dịch ngân hàng được rao bán trên chợ đen bởi các hacker hiện sử dụng một proxy hoặc VPN để thực hiện những hành vi gian lận trên website của ngân hàng;
• Tăng 40% số vụ đánh cắp chứng thư của các nhân viên làm việc trong các FSI bởi phần lớn các tổ chức này vẫn sử dụng cách thức đăng nhập bằng "username" và "password", thay vì sử dụng công nghệ xác thực hai nhân tố.

Những mối đe dọa từ các nhóm tấn công APT được chính phủ tài trợ

Chúng ta đều đã được cảnh báo rằng những nhóm tấn công APT được một số quốc gia tài trợ đang đóng vai trò ngày càng quan trọng trong năm qua bởi vì nhiều nước đã nhận thức được sức mạnh của an ninh mạng. Ngày càng có nhiều lĩnh vực quan trọng liên quan tới chính phủ hoặc liên quan tới một nền kinh tế thực bị các nhóm này nhắm vào. Hiện nay, nếu bạn đánh sập một ngân hàng hoặc một tổ chức tài chính, hậu quả gây ra trên phương diện tài chính thậm chí sẽ nghiêm trọng hơn so với hậu quả từ một cuộc tấn công khủng bố hoặc một cuộc chiến tranh. Và xu hướng hết sức đáng ngại trên thế giới hiện nay là ngày càng có nhiều quốc gia nỗ lực trang bị cho mình khả năng tấn công APT để có thể thâm nhập và kiểm soát nền kinh tế của các quốc gia khác.

Để đối phó với xu hướng gia tăng hoạt động của giới hacker được chính phủ chống lưng cần đến một cơ chế tự vệ hiện đại hơn nhiều bởi vì những nhân vật này luôn có được nguồn hỗ trợ rất lớn, kể cả về tiền bạc và công nghệ. Chúng không chỉ chỉnh sửa những công cụ phổ biến để phục vụ mưu đồ riêng, mà còn phát triển những công cụ độc quyền với mức độ tinh vi rất cao. Bên cạnh đó, các nhóm APT luôn nhận thức được mục đích chiến lược của những cuộc tấn công, và các tổ chức tài chính lại chính là những mục tiêu hàng đầu đối với chúng.

Hướng tấn công nhằm vào dịch vụ ngân hàng di động (m-banking)

Một trong những xu hướng mà thế giới sẽ được chứng kiến là các hacker có thể tiếp cận được với những thông tin tài chính không chỉ vì mục đích đánh cắp tiền, thay vào đó, chúng cố gắng tống tiền các ngân hàng. Do sự tồn tại của các bộ luật và quy định hiện hành liên quan đến vấn đề quyền riêng tư, những hành vi này sẽ có thể gây ra tác hại rất lớn đối với các ngân hàng và uy tín của họ.

Báo cáo một vụ lỗ hổng dữ liệu với cơ quan chính phủ hoặc giải quyết một vụ rò gỉ dữ liệu cụ thể chắc chắn sẽ mang lại cho các ngân hàng nhiều rắc rối và những khoản tiền phạt từ phía các cơ quan chức năng. Khi các hacker tống tiền một tổ chức tài chính, mục đích của chúng là kiếm được nhiều tiền nhất có thể, trong khi đó nhiều nhà băng hiện nay cũng cố gắng làm mọi cách để kẻ gian “ngậm miệng” nhằm bảo vệ thương hiệu của họ.

Ngân hàng di động (m-banking) đang nhanh chóng trở thành một hướng tấn công chủ lực và là ưu tiên lựa chọn hàng đầu của một hacker bởi vì kênh dịch vụ này nhắm thẳng vào người dùng cuối của ngân hàng. Thông thường, những người dùng cuối không có nhân viên giám sát và thiết bị bảo mật để bảo vệ họ, đặc biệt là trên điện thoại, vì vậy họ luôn là mục tiêu dễ dàng để thực hiện hành vi đánh cắp thông tin tài chính và chiếm quyền kiểm soát đối với các chứng thư.

Các hacker sử dụng quyền chọn nhị phân của các ứng dụng ngân hàng hiện hành hoặc cố tình tạo ra những ứng dụng di động giả mạo, tích hợp malware vào những ứng dụng này, sau đó tái xuất bản trong những kho ứng dụng, và hy vọng sẽ xuất hiện những "con mồi" ngây thơ tải ứng dụng gian lận về. Nếu ứng dụng gian lận được tích hợp "key logger", nó sẽ ngấm ngầm thu thập các chứng thư, từ đó cho phép kẻ gian kiểm soát ĐTDĐ của nạn nhân và sử dụng chiếc điện thoại này cùng với thông tin xác thực của nạn nhân để thực hiện một số hành vi gian lận; theo một cách khác, kẻ gian sẽ tích hợp máy đào tiền kỹ thuật số vào các ứng dụng ngân hàng trực tuyến để đánh cắp tiền từ nạn nhân và sử dụng CPU trên ĐTDĐ để đào Bitcoin.

Hướng tấn công nhằm vào mạng xã hội

Hiện nay, ngày càng có nhiều người sử dụng mạng xã hội để kế nối với các ngân hàng, vì vậy theo dự báo của iSMC, đây sẽ là môi trường lý tưởng để gian lận tài chính sinh sôi nảy nở. Giới tội phạm mạng sẽ dụ dỗ nạn nhân truy cập vào các website giả mạo và lừa họ tải về các ứng dụng di động độc hại nhằm mục đích đánh cắp định danh cá nhân (PI) và thông tin nhận dạng. Cũng theo iSMC, các mạng xã hội là những nền tảng hết sức thuận lợi (dễ dàng hơn rất nhiều so với các nền tảng khác) để giới tội phạm đánh cắp dữ liệu và tấn công người dùng cuối bởi các tổ chức tài chính cũng đang ngày càng trở nên phức tạp.

Các diễn đàn và cộng đồng "web đen"

Một xu hướng khác mà chúng tôi muốn nhắc tới là xu hướng chuyển dịch từ tất cả các diễn đàn và các cộng đồng "web đen" - những nơi thường xuyên diễn ra hoạt động bán chác thông tin thẻ tín dụng, tài khoản ngân hàng trong những năm gần đây - sang hoạt động tuyển chọn "nội gián" đang làm việc trong các tổ chức dịch vụ tài chính…

Một vài năm trở lại đây, các ngân hàng trung ương đã có thể tóm cổ được những kẻ điều hành của những diễn đàn này và đưa chúng ra trước ánh sáng công lý. Vì vậy, thay vì chỉ sử dụng những cộng đồng nói trên, các hacker hiện chuyển sang sử dụng những cơ chế ngang hàng để liên lạc - bất cứ thứ gì từ ICQ (viết tắt của "I Seek You", là một chương trình máy tính nhắn tin tức thì lần đầu tiên được Mirabilis, một công ty Israel phát triển và phổ biến vào năm 1996 - PV), nếu bạn đang giao dịch với các hacker trên các thị trường ở Nga, tới một số nhóm WhatsApp, Telegrams, Jabber - nhằm xác minh chính xác một cá nhân không phải là nhân viên của ngân hàng trung ương trước khi cho phép truy cập vào các kênh bí mật này.

Đây là thủ đoạn mới của những kẻ bất lương. Do thủ đoạn này rất dễ thay đổi nên những kênh bí mật nói trên rất thường xuyên "biến hình", khiến lực lượng chấp pháp gặp quá nhiều khó khăn trong công tác điều tra. Rất khó để đóng cửa những kênh này bởi chẳng có người nào có thể đánh sập các diễn đàn trên WhatsApp hoặc Telegram hoặc ICQ một cách nhanh chóng.

Lừa đảo núp bóng dịch vụ (Phishing-as-a-Service)

Các cuộc tấn công lừa đảo tiếp tục phát triển và hiện nhằm vào các nhân viên ngân hàng, khách hàng của các ngân hàng và các tổ chức tài chính nói chung. Trong quá khứ, bạn phải xây dựng malware cho riêng mình hoặc có được web hosting của riêng mình để tạo lập nên một trang web hoặc công ty lừa đảo. Hiện nay, rào cản đối với một cuộc tấn công lừa đảo là gần nhưng không có, đây là một phần của một Bitcoin. Bạn có thể truy cập vào một trang web đen và tải về một bộ công cụ tấn công lừa đảo - có mức độ tinh vi hơn so những cuộc tấn công sử dụng các công cụ cá nhân mà chúng ta từng được chứng kiến trước đây. Chúng có thể thay đổi tên miền (domain), IP, và nhà cung cấp web hosting một các nhanh chóng, vì vậy giới chuyên môn luôn gặp khó trong công tác phát hiện và tìm kiếm dấu vết.

Thông qua công tác phân tích một số bộ công cụ lừa đảo, chúng tôi khẳng định phần lớn trong số chúng đều có một backdoor (cửa hậu), vì thế khi được bán cho một kẻ gian nào đó thì toàn bộ chứng thư và thông tin mà hắn đánh cắp được (nhờ những bộ công cụ này) trong chiến dịch lừa đảo cũng sẽ ngấm ngầm được chuyển về tay kẻ phát triển, từ đó giúp "cha đẻ" có "hàng" để bán kiếm lời. Do việc triển khai các cuộc tấn công lừa đảo được thực hiện một cách hết sức dễ dàng, nên các mối rủi ro đi kèm như lộ lọt và sử dụng thông tin đánh cắp đang trở nên ngày càng nghiêm trọng./. (Còn tiếp)

*Mời Quý vị Độc giả đón đọc **Kỳ 2: "Những hiểm họa từ không gian mạng: Liều thuốc đặc trị"** tại bản tin E-TGT #84*

MK® group

Smart Digital Security

www.mkgroup.com.vn | contact@mkgroup.com.vn | www.facebook.com.vn/mkgroup1999

Hà Nội: Tầng 11, tòa nhà TTC, 19 Duy Tân, Cầu Giấy | Tel: (+84-24) 6266 2703

Tp. Hồ Chí Minh: Tầng 7 Thiên Sơn Building, 5 Nguyễn Gia Thiều, Quận 3 | Tel: (+84-28) 3930 5023