BẢO MẬT TRONG THƯƠNG MẠI DI ĐỘNG (TMDĐ) TẠI VIỆT NAM - CÁC NGUY CƠ VÀ BIỆN PHÁP PHÒNG CHỐNG

Nguyễn Trần Hưng
Trường Đại học Thương mại
Email: hung.tmdt@gmail.com

Ngày nhận: 05/8/2013 *Ngày nhận lại 1: 29/8/2013* *Mã số: 60.2TrEM.22*

Được đánh giá là một trong những yếu tố quan trọng ảnh hưởng đến sự phát triển của thương mại di động (TMDĐ), vấn đề bảo mật luôn thu hút sự quan tâm của rất nhiều tổ chức và người dùng trên khắp thế giới khi tương tác trên thiết bị di động. Thực tiễn tại Việt Nam đã chỉ ra rằng, mặc dù việc triển khai ứng dụng TMDĐ bắt đầu từ rất sớm nhưng đến nay sự phát triển này vẫn chưa có bước tiến đáng kể nào, hình thức mong đợi là các giao dịch trực tuyến như: mua bán, thanh toán trên thiết bị di động chưa thực hiện được. Nguyên nhân cơ bản của thực tiễn này chính là vấn đề bảo mật trên thiết bị di động tại Việt Nam còn nhiều yếu kém, từ đó gây ra sự lo lắng cho người dùng và cả các doanh nghiệp cung cấp dịch vụ khi tiến hành các giao dịch thương mại. Bài viết cung cấp sự phân loại các nguy cơ phổ biến nhất hiện nay có thể xảy ra trên thiết bị di động và đưa ra các phương pháp phòng chống thích hợp nhằm thúc đẩy sự phát triển của bảo mật, qua đó thúc đẩy sự phát triển của TMDĐ tại Việt Nam.

Từ khóa: *thương mại di động, bảo mật, thiết bị di động*

Với sự phát triển không ngừng, các thiết bị di động đang trở thành một phần tất yếu trong cuộc sống của mọi người, cả trong công việc và đời sống cá nhân. Các giao tiếp trên thiết bị di động đã tăng đột biến gấp nhiều lần so với các giao tiếp trên máy tính cá nhân trước đây. Cũng chính vì đặc điểm này, các thiết bị di động trở nên hấp dẫn với những kẻ tấn công, do đó hàng loạt các đoạn mã độc đã liên tiếp được tung ra nhằm thu thập các thông tin trái phép hoặc đánh cắp tài khoản trực tiếp trên thiết bị di động của người dùng.

1. Khái quát vài nét về bảo mật trong TMDĐ

Với các khả năng như: độ phủ sóng rộng, tương tác dễ dàng giữa những người sử dụng, quản trị các hoạt động, cá nhân hóa dữ liệu và chu trình thực hiện đang được xem là những ưu điểm vượt trội của công nghệ di động trong các lĩnh vực khác nhau từ giải trí, giao dịch ngân hàng cho đến các ứng dụng kinh doanh khác. Thiết bị di động đang có sự gia tăng nhanh chóng trong đời sống và công việc kinh doanh. Trong năm 2011, các giao dịch qua thiết bị di động toàn cầu đạt 1,6 tỷ giao dịch và việc giao dịch vận chuyển, trao đổi qua máy tính bảng đạt 66,9 triệu giao dịch. Tuy nhiên, đây vừa được xem như lợi thế lại vừa được xem là các cơ hội mở đối với các kẻ tấn công (hacker). Năm 2011, mã độc di động đã tạo ra mối nguy hiểm mới,

ngày càng mạnh mẽ hơn. Mục tiêu tấn công lên các điện thoại thông minh, máy tính bảng đã và đang tạo ra các thách thức lớn cho người sử dụng, các doanh nghiệp và các nhà cung cấp dịch vụ.

Báo cáo về tình hình bảo mật trên thiết bị di động năm 2011 của Juniper Networks đưa ra bằng chứng về những kẻ tấn công công nghệ dịch chuyển sự tấn công từ các máy tính cá nhân đến các thiết bị di động nhằm mục đích chủ yếu là kiếm tiền từ hoạt động đó. Hiện nay, bọn tấn công ngày càng trở nên nguy hiểm, chúng chuyên tìm kiếm các món lợi cao hơn, có giá trị lớn hơn. Điều đó có nghĩa là các thông tin nhạy cảm của các doanh nghiệp, chính phủ, những nhà cung cấp dịch vụ và người sử dụng gặp phải rủi ro cao hơn.

Từ những nhận định trên, bảo mật trong TMDĐ có thể hiểu một cách đơn giản là tập hợp các phương pháp hay cách thức nhằm bảo vệ tính bí mật, tính toàn vẹn của tất cả các giao tiếp và quyền kiểm soát các thông tin cá nhân của người dùng trên thiết bị di động.

Theo khái niệm trên, về cơ bản bảo mật trong TMDĐ có một số đặc điểm sau đây:

Đảm bảo tính bí mật của thông tin giao tiếp: tất cả các trao đổi hai chiều trên thiết bị di động cần phải được đảm bảo không bị bên thứ ba can thiệp hay nghe trộm. Cho dù kẻ thứ ba có chặn đó được thông tin thì những thông tin đó đã ở dạng mã hóa, cho nên không thể nào đọc được, hiểu được. Đặc biệt là đảm bảo tính bí mật đối với các thông tin nhạy cảm về mật tài chính như: số tài khoản, số PIN, mật khẩu, mã số thẻ tín dụng, lịch sử giao dịch... tránh sự xâm nhập của bên thứ ba khi tham gia giao dịch.

Đảm bảo tính toàn vẹn của thông tin giao tiếp: tất cả các trao đổi hai chiều trên thiết bị di động cần phải được đảm bảo không bị sửa đổi về mặt nội dung, tức là nội dung dữ liệu bên gửi và bên nhận phải giống nhau hoàn toàn. Hay nói cách khác là nội dung trao đổi hai chiều không bị biến đổi trong quá trình truyền. Từ đó có thể đảm bảo chống lại sự mạo danh và sự thay đổi nội dung giao dịch hay các giao tiếp trên thiết bị di động.

Đảm bảo quyền kiểm soát các thông tin tài chính cá nhân của người dùng: bản thân thiết bị di động là vật dụng có tính cá nhân hóa rất cao, khác hẳn với một máy tính cá nhân có thể được sử dụng bởi nhiều người, thiết bị di động hầu như thuộc sở hữu của một cá nhân riêng lẻ. Chính vì vậy mà có nhiều dữ liệu nhạy cảm chẳng hạn như thông tin tài chính cá nhân được người dùng lưu trữ trên thiết bị di động, trong khi đó có rất nhiều ứng dụng hoặc đoạn mã độc tự động truy xuất dữ liệu người dùng khi người dùng tải ứng dụng, do đó những thông tin tài chính cá nhân bị đánh cắp và dẫn tới người dùng không thể kiểm soát được các thông tin đó. Do đó đặc điểm này của bảo mật yêu cầu các nhà cung cấp dịch vụ cần phải đảm bảo các ứng dụng của mình và để người dùng quyền cho phép sự truy xuất vào dữ liệu di động hay không của các ứng dụng đó.

2. Các nguy cơ đe dọa an toàn thông tin trong TMDĐ

Hiện nay, với sự gia tăng nhanh chóng của các giao dịch thương mại trên thiết bị di động đã làm xuất hiện một loạt các nguy cơ mới đe dọa sự bảo mật các dữ liệu cá nhân và tính riêng tư các giao dịch của người dùng bao gồm cả các đoạn mã độc và các nguy cơ lừa đảo người dùng.

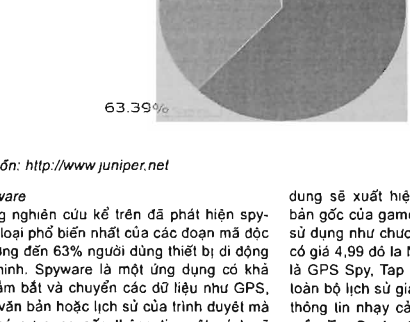
Theo báo cáo của một số tổ chức bảo mật lớn trên thế giới (Symantec.com, Kapersky) thì phần lớn thiết bị di động chưa triển khai một số giải pháp chống lại các đoạn mã độc (malware) một cách triệt để, điều này đặc biệt phổ biến tại một số quốc gia, trong đó có Việt Nam, Trung Quốc. Để phát tán đến một thiết bị di động, cách thông thường nhất là kẻ phát tán tạo ra các ứng dụng mã độc, đưa ứng dụng đến một kho ứng dụng và đơn giản là đợi người sử dụng tải về cài đặt trên thiết bị di động của mình. Bên cạnh đó, các nguy cơ lừa đảo người dùng trên thiết bị di động cũng không ngừng gia tăng.

Trong năm 2012, với sự phối hợp các tổ chức bảo mật uy tín của Juniper Networks, Junos - Pulse Mobile Security Suite, Symantec, Kapersky, Mobile info, Lockout Mobile Security đã phân tích 793.631 ứng dụng trên thiết bị di động từ các nguồn chính thức và không chính thức như: các kho ứng dụng hệ điều hành điện thoại, các kho ứng dụng bên thứ ba trên thế giới, các kho của website có các ứng dụng mã độc, các kho và web-

site của các hacker, các mẫu ứng dụng được đưa lên bởi người sử dụng, các mẫu ứng dụng được đưa lên bởi các thành viên trên diễn đàn. Kết quả của nghiên cứu đã đưa ra sự phân loại các nguy cơ trên thiết bị di động như sau:

Những đoạn mã độc trên thiết bị di động (biểu đồ 1):

Biểu đồ 1: *Những đoạn mã độc trên thiết bị di động năm 2012*



Nguồn: http://www.juniper.net

Spyware

Trong nghiên cứu kể trên đã phát hiện spyware là loại phổ biến nhất của các đoạn mã độc ảnh hưởng đến 63% người dùng thiết bị di động thông minh. Spyware là một ứng dụng có khả năng nắm bắt và chuyển các dữ liệu như GPS, ghi âm văn bản hoặc lịch sử của trình duyệt mà không có sự cung cấp thông tin một cách rõ ràng cho người sử dụng để nhận dạng các hoạt động của ứng dụng. Cuối cùng, các dữ liệu nắm giữ chuyển đến cho kẻ tấn công nhằm mục đích thu thập thông tin tài chính hoặc gây thiệt hại tài chính cũng như xâm nhập đến tính cá nhân của người sử dụng thiết bị di động. Giám đốc điều hành John Herring của công ty bảo mật Lookout Mobile Security đã cho biết ứng dụng Wallpaper Jackeey trên thiết bị di động sử dụng hệ điều hành Android đã được người dùng Việt Nam tải về hàng triệu lần, có thể thu thập số điện thoại của thiết bị, danh tính thuê bao và thậm chí cả thông tin thanh toán khi người dùng tiến hành các giao dịch thương mại. Mới đây nhất các nhà sản xuất bảo mật Symantec và F-Secure đã cảnh báo rằng Tap Snake, ứng dụng chơi game miễn phí trên thiết bị di động dùng để theo dõi và giám sát vị trí của người dùng. Tap Snake là phiên bản 2010 cho video game "Snake" mà những ai dùng điện thoại di động của Nokia đều biết. Tap Snake là một trong những ứng dụng di động phổ biến nhất ở Việt Nam cho những người dùng thiết bị di động sử dụng hệ điều hành Symbian hiện nay và nó cũng đang xuất hiện trên cửa hàng trực tuyến Android Market. Mặc dù ứng dụng sẽ xuất hiện cho người dùng như phiên bản gốc của game, nó cũng có thể được bí mật sử dụng như chương trình gián điệp thương mại có giá 4,99 đô la Mỹ (khoảng 100.000 đồng) tên là GPS Spy. Tap Snake cũng có khả năng đọc toàn bộ lịch sử giao dịch và truy cập vào những thông tin nhạy cảm trên thiết bị di động. Phần mềm Tap Snake được thiết kế để liên tục chạy ở chế độ nền (background) trên hệ thống di động.

SMS Trojan

Theo nghiên cứu của Juniper Networks, SMS trojan chiếm 36% trên tổng số các đoạn mã độc, chạy trên nền của ứng dụng và bí mật gửi tin nhắn SMS để lấy cắp tiền từ tài khoản sở hữu của người dùng di động, số tiền đó sẽ được chuyển vào tài khoản của kẻ tấn công. Khi tin nhắn được gửi, tiền không thể lấy lại và kẻ tấn

công được ẩn danh, vì vậy rất khó có thể dò tìm kẻ tấn công. Vào ngày 11/8/2010 trên thế giới phát hiện đoạn mã độc SMS Trojan đầu tiên trên các thiết bị di động thông minh có tên là FakePlayer. Mặc dù đoạn mã này chủ yếu thực hiện trên các thiết bị cài hệ điều hành Android, Symbian, tuy nhiên theo khuyến cáo của hãng bảo mật Kapersky, nó có thể thực hiện trên các hệ điều hành di động khác nhau. Mã độc mới lây nhiễm lên các thiết bị di động thông minh dưới dạng ứng dụng mở video. Nếu người dùng đồng ý sử dụng cài đặt ứng dụng này, Trojan sẽ thâm nhập hệ thống và gửi đi các thông báo SMS đến các số điện thoại mất phí mà không được sự đồng ý hay cho phép của người dùng thiết bị. Kết quả là tài khoản của người dùng bị trừ đi một số tiền tương ứng vào túi của tin tặc. Đối với người dùng Việt Nam gần đây cũng gặp phải các tình trạng tương tự, nhiều thuê bao di động mạng MobiFone và Vinaphone bống dưng nhận được nhiều cuộc gọi nhỡ từ các số điện thoại dạng: +88213300207, +88213300263, +88213300042, +88213300036 và trong tài khoản lập tức bị trừ đi một số tiền rất lớn, thường là hết sạch tiền trong tài khoản.

Các nguy cơ khác

Theo báo cáo bảo mật quý II/2013của Trend Micro, hãng bảo mật nổi tiếng thế giới dựa trên công nghệ điện toán đám mây, Việt Nam là quốc gia đứng thứ 3 trong việc tải về các phần mềm độc hại trên ứng dụng Android và là quốc gia đứng thứ 2 thế giới về mức độ rủi ro gặp phải về thông tin riêng tư trên thiết bị điện thoại di động. Ngoài những loại mã độc như trên, người dùng thiết bị di động trên thế giới cũng như tại Việt Nam còn phải đối mặt với các nguy cơ sau đây:

Các nguy cơ trên cơ sở trình duyệt

Không giống với các rủi ro dựa trên ứng dụng, dựa trên sự hiểu biết của người sử dụng khi tải các ứng dụng, sự tấn công dựa trên trình duyệt được tạo nên khi người dùng lướt qua một website. Thông qua một kỹ thuật được gọi là "drive-by download" người sử dụng không nghi ngờ việc ghé thăm một trang web và đoạn mã độc bắt đầu tải tự động không có sự cho phép hoặc hay biết của người sử dụng. Ví dụ như mối đe dọa trình duyệt được biết đến vào ngày 18/7/2010 có tên là CVE-2010-1807 cho phép kẻ tấn công từ xa có thể điều khiển các mã hoặc gây ra các DOS - tấn công từ chối dịch vụ thông qua các văn bản HTML hoặc phá hủy các ứng dụng. Tại Việt Nam số lượng các vụ tấn công kiểu này trên thiết bị di động xảy ra nhiều nhưng chưa có một sự thống kê cụ thể con số của các vụ tấn công. Trên thực tế khi xảy ra kiểu tấn công này, kẻ tấn công chỉ lợi dụng thiết bị di động của người dùng như một truy vấn thông tin hay một mũi tấn công để hướng tới máy chủ di động của một website nào đó, làm cho website đó bị gián đoạn hoạt động và máy chủ bị quá tải.

WiFi hacking

Với sự gia tăng của các thiết bị điện thoại thông minh và máy tính bảng có thể truy cập WiFi, số lượng WiFi hotspots toàn cầu được mong đợi có sự tăng trưởng từ 1,3 triệu năm 2011 đến 5,8 triệu năm 2015, tăng 350%. WiFi hotspots được xem là một kênh dễ dàng đối với kẻ tấn công. Với các công cụ FaceNiff và Firesheep, kẻ tấn công dễ dàng phát hiện người sử dụng trên mạng WiFi và có thể đánh cắp mật khẩu, thông tin tài chính và trong một số trường hợp lừa đảo sự xác nhận người sử dụng. Theo chuyên gia bảo mật cao cấp Sean Sullivan của hãng F- Secure thì Việt Nam là một trong 3 quốc gia Châu Á tải ứng dụng FaceNiff và Firesheep nhiều nhất, đây là các ứng dụng cho phép kẻ sử dụng chiếm quyền truy cập của người dùng Facebook, Twitter và các dịch vụ phổ biến khác qua mạng WIFi. Trong thực tế vừa qua tại Việt Nam, rất nhiều người dùng các tài khoản cá nhân trên mạng xã hội như Facebook, Twitter, Yahoo thông qua thiết bị di động và sử dụng mạng WiFi mở như ở các quán cà phê, hay những nơi công cộng đã bị mất tài khoản, mất quyền truy cập. Kẻ tấn công đã sử dụng chính những tài khoản mạo danh này để lừa đảo những người sử dụng khác như nhờ nạp thẻ điện thoại, hay vay tiền...

Tấn công MITM (Man-in-the-middle)

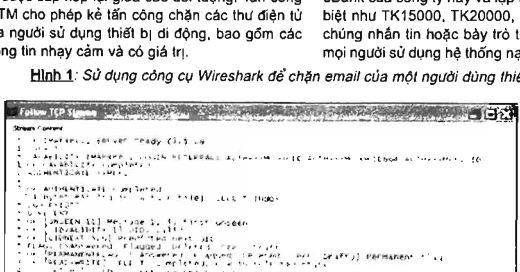
Tấn công MITM hoạt động bằng cách thiết lập các kết nối đến thiết bị di động của nạn nhân và tạm ngưng các tin nhắn gửi giữa các nạn nhân với nhau. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng mình đang truyền thông một cách trực tiếp với nạn nhân kia, trong khi đó sự

thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.

Các mạng WiFi có thể dễ dàng bị tấn công theo kiểu MITM (Man-in-the-middle). Khi thực hiện một tấn công MITM, kẻ tấn công chèn trong một dòng truyền thông từ thiết bị di động được kết nối với hệ thống WiFi không an toàn, truy nhập thông tin được sắp xếp lại giữa các đối tượng. Tấn công MITM cho phép kẻ tấn công chặn các thư điện tử của người sử dụng thiết bị di động, bao gồm các thông tin nhạy cảm và có giá trị.

tính cá nhân, lừa đảo qua tin nhắn SMS có nhiều biến thể khác nhau, mục đích cuối cùng đương nhiên là lấy cắp tiền trong tài khoản di động của người dùng. Kẻ tấn công có thể nhắn tin đánh lừa người dùng, thường là nội dung của các tin nhắn này nói về một chương trình khuyến mại hoặc phần thưởng nào đó và yêu cầu người dùng soạn tin nhắn theo mẫu gửi tới một tổng đài xác định. Tại Việt Nam trước đây, Công ty cổ phần Truyền thông và Công nghệ Quang Minh DEC cảnh báo khách hàng về việc một số kẻ đã lợi dụng hệ thống eBank của công ty này và lập tài khoản có tên đặc biệt như TK15000, TK20000, TK30000... Sau đó, chúng nhắn tin hoặc bày trò trên diễn đàn để lừa mọi người sử dụng hệ thống nạp tiền qua SMS của

Hình 1: *Sử dụng công cụ Wireshark để chặn email của một người dùng thiết bị di động*



Nguồn: http://www.f-secure.com

Fishing

Lừa đảo qua tin nhắn SMS luôn là nguy cơ thường trực và phổ biến với người dùng thiết bị di động. Khác hoàn toàn với lừa đảo trên các máy game chuyển tiền vào tài khoản. Mẫu tin nhắn người bị hại nhận được có dạng: "Để được thưởng 20.000 VND trong tài khoản, bạn hãy soạn tin nhắn theo cú pháp sau: NAPTIEN TK20000 và gửi

đến số 8778", hoặc "Chúc mừng bạn: Bạn là người may mắn trong chương trình khuyến mãi của chúng tôi, hãy soạn tin nhắn: NAPTIEN TK20000 và gửi đến số 8778 để nhận thưởng". Sau khi gửi đi, người dùng sẽ mất 20.000 đồng, còn kẻ tấn công sở hữu tài khoản eBank có tên truy cập TK20000 sẽ nhận được 10.000 DEC, loại tiền thanh toán các dịch vụ liên quan đến trò chơi Thế giới hoàn mỹ.

3. Các giải pháp bảo mật trên thiết bị di động

Sự gia tăng của các đoạn mã độc, các mối đe dọa và các nguy cơ lừa đảo trên thiết bị di động đã phản ánh sự tăng trưởng và cách thức sử dụng của người dùng trên toàn thế giới. Tại Việt Nam cũng vậy, ngày càng nhiều người sử dụng các thiết bị thông minh và máy tính bảng, tải các ứng dụng về các thiết bị này với mục đích giải trí như game, mạng xã hội hoặc điều khiển và quản lý các giao dịch tài chính. Điều này đã thu hút sự chú ý của các kẻ tấn công công nghệ, từ đó kẻ tấn công có sự điều chỉnh việc tấn công hoặc thay đổi hành vi nhằm truy cập trái phép vào các thiết bị di động.

Như phần tích ở trên, tại Việt Nam xuất hiện hầu hết các nguy cơ trên thiết bị di động, trong số đó có những nguy cơ người dùng biết và cả những nguy cơ người dùng không hay biết. Để chống lại những loại nguy cơ kể trên, giải pháp đưa ra phải đảm bảo thực hiện đồng bộ từ cả hai phía: cá nhân người dùng và doanh nghiệp cung cấp dịch vụ.

Đối với các cá nhân

Để có thể bảo vệ tốt hơn các thiết bị di động, dữ liệu và sự riêng tư từ gia tăng các đe dọa trên thiết bị di động, các cá nhân người dùng cần phải thực hiện những biện pháp sau đây:

Thứ nhất, người dùng thiết bị di động nếu sử dụng thường xuyên mạng 3G hoặc WiFi cần cài đặt chương trình như phần mềm diệt vi rút của chính các nhà cung cấp hệ điều hành của thiết bị như: Google, Apple hoặc của các tổ chức bảo mật uy tín: Symantec, Kapersky, F-Secure... để chống lại các ứng dụng trên thiết bị do không biết hoặc cố ý tải về.

Thứ hai, thiết bị di động dù thông minh thì về mặt bản chất cũng tương tự như máy tính cá nhân. Việc cài đặt bức tường lửa cá nhân trên thiết bị để bảo vệ các giao diện của thiết bị di động từ tấn công trực tiếp như: WiFi hacking hay MITM là điều cần thiết.

Thứ ba, hầu hết người dùng đều có suy nghĩ coi thiết bị di động là vật dụng bất ly thân nên thường không đặt mật khẩu. Điều này tạo ra lỗ hổng rất lớn khi sử dụng các mạng băng rộng như 3G hay WiFi vì khả năng bị truy cập từ xa vào thiết bị để lấy cắp thông tin mà người dùng không hay biết. Vì vậy, người dùng cần thiết phải sử dụng mật khẩu để truy cập vào thiết bị di động của mình.

Thứ tư, người dùng cần thận trọng khi tải các ứng dụng về thiết bị di động. Tương tự như máy tính cá nhân, các ứng dụng tải về từ những nguồn không rõ ràng thường tiềm ẩn những nguy cơ rất lớn như spyware hay trojan. Mặc dù các ứng dụng lan truyền đoạn mã độc có thể xuất hiện cả trong các kho và thị trường ứng dụng được cấp phép, nhưng tốt nhất là người dùng nên tránh các kho ứng dụng của bên thứ ba nhiều nhất có thể hoặc chỉ tải các ứng dụng từ các nguồn đáng tin cậy, chính thức.

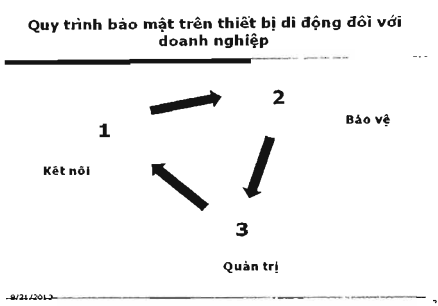
Thứ năm, một người dùng thiết bị di động chuyên nghiệp cũng nên cài đặt các phần mềm lưu trữ, xóa vị trí, khóa thiết bị từ xa, quét hoặc khôi phục để tìm lại thiết bị nhằm bảo vệ hoặc lưu trữ các dữ liệu cá nhân trên thiết bị di động bị đánh cắp.

Thứ sáu, người dùng thiết bị di động nên sử dụng phần mềm chống thư rác để bảo vệ các truyền thông dữ liệu qua đàm thoại, tin nhắn SMS và MMS không mong muốn. Tuy nhiên có một lưu ý là người dùng nên sử dụng những phần mềm chống thư rác thích hợp trong các kho ứng dụng đã được xét duyệt và kiểm tra kỹ lưỡng của Google Adroid hay Apple stores, tránh sự mạo danh của các ứng dụng độc hại từ các nguồn không rõ ràng.

Đối với các doanh nghiệp

Việc chống lại các nguy cơ trên thiết bị di động không chỉ là việc của cá nhân người dùng. Các doanh nghiệp, tổ chức cung cấp thiết bị, dịch vụ ứng dụng, dịch vụ viễn thông di động phải là những doanh nghiệp chủ động và tiên phong khi thực hiện các giải pháp an toàn, an ninh di động. Nhìn chung với bất kỳ một doanh nghiệp nào, kinh doanh trên thiết bị di động đều phải thực hiện đồng thời và liên tục quy trình bảo mật sau đây (hình 2):

Hình 2: *Quy trình bảo mật trên thiết bị di động đối với doanh nghiệp*



Nguồn: Bộ môn Nguyên lý Thương mại điện tử 2012, Bài giảng Thương mại di động

Kết nối

Đối với một doanh nghiệp cung cấp dịch vụ dù là doanh nghiệp viễn thông hay doanh nghiệp giá trị gia tăng thì việc bảo vệ dữ liệu khi kết nối với người dùng là điều cần thiết.

Thứ nhất, doanh nghiệp cần phải sử dụng một mạng riêng ảo - VPN (Virtual Private Network) và giao thức bảo mật tối thiểu SSL (Secure Socket Layer) cho phép doanh nghiệp bảo vệ dữ liệu trong việc truyền, đảm bảo an ninh, an toàn trong truy cập mạng dữ liệu di động của người dùng như 3G và WiFi

Thứ hai, để đảm bảo kết nối an toàn, doanh nghiệp cần tích hợp với các công nghệ kiểm soát truy cập mạng - Network access control (NAC) để quyết định quyền truy cập thích hợp dựa trên nhận diện người sử dụng và đặc điểm an ninh thiết bị, nhằm ngăn chặn những người hoặc những dữ liệu không hợp pháp.

Bảo vệ

Bảo vệ được hiểu theo hai khía cạnh, đó là bảo vệ dữ liệu truy cập để đảm bảo truy cập luôn thông suốt và bảo vệ người dùng trước những nguy cơ tiềm ẩn trên thiết bị di động khi tải các ứng dụng. Để làm được điều này, doanh nghiệp cần thực hiện các nhiệm vụ sau đây:

Thứ nhất, một doanh nghiệp kinh doanh trên thiết bị di động, các dịch vụ hỗ trợ cho người dùng phải tương thích trên các nền di động chủ yếu, như: Google Android, RIM Black Berry, Apple IOS, M.Windows Mobile và Nokia Symbian.

Thứ hai, doanh nghiệp có phần mềm quét và phát hiện các đoạn mã độc ẩn mình, đồng thời phải có thông báo cụ thể dưới dạng các cảnh báo an ninh tới thiết bị di động để bảo vệ người dùng chống lại các ứng dụng mã độc hại khi họ vô tình tải về máy như: spyware, các thẻ SD nhiễm độc và các tấn công dựa trên kết nối thiết bị di động.

Thứ ba, doanh nghiệp cần tập trung vào các công cụ, phần mềm truy xét địa điểm, dấu vết để tìm lại thiết bị, có thể cho phép khóa thiết bị, khôi phục hoặc bảo vệ sự lưu trữ dữ liệu trên thiết bị nhằm hỗ trợ người dùng, chẳng hạn như: iOS của Apple cho phép dò tìm thiết bị và khóa thiết bị từ xa

Thứ tư, khi người dùng tải ứng dụng doanh nghiệp phải thực hiện kiểm tra bằng phần mềm bức tường lửa trên thiết bị di động để tự bảo vệ trước các tấn công DDOS nhằm đảm bảo truy cập luôn thông suốt cho những người dùng hợp pháp.

Quản trị

Công tác quản trị của doanh nghiệp kinh doanh trong bảo mật trên thiết bị di động cần thực hiện các nhiệm vụ sau đây:

Thứ nhất, quản trị tập trung để có sự nhất quán trong thực thi và báo cáo các chính sách an toàn thông qua sự phổ biến bằng tin nhắn SMS trên toàn bộ các thiết bị di động, nhằm cảnh báo cho người dùng ở mức tốt nhất.

Thứ hai, doanh nghiệp cần phải Giám sát thiết bị và kiểm soát, chẳng hạn như giám sát của tin nhắn (SMS và MMS) từ các nguồn không rõ ràng, kiểm soát các ứng dụng đã được cài đặt và các ứng dụng mới được đưa lên các kho ứng dụng. Điều này sẽ giúp giảm thiểu các ứng dụng độc hại và có thể đo lường được mức độ lan tỏa của các ứng dụng hay các đoạn mã độc để đưa ra những cảnh báo thích hợp cho người dùng.

Thứ ba, nâng cao khả năng quản lý để thực thi chính sách bảo mật, chẳng hạn như khi khách hàng truy cập dịch vụ, doanh nghiệp nên yêu cầu khách hàng phải sử dụng các mã PIN, mật khẩu, cũng như khuyến cáo khách hàng xác định và thực thi sức mạnh mật mã thiết bị trước khi kết nối để thực hiện giao dịch.

Kết luận

Bảo mật trong TMDĐ là một trong những vấn đề phức tạp nhất và làm nền tảng thúc đẩy các hoạt động mua bán thanh toán trên thiết bị di động của người dùng vì tạo được sự yên tâm, tin tưởng khi kết nối và truy xuất dữ liệu nhạy cảm như các thông tin tài chính cá nhân. Tại Việt Nam, mặc dù được đánh giá là quốc gia có sự phát triển khá nhanh về các hoạt động TMDĐ, tuy nhiên bảo mật lại là vấn đề nhức nhối chưa có lời giải đáp thỏa đáng. Trước sự bùng nổ của các thiết bị di động thông minh, tìm hiểu các nguy cơ có thể xảy ra trên thiết bị di động khi tiến hành giao dịch và đưa ra các giải pháp thích hợp cho cả người dùng cá nhân và doanh nghiệp giúp gia tăng nhận thức, đồng thời thúc đẩy sự phát triển TMDĐ của Việt Nam lên một tầm cao mới.◆

Tài liệu tham khảo:

1. Strategy Analytics, *Global Handset Shipments Reach 1.6 Billion Units in 2011*, January 26, 2012.

2. Strategy Analytics, *Android Captures Record 39 Percent Share of Global Tablet Shipments in Q4 2011*, January 26, 2012.

3. ComScore MobiLens, *ComScore Reports November 2011 U.S. Mobile Subscriber Market Share*, December 29, 2011.

4. Dasient, *Mobile Malware Madness and How to Cap the Mad Hatters: A Preliminary Look at Mitigating Mobile Malware*,July 2011.

5. Consumer Reports, *Online exposure: Social networks, mobile phones, and scams can threaten your security*, June 2011.

6. Juniper Networks, *2011 Mobile Threats Report*, February 2012.

7. Juniper Networks, *Third Annual Mobile Threats Report*, March 2013.

8. Efraim Turban, *Electronic Commerce - A Managerial Perspective*, Prentice Hall PTR 2012.

9. Các website:
http://www.strategyanalytics.com
http://www.comscore.com
http://www.dasient.com/mobile-malware-madness/
http://www.consumerreports.org
http://www.f-secure.com
http://www.symantec.com
http://www.kapersky.com

Summary

As one of the most influential factors to the development of mobile commerce, security has always been the big concern of many organizations and users all over the world when interacting on mobile devices. The situation in Vietnam revealed that despite the early implementation of mobile commerce application, its development to now has yet made any remarkable progress. Moreover, such expected online commerce as trading, payment on mobile devices have not been widely exercised. Weak security on mobile devices in Vietnam is said to be the reason for this situation, which generates worry among users and even service providers in dealing with trading transactions. The article provides the classification of the current most popular forms of possible risks for mobile devices. Furthermore, it also suggests some relevant prevention methods to promote the development of security and mobile commerce in Vietnam.