Chương IV.

Rủi ro và phòng tránh rủi ro trong thương mại điện tử

1. Tổng quan về an toàn và phòng tránh rủi ro trong thương mại điện tử

1.1. Vai trò của an toàn và phòng tránh rủi ro trong thương mại điện tử

Ngày nay, vấn đề an ninh cho thương mại điện tử đã không còn là vấn đề mới mẻ. Các bằng chứng thu thập được từ hàng loạt các cuộc điều tra cho thấy những vụ tấn công qua mạng hoặc tội phạm mạng trong thế giới thương mại điện tử đang gia tăng nhanh từng ngày. Theo báo cáo của Viện An ninh Máy tính (CSI) và FBI (Mỹ) về thực trạng các vụ tấn công vào hoạt động thương mại điện tử năm 2002 cho biết:

- Các tổ chức tiếp tục phải chịu những cuộc tấn công qua mạng từ cả bên trong lẫn bên ngoài tổ chức. Trong những tổ chức được điều tra, khoảng 90% cho rằng họ đã thấy có sự xâm phạm an ninh trong vòng 12 tháng gần nhất.

- Các hình thức tấn công qua mạng mà các tổ chức phải chịu rất khác nhau: 85% bị virus tấn công, 78% bị sử dụng trái phép mạng internet, 40% là nạn nhân của tấn công từ chối dịch vụ (DoS).

- Thiệt hại về tài chính qua các vụ tấn công qua mạng là rất lớn: 80% các tổ chức được điều tra trả lời rằng họ đã phải chịu thiệt hại về tài chính do hàng loạt các kiểu tấn công khác nhau qua mạng. Tổng thiệt hại của những tổ chức này khoảng 455 triệu đôla Mỹ.

- Cần phải sử dụng nhiều biện pháp đồng thời để nâng cao khả năng phòng chống các vụ tấn công qua mạng. Hầu hết các tổ chức được điều tra đều trả lời rằng họ đã sử dụng các thiết bị bảo vệ an ninh, tường lửa, quản lý việc truy cập hệ thống. Tuy nhiên, không có tổ chức nào tin rằng hệ thống thương mại điện tử của mình tuyệt đối an toàn.

Ngoài ra, theo báo cáo của Trung tâm ứng cứu khẩn cấp máy tính (CERT) của đại học Carnegie Mellon (Mỹ), số lượng nạn nhân của những vụ tấn công qua mạng tăng từ 22.000 vụ năm 2000 lên đến 82.000 vụ năm 2002, và con số này cao gấp 20 lần so với con số nạn nhân năm 1998. Để đối phó với tình trạng mất an ninh qua mạng, ở

hầu hết các nước đã thành lập những trung tâm an ninh mạng mang tính quốc gia, như Trung tâm bảo về Cơ sở hạ tầng quốc gia (NIPC) trực thuộc FBI (Mỹ), có chức năng ngăn chặn và bảo vệ hạ tầng quốc gia về viễn thông, năng lượng, giao thông vận tải, ngân hàng và tài chính, các hoạt động cấp cứu và các hoạt động khác của chính phủ. Tại Việt Nam cũng đã thành lập Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VnCERT- Vietnam Computer Emergency Response Teams) vào tháng 12/2005 theo quyết định số 13/2006/QĐ-BBCVT. Trung tâm VNCERT sẽ là đầu mối trao đổi thông tin với các trung tâm an toàn mạng quốc tế của Việt Nam và hợp tác với các tổ chức CERT trên thế giới. Theo ông Đỗ Duy Trác, phụ trách CERT, thì trong những năm gần đây, tội phạm tin học gia tăng cả về phạm vi và mức độ chuyên nghiệp. Ban đầu là lấy cắp mật khẩu thể tín dụng để mua sách và phần mềm qua mạng, tiếp đến là làm thẻ tín dụng giả để lấy cắp tiền từ máy ATM, thiết lập các mạng máy tính giả để gửi thư rác, thư quảng cáo, hay tấn công từ chối dịch vụ, thậm chí ngang nhiên hơn nữa là đe dọa tấn công, tống tiền hay bảo kê các website thương mại điện tử

1.2. Rủi ro trong thương mại điện tử tại Việt Nam

Việt Nam là nước đi sau trong ứng dụng thương mại điện tử và mức độ phát triển của lĩnh vực này còn hạn chế. Tuy nhiên Việt Nam cũng không tránh khỏi được những rủi ro mà các nước phát triển về thương mại điện tử gặp phải. Số vụ tấn công các trang web với mục đích xấu hay cảnh bảo, cũng như số vụ ăn trộm thông tin tài khoản thanh toán của cá nhân trên mạng ngày càng gia tăng.

Báo động nạn "đi chợ mạng" rút tiền tỷ trong tài khoản người khác

Vào 16h30' ngày 18-12-2005, cơ quan điều tra Công an quận Đống Đa đã phối hợp với một đơn vị Công an quận Ba Đình (Hà Nội) thực hiện lệnh bắt và khám xét khẩn cấp nơi ở của Nguyễn Anh Tuấn, một đối tượng trong đường dây trộm cắp tiền qua mạng. Tuấn (sinh năm 1986) có hộ khẩu thường trú tại phường Bắc Hà, thị xã Hà Tĩnh, hiện đang là sinh viên của Trường đại học Bách khoa Hà Nội. Theo như khai nhận của Tuấn trước cơ quan điều tra thì sau khoảng một năm ra Hà Nội học đại học, thấy Tuấn có khả năng tin học, một số anh chị quen biết học khóa trên đã rủ "vào mạng" chơi. Họ cũng hướng dẫn Tuấn cách rút tiền bằng việc làm giả các thẻ ATM của các ngân hàng ở Việt Nam. Lâu dần, Tuấn trở thành một thành viên trong đường dây lừa đảo chiếm đoạt tài sản tiền gửi tại ngân hàng Mỹ mà cơ quan Công an đang bóc gỡ. Qua máy tính, ngồi ngay tại nhà riêng, các đối tượng này đã rút số tiền tương đương 590 triệu đồng về Việt Nam qua hệ thống ngân hàng Vietcombank.

Ngày 22-11, các điều tra viên Đội 3, Phòng Cảnh sát điều tra tội phạm về Trật tự xã hội Công an Hà Nội phát hiện được một vụ "đi chợ mạng" gồm 5 đối tượng, hầu hết đang là sinh viên đã thực hiện hàng chục vụ "bẻ" mật mã trộm tiền trong tài khoản của người nước ngoài... Các đối tượng này đã vào mạng, lợi dụng các mã số tài khoản của người nước ngoài để làm lệnh rút tiền ra. Từ đó, họ không chuyển tiền mặt về Việt Nam mà thông qua một mạng bán hàng trung gian để mua các loại hàng hóa có giá trị như điện thoại di động, máy tính xách tay, sách tin học, ngoại ngữ... với số tiền hàng nghìn USD rồi chuyển về.

Nguồn: Báo Công an nhân dân 22/12/2005 & Báo cáo TMĐT Việt Nam 2005

Chỉ tính riêng từ đầu năm 2006 đến 8/2006 tại Việt Nam đã có 4 virus được tung lên mạng, trong tháng 9/2006 có 15 virus.

1.3. Vai trò của chính sách và quy trình bảo đảm an toàn đối với TMĐT

Xây dựng chính sách về an ninh an toàn mạng và yêu cầu mọi người phải chấp hành có ý nghĩa quan trọng trong việc xây dựng ý thức và thể chế hóa hoạt động bảo vệ an ninh cho thương mại điện tử. Chính sách này thường bao gồm các nội dung sau:

- Quyền truy cập: xác định ai được quyền truy cập vào hệ thống, mức độ truy cập và ai giao quyền truy cập

- Bảo trì hệ thống: ai có trách nhiệm bảo trì hệ thống như việc sao lưu dữ liệu, kiểm tra an toàn định kỳ, kiểm tra tính hiệu quả các biện pháp an toàn,…

- Bảo trì nội dung và nâng cấp dữ liệu: ai có trách nhiệm với nội dung đăng tải trên mạng intranet, internet và mức độ thường xuyên phải kiểm tra và cập nhật những nội dung này

- Cập nhật chính sách an ninh thương mại điện tử: mức độ thường xuyên và ai chịu trách nhiệm cập nhật chính sách an ninh mạng và các biện pháp đảm bảo việc thực thi chính sách đó.

2. Rủi ro chính trong thương mại điện tử

2.1. Một số rủi ro chính doanh nghiệp có thể gặp phải trong thương mại điện tử

Rủi ro trong thương mại điện tử có thể chia thành bốn nhóm cơ bản sau:

- Nhóm rủi ro dữ liệu
- Nhóm rủi ro về công nghệ
- Nhóm rủi ro về thủ tục quy trình giao dịch của tổ chức
- Nhóm rủi ro về luật pháp và các tiêu chuẩn công nghiệp

Các nhóm rủi ro này không hoàn toàn độc lập với nhau mà đôi khi chúng đồng thời cùng xảy đến và không xác định tách bạch rõ ràng được. Nếu các rủi ro này đồng thời xảy ra, thiệt hại đối với tổ chức có thể rất lớn cả về uy tín, thời gian và chi phí đầu tư để khôi phục hoạt động trở lại bình thường.

2.2. Một số dạng tấn công chính vào các website thương mại điện tử

Trong thương mại điện tử, ngoài những rủi ro về phần cứng do bị mất cắp hay bị phá hủy các thiết bị (máy tính, máy chủ, thiết bị mạng...), các doanh nghiệp có thể phải chịu những rủi ro về mặt công nghệ phổ biến như sau:

- Virus

Virus tấn công vào thương mại điện tử thường gồm 3 loại chính: virus ảnh hưởng tới các tệp (file) chương trình (gắn liền với những file chương trình, thường là .COM hoặc .EXE), virus ảnh hưởng tới hệ thống (đĩa cứng hoặc đĩa khởi động), và virus macro. Virus macro là loại virus phổ biến nhất, chiếm từ 75% đến 80% trong tổng số các virus được phát hiện. Đây là loại virus đặc biệt chỉ nhiễm vào các tệp ứng dụng

soạn thảo, chẳng hạn như các tệp ứng dụng của MS Word, Excel và Power Point . Khi người sử dụng mở các tài liệu bị nhiễm virus trong các chương trình ứng dụng, virus này sẽ tự tạo ra các bản sao và nhiễm vào các tệp chứa đựng các khuôn mẫu của ứng dụng, để từ đó lây sang các tài liệu khác.

Các loại virus có thể gây ra những tác hại nghiêm trọng, đe doạ tính toàn vẹn và khả năng hoạt động liên tục, thay đổi các chức năng, thay đổi các nội dung dữ liệu hoặc đôi khi làm ngưng trệ toàn bộ hoạt động của nhiều hệ thống trong đó có các website thương mại điện tử. Nó được đánh giá là mối đe doạ lớn nhất đối với an toàn của các giao dịch thương mại điện tử hiện nay.

- Tin tặc (hacker) và các chương trình phá hoại (cybervandalism)

Tin tặc hay tội phạm máy tính là thuật ngữ dùng để chỉ những người truy cập trái phép vào một website, một cơ sở dữ liệu hay hệ thống thông tin. Thực chất mục tiêu của các hacker rất đa dạng. Có thể là hệ thống dữ liệu của các website thương mại điện tử, hoặc với ý đồ nguy hiểm hơn chúng có thể sử dụng các chương trình phá hoại (cybervandalism) nhằm gây ra các sự cố, làm mất uy tín hoặc phá huỷ website trên phạm vi toàn cầu.

Ngày 1-4-2001, tin tặc đã sử dụng chương trình phá hoại tấn công vào các máy chủ có sử dụng phần mềm Internet Information Server (IIS) của Microsoft nhằm làm giảm uy tín của phần mềm này và rất nhiều nạn nhân như hãng hoạt hình Walt Disney, Nhật báo phố Wall …đã phải gánh chịu hậu quả cả về tài chính và uy tín.

- Rủi ro về gian lận thẻ tín dụng

Trong thương mại điện tử, các hành vi gian lận thẻ tín dụng xảy ra đa dạng và phức tạp hơn nhiều so với thương mại truyền thống. Nếu như trong thương mại truyền thống, việc mất thẻ hoặc thẻ bị đánh cắp là mối đe doạ lớn nhất đối với khách hàng thì trong thương mại điện tử mối đe doạ lớn nhất là bị "mất" (hay bị lộ) các thông tin liên quan đến thẻ tín dụng hoặc các thông tin giao dịch sử dụng thẻ tín dụng trong quá trình thực hiện các giao dịch mua sắm qua mạng và các thiết bị điện tử. Các tệp chứa dữ liệu thẻ tín dụng của khách hàng thường là những mục tiêu hấp dẫn đối với tin tặc khi tấn công vào website thương mại điện tử. Hơn thế, những tên tội phạm có thể đột nhập vào

các cơ sở dữ liệu của website thương mại điện tử để lấy cắp các thông tin của khách hàng như tên, địa chỉ, điện thoại… với những thông tin này chúng có thể mạo danh khách hàng thiết lập các khoản tín dụng mới nhằm phục vụ những mục đích phi pháp.

- Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (DOS - Denial Of Service attack, DDOS – Distributed DOS hay DR DOS) là kiểu tấn công khiến một hệ thống máy tính hoặc một mạng bị quá tải, dẫn tới không thể cung cấp dịch vụ hoặc phải dừng hoạt động. Sơ khai nhất là hình thức DoS (Denial of Service), lợi dụng sự yếu kém của giao thức TCP, tiếp đến là DDoS (Distributed Denial of Service) - tấn công từ chối dịch vụ phân tán, và gần đây là DRDoS - tấn công theo phương pháp phản xạ phân tán (Distributed Reflection Denial of Service).

Những cuộc tấn công DoS có thể là nguyên nhân khiến cho mạng máy tính ngừng hoạt động và trong thời gian đó, người sử dụng sẽ không thể truy cập vào các website thương mại điện tử. Những tấn công này cũng đồng nghĩa với những khoản chi phí rất lớn vì trong thời gian website ngừng hoạt động, khách hàng không thể thực hiện các giao dịch mua bán. Đồng thời, sự gián đoạn hoạt động này sẽ ảnh hưởng đến uy tín và tiếng tăm của doanh nghiệp, những điều không dễ dàng gì lấy lại được. Mặc dù những cuộc tấn công này không phá huỷ thông tin hay truy cập vào những vùng cấm của máy chủ nhưng tạo ra phiền toái, gây trở ngại cho hoạt động của nhiều doanh nghiệp**.** Vụ tấn công DOS điển hình đầu tiên xảy ra vào tháng 2-2000, các hoạt động tấn công liên tục khiến hàng loạt website trên thế giới ngừng hoạt động trong nhiều giờ, trong đó có những website hàng đầu như: eBay ngừng hoạt động trong 5 giờ, Amazon gần 4 giờ, CNN gần 3.5 giờ, E-Trade gần 3 giờ, Yahoo và Buy.com và ZDNet cũng ngừng hoạt động từ 3 đến 4 giờ. Ngay cả người khổng lồ Microsoft cũng đã từng phải gánh chịu hậu quả của những cuộc tấn công này. Ở Việt Nam,cũng đã có rất nhiều doanh nghiệp bị tấn công dưới hình thức này.

- Kẻ trộm trên mạng (sniffer)

Kẻ trộm trên mạng (sniffer) là một dạng của chương trình theo dõi, nghe trộm, giám sát sự di chuyển của thông tin trên mạng. Khi sử dụng vào những mục đích hợp pháp, nó có thể giúp phát hiện ra những yếu điểm của mạng, nhưng ngược lại, nếu sử

dụng vào các mục đích phi pháp, các phần mềm ứng dụng này sẽ trở thành các mối hiểm hoạ lớn và rất khó có thể phát hiện. Kẻ trộm sử dụng các phần mềm này nhằm lấy cắp các thông tin có giá trị như thư điện tử, dữ liệu kinh doanh của các doanh nghiệp, các báo cáo mật…từ bất cứ nơi nào trên mạng.

Xem lén thư điện tử là một dạng mới của hành vi trộm cắp trên mạng. Kỹ thuật xem lén thư điện tử là sử dụng một đoạn mã (ẩn) bí mật gắn vào thông điệp thư điện tử, cho phép người nào đó có thể giám sát toàn bộ các thông điệp chuyển tiếp được gửi đi cùng với thông điệp ban đầu. Chẳng hạn một nhân viên phát hiện thấy lỗi kỹ thuật trong khâu sản xuất, anh ta lập tức gửi một báo cáo thông báo cho cấp trên về phát hiện của mình. Người này sau đó sẽ tiếp tục gửi thông báo đến tất cả các bộ phận có liên quan trong doanh nghiệp. Một kẻ nào đó sử dụng kỹ thuật xem lén thư điện tử có thể theo dõi và biết được toàn bộ thông tin trong bức thư điện tử gửi tiếp sau đó bàn về vấn đề này.

- Phishing – " kẻ giả mạo"

Phishing là một loại tội phạm công nghệ cao sử dụng email, tin nhắn pop-up hay trang web để lừa người dùng cung cấp các thông tin cá nhân nhạy cảm như thẻ tín dụng, mật khẩu, số tài khoản ngân hàng. Thông thường các tin tặc thường giả mạo là các công ty nổi tiếng yêu cầu khách hàng cung cấp những thông tin nhạy cảm này. Các website thường xuyên bị giả mạo đó là Paypal, Ebay, MSN, Yahoo, BestBuy, American Online….Kẻ giả mạo thường hướng tới phishing những khách hàng của ngân hàng và người tiêu dùng thường mua sắm trực tuyến. Những thông tin ăn cắp đươc sẽ được kẻ giả mạo dùng để truy cập với mục đích xấu, nếu là thông tin về tài khoản thanh toán thì sẽ dùng vào mục đích mua hàng hoặc rút tiền. Bất cứ ai cũng có thể phishing được vì phần mềm phishing là có nhiều trên mạng với hướng dẫn chi tiết cùng với danh sách địa chỉ email. Công nghệ phishing là đã có từ những năm 1987, tuy nhiên nó chỉ thực sự biết đến rộng rãi vào năm 1996. AOL là công ty đầu tiên đã bị kẻ giả mạo tấn công ăn cắp thông tin của khách hàng. Hay Vào 17/12/2003 một số khách hàng của eBay nhận đươc email với thông báo rằng hiện tại tài khoản của họ tạm ngừng hoạt động cho tới khi họ kích vào đường link được cung cấp trong email và cập nhật thông tin về thẻ tín dụng, cùng với các thông tin cá nhân khác như ngày sinh, tên thời

con gái của mẹ, số Pin của thẻ ATM. Đường link trong địa chỉ email kết nối tới trang web của ebay nhưng đây không phải là trang web thật của ebay mà chỉ là một trang web giả mạo có logo và hình thức giống với trang web ebay thật. PayPal một trang web giải pháp thanh toán cũng là đối tượng thường xuyên bị giả mạo. Kẻ giả mạo Paypal đã xây đường URL cải trang giống URL của Paypal bằng cách sử dụng ký hiệu @ (http://paypal.com@218.36.41.188/fl/login.html). Thường thì các server bỏ qua các ký tự trước @ và chỉ sử dụng những ký tự sau nó. Như vậy là khách hàng chỉ có thể nhìn thấy đường link trong mail như http://paypal.com Chính vì vậy mà khách hàng đã không nhận ra được là mình đang bị tấn công từ các tin tặc và đã cung cấp nhưng thông tin cá nhân và tài khoản.

- Ngoài ra, tội phạm TMĐT được thực hiện dưới nhiều hình thức sau: phát triển các mạng máy tính ma (bots network) để tấn công DOS, gửi thư rác, gửi thư rác với quy mô lớn (dịch vu thư rác), thuê hacker phá hoại website của đối thủ cạnh tranh, thu thập thông tin người sử dụng bằng spyware.

3. Xây dựng kế hoạch an ninh cho thương mại điện tử

Việc xây dựng kế hoạch an ninh thương mại điện tử cho doanh nghiệp bao gồm 4 giai đoạn sau:

- Giai đoạn đánh giá: Giai đoạn này xác định những tài sản doanh nghiệp có, bao gồm cả tài sản hữu hình và vô hình. Giá trị tài sản phải được định rõ, cả về mặt tài chính và phi tài chính và định rõ tầm quan trọng của từng tài sản đối với doanh nghiệp và từ đó đánh giá khả năng bị tấn công của từng tài sản. Việc đánh giá gồm các nội dung sau:

+ *Xác định các mối đe dọa:* đa số những vụ xâm phạm an ninh trái phép là do sự can thiệp trực tiếp hay gián tiếp của con người các hệ thống và những người có quyền truy cập tới tài sản phải được định rõ như giám đốc IT, nhân viên, các nhà tư vấn,… Khả năng mối đe dọa trở thành hiện thực cũng cần được đánh giá.

+ *Xác định hình thức thiệt hại:* ví dụ các thông tin quan trọng có thể bị sửa đổi hoặc đánh cắp bởi các cá nhân, hoặc có thể bị phá hủy do bị tấn công.

- Giai đoạn lên kế hoạch: Xác định rõ ràng đe dọa nào cần phải chống đỡ và giải pháp tương ứng cần được tiến hành, thời gian cụ thể và người chịu trách nhiệm triển khai. Đánh giá và lựa chọn các giải pháp phù hợp.

- Giai đoạn thực thi: Các công nghệ đặc thù có thể được chọn để chống đỡ với các nguy cơ dễ xảy ra nhất. Việc lựa chọn công nghệ dựa vào những định hướng đã được nêu ra ở giai đoạn Lập kế hoạch. Ngoài những công nghệ đặc thù, các phần mềm an ninh từ những nhà cung cấp khác cũng có thể được lựa chọn.

- Giai đoạn giám sát: Xác định những biện pháp nào mang lại thành công, những biện pháp nào không hiệu quả cần thay đổi, liệu có những mối đe dọa mới xuất hiện hay có những cải tiến hoặc thay đổi gì trong công nghệ, hoặc có những tài sản nào khác của doanh nghiệp cần bảo đảm an ninh.

3.1. Những biện pháp cơ bản nào đảm bảo an toàn cho giao dịch TMĐT

Biện pháp hữu hiệu nhất hiện nay trong việc đảm bảo tính xác thực là sử dụng hạ tầng khóa công khai (PKI – Public Key Infrastructure) trong đó có sử dụng các thiết bị kỹ thuật, hạ tầng và quy trình để ứng dụng việc mã hóa, chữ kỹ số và chứng chỉ số. Các kỹ thuật sử dụng trong Hạ tầng khóa công khai có thể hiểu như sau:

- Sử dụng kỹ thuật mã hoá thông tin:

Mã hoá thông tin là quá trình chuyển các văn bản hay các tài liệu gốc thành các văn bản dưới dạng mật mã bằng cách sử dụng một thuật mã hóa. Giải mã là quá trình văn bản dạng mật mã được chuyển sang văn bản gốc dựa trên mã khóa. Mục đích của kỹ thuật mã hoá nhằm đảm bảo an toàn cho các thông tin được lưu giữ và đảm bảo an toàn cho thông tin khi truyền phát.

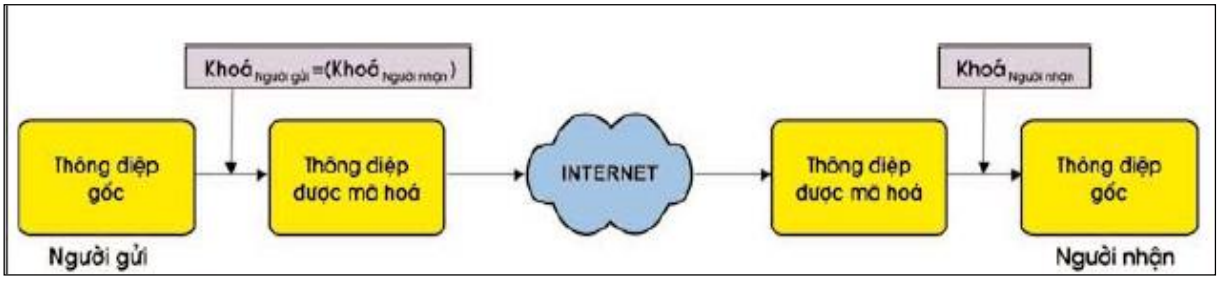
Mã hoá thông tin là một kỹ thuật được sử dụng rất sớm kể từ khi loài người bắt đầu giao tiếp với nhau và thuật mã hóa cũng phát triển từ những thuật toán rất sơ khai trước đây tới các công nghệ mã hóa phức tạp hiện nay. Một phần mềm mã hóa sẽ thực hiện hai công đoạn: thứ nhất là tạo ra một chìa khóa và thứ hai là sử dụng chìa khóa đó cùng thuật mã hóa để mã hóa văn bản hoặc giải mã.

Có hai kỹ thuật cơ bản thường được sử dụng để mã hoá thông tin là mã hoá "khoá đơn" sử dụng một "khoá bí mật" và mã hoá kép sử dụng hai khóa gồm "khoá công khai" và "khóa bí mật".

+ Kỹ thuật mã hóa đơn sử dụng một khoá khoá bí mật:

Mã hoá khoá bí mật, còn gọi là mã hoá đối xứng hay mã hoá khoá riêng, là việc sử dụng một khoá chung, giống nhau cho cả quá trình mã hoá và quá trình giải mã. Quá trình mã hoá khoá bí mật được thực hiện như minh họa trong hình 6.1.

Hình 4.1: Phương pháp mã hoá khoá riêng

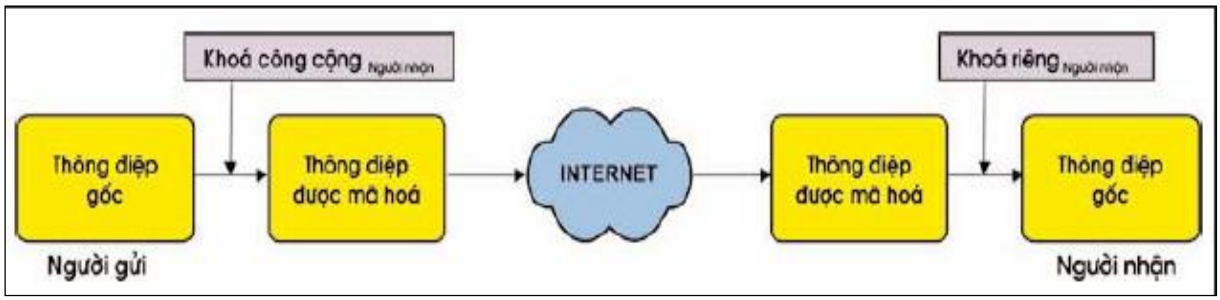


Tuy nhiên, tính bảo mật trong phương pháp mã hóa bí mật phụ thuộc rất lớn vào chìa khóa bí mật. Ngoài ra, sử dụng phương pháp mã hoá khoá bí mật, một doanh nghiệp rất khó có thể thực hiện việc phân phối an toàn các mã khoá bí mật với hàng ngàn khách hàng trực tuyến của mình trên những mạng thông tin rộng lớn. Và doanh nghiệp sẽ phải bỏ ra những chi phí không nhỏ cho việc tạo một mã khoá riêng và chuyển mã khoá đó tới một khách hàng bất kỳ trên mạng Internet khi họ có nhu cầu giao dịch với doanh nghiệp. Ví dụ, một trong các hình thức đơn giản của khóa bí mật là password để khóa và mở khóa các văn bản word, excel hay power point.

+ Kỹ thuật mã hóa kép sử dụng khoá công khai và khóa bí mật

Kỹ thuật mã hoá này sử dụng hai khoá khác nhau trong quá trình mã hoá và giải mã: một khoá dùng để mã hoá thông điệp và một khoá khác dùng để giải mã. Hai mã khoá này có quan hệ với nhau về mặt thuật toán sao cho dữ liệu được mã hoá bằng khoá này sẽ được giải mã bằng khoá kia. Khoá công cộng là phần mềm có thể công khai cho nhiều người biết, còn khoá riêng được giữ bí mật và chỉ mình chủ nhân của nó được biết và có quyền sử dụng.

Hình 4.2: Phương pháp mã hoá khoá công cộng



Như vậy, kỹ thuật mã hóa này đảm bảo tính riêng tư và bảo mật, vì chỉ có người nhận thông điệp mã hóa được gửi đến mới có thể giải mã được. Ngoài ra kỹ thuật này cũng đảm bảo tính toàn vẹn, vì một khi thông điệp mã hóa bị xâm phạm, quá trình giải mã sẽ không thực hiện được.

Trong quá trình sử dụng, có một số đặc điểm cần lưu ý đối với hai kỹ thuật mã hóa trên.

Bảng 4.1: So sánh phương pháp mã hoá khóa riêng và mã hoá khoá công cộng

Đặc điểm	Mã hoá khoá riêng	Mã hoá khoá công cộng
Số khoá	Một khoá đơn	Một cặp khoá
Loại khoá	Khoá bí mật	Một khóa bí mật và một khóa công khai
Quản lý khoá	Đơn giản, nhưng khó quản lý	Yêu cầu các chứng nhận điện tử và bên tin cậy thứ ba
Tốc độ giao dịch	Nhanh	Chậm
Sử dụng	Sử dụng để mã hoá những dữ liệu lớn (hàng loạt)	Sử dụng đối với những ứng dụng có nhu cầu mã hoá nhỏ hơn như mã hoá các tài liệu nhỏ hoặc để ký các thông điệp

- Chữ ký số (Digital signature)

Về mặt công nghệ, chữ ký số là một thông điệp dữ liệu đã được mã hóa gắn kèm theo một thông điệp dữ liệu khác nhằm xác thực người gửi thông điệp đó. Quá trình ký và xác nhận chữ ký số như sau: Người gửi muốn gửi thông điệp cho

bên khác thì sẽ dùng một phần mềm rút gọn thông điệp dữ liệu điện tử, xử lý chuyển thông điệp dữ liệu điện tử thành một "thông điệp tóm tắt" (Message Digest), thuật toán này được gọi là thuật toán rút gọn (hash function). Người gửi mã hoá bản tóm tắt thông điệp bằng khóa bí mật của mình (sử dụng phần mềm bí mật được cơ quan chứng thực cấp) để tạo thành một chữ ký điện tử. Sau đó, người gửi tiếp tục gắn kèm chữ ký điện tử này với thông điệp dữ liệu ban đầu. Sau đó gửi thông điệp đã kèm với chữ ký điện tử một cách an toàn qua mạng cho người nhận. Sau khi nhận được, người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký điện tử thành bản tóm tắt thông điệp. Người nhận cũng dùng rút gọn thông điệp dữ liệu giống hệt như người gửi đã làm đối với thông điệp nhận được để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Người nhận so sánh hai bản tóm tắt thông điệp này. Nếu chúng giống nhau tức là chữ ký điện tử đó là xác thực và thông điệp đã không bị thay đổi trên đường truyền đi.

Ngoài ra, chữ ký số có thể được gắn thêm một "nhãn" thời gian: sau một thời gian nhất định quy định bởi nhãn đó, chữ ký số gốc sẽ không còn hiệu lực, đồng thời nhãn thời gian cũng là công cụ để xác định thời điểm ký.

- Phong bì số (Digital Envelope)

Tạo lập một phong bì số là một quá trình mã hoá sử dụng khoá công khai của người nhận (phần mềm công khai của người nhận, phần mềm này cũng do cơ quan chứng thực cấp cho người nhận, và được người nhận thông báo cho các đối tác biết để sử dụng khi họ muốn gửi thông điệp cho mình). Khóa bí mật này được dùng để mã hoá toàn bộ thông tin mà người gửi muốn gửi cho người nhận, khóa này đảm bảo chỉ có duy nhất người nhận là người mở được thông điệp để đọc. Vì duy nhất người nhận là người nắm giữ khóa tương ứng để giải mã (phần mềm bí mật hay khóa bí mật, khóa này cũng do cơ quan chứng thực cấp cho người nhận).

- Chứng thư số hóa (Digital Certificate):

Nếu một bên có mã khóa công khai của bên thứ 2 để có thể tiến hành mã hóa và gửi thông điệp cho bên đó, mã khóa công khai này sẽ được lấy ở đâu và liệu bên này có thể đảm bảo định danh chính xác của bên thứ 2 không? Chứng thư điện tử xác minh rằng người cầm giữ mã khóa công cộng hoặc mã khóa bí mật

chính là người chủ của mã khóa đó. Bên thứ ba, Cơ quan chứng thực, sẽ phát hành chứng thư điện tử cho các bên tham gia. Nội dung Chứng thư điện tử bao gồm: tên, mã khoá công khai, số thứ tự của chứng thực điện tử, thời hạn hiệu lực, chữ ký của cơ quan chứng nhận (tên của cơ quan chứng nhận có thể được mã hoá bằng mã khoá riêng của cơ quan chứng nhận) và các thông tin nhận dạng khác. Các chứng thư này được sử dụng để xác minh tính chân thực của website (website certificate), của cá nhân (personal certificate) và của các công ty phần mềm (software publisher certificate).

3.2. Các biện pháp cơ bản nhằm đảm bảo an toàn cho hệ thống TMĐT

Một số công nghệ được phát triển nhằm đảm bảo rằng trong nội bộ mạng của một doanh nghiệp, các hoạt động sẽ được đảm bảo an toàn khỏi các vụ tấn công hoặc xâm phạm từ bên ngoài, đồng thời có chức năng cảnh báo các hoạt động tấn công từ bên ngoài vào hệ thống mạng.

- Tường lửa:

Tường lửa là một thành phần của mạng, gồm phần mềm hoặc phần cứng hoặc kết hợp cả phần mềm và phần cứng, cho phép những người sử dụng mạng máy tính của một tổ chức có thể truy cập tài nguyên của các mạng khác (ví dụ, mạng Internet), nhưng đồng thời ngăn cấm những người sử dụng khác, không được phép từ bên ngoài truy cập vào mạng máy tính của tổ chức. Một bức tường lửa có những đặc điểm sau:

- Tất cả các luồng thông tin từ bên trong mạng máy tính của tổ chức đi ra ngoài và ngược lại đều phải đi qua thiết bị hay phần mềm này;

- Chỉ các luồng thông tin được phép và tuân thủ đúng quy định về an toàn mạng máy tính của tổ chức, mới được phép đi qua;

Về cơ bản, tường lửa cho phép những người sử dụng mạng máy tính bên trong tường lửa được bảo vệ nhưng vẫn có khả năng truy cập toàn bộ các dịch vụ bên ngoài mạng ; đồng thời ngăn chặn và chỉ cho phép một số các truy cập từ bên ngoài vào mạng trên cơ sở đã kiểm tra tên và mật khẩu của người sử dụng, địa chỉ IP hoặc tên miền (domain name) … Ví dụ, một nhà sản xuất chỉ cho phép những người sử dụng có tên miền thuộc các công ty đối tác là khách hàng lâu năm, truy

cập vào website của họ để mua hàng. Như vậy, công việc của bức tường lửa là thiết lập một rào chắn giữa trong và ngoài mạng máy tính của tổ chức. Tường lửa bảo vệ mạng máy tính của tổ chức tránh khỏi những tổn thương do những tin tặc, những người tò mò từ bên ngoài tấn công. Tất cả mọi thông điệp được gửi đến và gửi đi đều được tường lửa kiểm tra đối chiếu với những quy định về an toàn do tổ chức xác lập. Các tường lửa phổ biến hiện nay gồm: Windows XP Personal firewall, Microsoft ISA server (đa chức năng), Checkpoint.

- Mạng riêng ảo (VPN)

Khi công ty muốn tạo ra một ứng dụng B2B, cung cấp cho các nhà cung cấp, đối tác và những đối tượng khác quyền truy cập không chỉ với dữ liệu đặt trên trang web của họ, mà còn cả quyền truy cập đối với dữ liệu chứa trong các tệp khác (như tệp Word, Excel, file đồ họa, file âm thanh, hình ảnh...). Theo cách truyền thống, liên lạc với công ty có thể thực hiện thông qua một đường truyền riêng hoặc thông qua một đường quay số tới modem hoặc tới một máy chủ truy cập từ xa (RAS – Remote Access Server) mà máy chủ này cho phép kết nối trực tiếp tới mạng LAN của công ty. Ưu điểm của việc thuê đường truyền riêng là giảm thiểu khả năng bị hacker nghe trộm các liên lạc, tuy nhiên chi phí lại cao. Do đó, doanh nghiệp có thể tham khảo một giải pháp kinh tế hơn đó là sử dụng mạng riêng ảo. Mạng riêng ảo sử dụng mạng internet để truyền tải thông tin nhưng vẫn duy trì sự bí mật bằng cách sử dụng thuật mã khóa (để mã giao dịch, xác minh tính chân thực để đảm bảo rằng thông tin không bị truy xuất trái phép và thông tin đến từ những nguồn tin cậy) và quản lý quyền truy cập để xác định danh tính của bất kỳ ai sử dụng mạng này. Hơn nữa, một mạng riêng ảo cũng có thể được sử dụng để hỗ trợ những liên lạc giữa các chi nhánh và trụ sở công ty và những liên lạc giữa các công nhân lưu động với trụ sở làm việc của họ. Số lượng các doanh nghiệp sử dụng hình thức này ngày càng tăng, điều này thể hiện ở doanh số của thị trường dịch vụ mạng riêng ảo toàn thế giới, năm 2005 đã đạt mức 23 tỷ USD vào năm 2005 và hứa hẹn sẽ tăng thêm 22% trong vòng 3 năm tới.

3.3. Một số biện pháp khác nhằm đảm bảo an toàn cho hệ thống TMĐT

- Sử dụng password đủ mạnh

Để đảm bảo bí mật cho mật khẩu, khi thiết lập nên xem xét các tiêu chí như:

+ Mật khẩu có số ký tự đủ lớn, tối thiểu 8 ký tự và có sự kết hợp giữa chữ hoa, chữ thường, chữ số và biểu tượng. Như vậy sẽ mất rất nhiều thời gian mới có thể tìm ra và phá mật khẩu, mà tới thời gian đó mật khẩu đã có thể đã được thay đổi. Mật khẩu cũng nên thường xuyên thay đổi (thường từ 30-60 ngày) và không nên sử dụng lại mật khẩu cũ.

+ Kích hoạt tự động việc khóa không cho truy cập hệ thống nếu sau từ 3-5 lần nhập mật khẩu vẫn không đúng.

+ Không sử dụng chức năng tự động điền (auto complete) của một số phần mềm ứng dụng như Microsoft Explorer để lưu mật khẩu và số tài khoản

- Phòng chống virus

Theo thống kê, trung bình mỗi tháng có hơn 500 virus ra đời, do đó doanh nghiệp nên sử dụng các phần mềm chống virus để kiểm tra tất cả các dữ liệu hoặc được truyền qua cổng máy chủ ở mạng hoặc truyền giữa các cổng nội bộ. Các phần mềm chống virus cũng nên được cập nhật thường xuyên (hàng ngày, hàng tuần). Thông thường, các công ty phần mềm virus uy tín thường gửi email tới khách hàng thông báo về việc xuất hiện những virus mới và cung cấp công cụ update tự động cho khách hàng.

Định dạng cổng email để khóa các tệp có đuôi dạng VBS, SHS, EXE, SCR, CHM và BAT hoặc những tệp có hai phần mở rộng dạng như .txt.vbs hoặc .jpg.vbs vì những tệp dạng này thường do virus tạo ra.

Phổ biến kiến thức cho người sử dụng, ví dụ, không mở những email lạ có tệp đính kèm, thậm chí từ người gửi có tên trong sổ địa chỉ; không tải về những tệp từ những nguồn không rõ ràng; thường xuyên quét virus; cập nhật phần mềm quét virus thường xuyên; không gửi những cảnh báo về virus hoặc các thư dây chuyền cho những người sử dụng khác.

- Giải pháp an ninh nguồn nhân lực

Các doanh nghiệp cần lưu ý mọi nhân viên trong doanh nghiệp mình ý thức về vấn đề an ninh mạng và những nguy cơ tấn công doanh nghiệp có thể chịu trong trường hợp thiếu kinh nghiệm hoặc thiếu sự lưu tâm đúng mức từ phía các

nhân viên. Nhân viên cũng cần được lưu ý về các giải pháp an toàn mạng nên áp dụng như việc chọn mật khẩu, thay đổi mật khẩu, quét virus thường xuyên hay xóa bỏ những email lạ.

- Giải pháp về trang thiết bị an ninh mạng

Sử dụng các thiết bị kiểm soát việc ra vào trụ sở làm việc như : các thẻ từ, mã điện tử, thẻ thông minh hoặc các thiết bị nhận dạng nhân trắc như kiểm tra vân tay, võng mạc hoặc giọng nói. Các biện pháp khác có thể là sao lưu dữ liệu vào những nơi an toàn, đánh dấu nhận dạng tia cực tím, các hệ thống phát hiện xâm phạm như camera và chuông báo động.

4. Bài tập tình huống

4.1. Đối phó với các vụ tấn công vào website thương mại điện tử

Vụ tấn công vào Chodientu.com

Ngày 19/9/2006. công ty Giải pháp phần mềm Hòa Bình chính thức (Peacesoft) chính thức thừa nhận tên miền www.chodientu.com bị tấn công, mất quyền kiểm soát và phải chuyển sang dùng tên miền mới là www.chodientu.vn. Theo giải thích của ban giám đốc, hacker tấn công vào máy chủ quản lý tên miền của www.register.com và lấy quyền kiểm soát tên miền www.chodientu.com tại đó.

Ngày 23/9/2006, www.chodientu.com tiếp tục bị chiếm quyền kiểm soát và trỏ sang một trang web với nội dung bôi nhọ giám đốc công ty.

Ngày 27/9/2006, đại diện Chợ điện tử đã chính thức làm việc với Trung tâm An ninh mạng (BKIS) và các cơ quan chức năng để nhanh chóng truy tìm thủ phạm. Tuy nhiên, với hình thức tấn công vào tên miền, thủ phạm sẽ khó có thể bị phát hiện do cơ chế tấn công không liên tục như tấn công từ chối dịch vụ (DOS).

Virus lây lan qua YM, "Tháng 9 kinh hoàng", hơn 20.000 máy tính bị nhiễm và đã phải cầu cứu đến BKAV khi người sử dụng tò mò kích vào những đường link "mời mọc" hay "kích động" được gửi đến thông qua YM.

4.2. Phòng chống lừa đảo qua mạng (phishing)

Vấn đề

Ngày 17 tháng 11 năm 2003, một số khách hàng của eBay được thông báo bằng email rằng tài khoản của họ trên eBay đang được cập nhật và tăng cường mức độ an toàn. Thông báo cũng kèm theo một đường link đến một trang web của eBay tại đó khách hàng có thể đăng ký để chấp nhận các dịch vụ này. Tất cả các thông tin khách hàng cần cung cấp để nhận được dịch vụ này là cung cấp số thẻ tín dụng, số bảo hiểm xã hội, ngày sinh, tên bí mật, số pin thẻ ATM. Vấn đề duy nhất là thực tế eBay chưa từng bao giờ gửi đi các thông điệp như thế này cả và trang web mà khách hàng được link tới cũng không thuộc sự quản lý của eBay. Mặc dù trang web giả trông rất giống trang web thực của eBay, cũng có logo của eBay, giao diện tương tự, trang web này thực chất được tạo ra với mục đích lừa đảo. Những khách hàng "ngây thơ" điền thông tin được yêu cầu vào trang web này đã ngay lập tức trở thành nạn nhân của vụ lừa đảo trên mạng được biết đến với thuật ngữ "phishing". Phishing là kỹ thuật lừa đảo sử dụng thư điện tử, pop-up, trang web để dụ dỗ người dùng cung cấp các thông tin nhạy cảm như thẻ tín dụng, tài khoản ngân hàng, mật khẩu…

Giải pháp

Bản chất kỹ thuật lừa đảo này không mới, tuy nhiên "công nghệ" được sử dụng lại mới và có nhiều người sử dụng bị mắc bẫy. Trước đây, công nghệ được ưa chuộng cho kiểu lừa này là điện thoại. Ngày nay, những kẻ chủ mưu sử dụng thư điện tử, thông điệp pop-up, trang web giả để người sử dụng tưởng lầm họ đang giao dịch với các doanh nghiệp chính thức. Các thông điệp này thường dẫn dắt người sử dụng đến một website khác, tại đó, người sử dụng sẽ được yêu cầu cung cấp hoặc cập nhật thông tin mới cho tài khoản của họ. Mặc dù các website này trông hoàn toàn giống như website thật, đó là website giả mạo. Tổ chức phòng chống kiểu lừa đảo này có tên gọi Anti-Phishing Working Group (APWG, antiphishing.org). Tháng 7 năm 2004, số vụ lừa đảo kiểu này được thông báo đến APWG lên đến 1.974 vụ, tăng 39% so với tháng 6 cùng năm. Ngành chịu tấn công nhiều nhất là dịch vụ tài chính (1.649 trong tổng số 1.974 vụ tấn công). Thương

hiệu bị tấn công nhiều nhất là Citibank, U.S. Bank, eBay và PayPal (1.191 trong tổng số 1.974). Những website giả mạo được lưu trữ nhiều nhất tại Hoa Kỳ (35%) tiếp đến là Hàn Quốc, Trung Quốc và Nga. Để tránh bị điều tra, các website giả mạo thường hoạt động trong một thời gian ngắn, trung bình khoảng 6 ngày.

Các công ty chuyên về an ninh trên mạng như VeriSign (verisign.com) và Name Protect (nameprotect.com) đang phối hợp triển khai để ngăn chặn hình thức tấn công này. Cả hai công ty này đều chủ động nghiên cứu các website (tên miền, tên máy chủ, các trang, nhóm tin tức, chatroom…) để phát hiện các dấu hiệu phishing. Những dịch vụ này được các công ty như MasterCard, các công ty bán lẻ và tổ chức tài chính hỗ trợ. Khi phát hiện các dấu hiệu lừa đảo, những thông tin này được chuyển đến các tổ chức hỗ trợ và các cơ quan quản lý liên quan. Tuy nhiên, các dịch vụ này không được thông báo trực tiếp đến các khách hàng dù là tổ chức hay cá nhân. Do đó, khách hàng vẫn cần chủ động phòng tránh những vụ lừa đảo kiểu này. Ủy ban Thương mại Liên bang (FDC-Federal Trade Commision) khuyến cáo:

- Tránh trả lời các thư điện tử hay thông điệp pop-up yêu cầu cung cấp thông tin cá nhân
- Tránh gửi các thông tin cá nhân hay tài chính dưới bất kỳ hình thức nào
- Kiểm tra kỹ các thông tin tài khoản và chi tiết mua sắm thẻ tín dụng hàng tháng
- Sử dụng và cập nhật các phần mềm diệt virus thường xuyên
- Cẩn trọng khi mở bất kỳ thông điệp dữ liệu gắn kèm theo thư điện tử
- Gửi các thông báo đến FTC về các thông điệp bị nghi ngờ

Kết quả

Theo điều tra của Tổ chức Chống lừa đảo qua mạng (APWG), ước tính khoảng 5% người sử dụng mắc phải bẫy phishing. Tổng thiệt hại không được thống kê chi tiết, tuy nhiên đến nay vẫn chưa có quy định cụ thể xử lý các kẻ chủ mưu của những vụ lừa đảo dạng phishing.

Bài học kinh nghiệm

Các mô hình thương mại điện tử đều có điểm chung là nhiều bên tham gia, sử dụng nhiều mạng khác nhau, nhiều ứng dụng và nhiều cơ sở dữ liệu… do đó đảm bảo an toàn trong thương mại điện tử rất khó khăn. Kẻ tấn công chỉ cần phát hiện ra một điểm yếu trong toàn bộ hệ thống là có khả năng thành công. Một số vụ tấn công đòi hỏi công nghệ và kỹ năng cao. Tuy nhiên, hầu hết các vụ tấn công như phishing chỉ cần sử dụng những công nghệ rất đơn giản để đánh vào điểm yếu của con người và các tập quán an ninh mạng mới đang hình thành. Do đa số các vụ tấn công không tinh vi và phức tạp, những quy định rõ ràng về phòng tránh rủi ro trong thương mại điện tử sẽ giúp giảm thiểu đáng kể nguy cơ và thiệt hại.

4.3. Giải pháp giảm rủi ro trong thương mại điện tử của iPremier

Giới thiệu về iPremier

Do hai sinh viên từ trường UFT đã có nhiều thành công lớn trong thương mại điện tử thành lập năm 1994 với tên gọi iPremier. Đến nay công ty đã là một trong hai nhà bán lẻ hàng đầu về những mặt hàng sang trọng, quý hiếm trên mạng. Công ty có trụ sở tại Seattle, Washington. Công ty có tốc độ tăng trưởng rất nhanh khoảng 50% mỗi năm, đến năm 1999, lợi nhuận đạt 2.1 triệu USD trên doanh số 32 triệu USD.

Từ khi cổ phần hoá năm 1998, giá cổ phiếu tăng gần ba lần. Sau cuộc khủng hoảng năm 2000, iPremier là một trọng số rất ít các công ty thương mại điện tử B2C sống sót và tiếp tục phát triển. Trong con mắt các nhà phân tích, đây là một mô hình thành công điển hình trong kinh doanh thương mại điện tử.

Hầu hết các mặt hàng công ty kinh doanh có giá từ 50 đến vài trăm USD, tuy nhiên một số có giá hàng nghìn USD. Công ty áp dụng chính sách trả lại hàng rất linh hoạt theo đó cho phép khách hàng kiểm tra kỹ lưỡng hàng hoá trước khi quyết định có nên mua hay không. Khách hàng của công ty thường có thu nhập rất cao và vì thế vấn đề về giới hạn tín dụng dường như chưa bao giờ gặp phải cho dù đối với những mặt hàng có giá trị rất cao.

Cơ cấu tổ chức kỹ thuật

Công ty thuê ngoài các dịch vụ Internet từ một nhà cung cấp nhiều kinh nghiệm là Qdata. Qdata cung cấp dịch vụ về máy chủ, đường truyền internet, các

dịch vụ quản lý như theo dõi website cho các khách hàng thông quan Network Operations Center (NOC) và một số dịch vụ bảo mật khác. Tuy nhiên, Qdata chậm trong việc đầu tư vào các hệ thống máy chủ mới nhất cũng như nâng cao chất lượng đội ngũ nhân viên.

iPremier đã có kế hoạch chuyển sang nhà cung cấp dịch vụ khác nhưng có một số lý do khiến việc chuyển đổi bị trễ lại. Thứ nhất, tốc độ tăng trưởng nhanh khiến công ty luôn bận rộn và việc chuyển đổi không được coi là ưu tiên số một. Thứ hai, chi phí cho một hệ thống hiện đại hơn luôn có chi phí cao gấp hai đến ba lần hệ thống hiện tại. Thứ ba, việc chuyển đổi hệ thống có thể gây gián đoạn công việc kinh doanh, đặc biệt ảnh hưởng đến các khách hàng qua mạng. Hơn nữa, kế hoạch triển khai lắp đặt mới tại nhà cung cấp khác cũng chưa bao giờ được bàn cụ thể. Lý do cuối cùng là một thành viên trong ban lãnh đạo iPremier có quan hệ cá nhân mật thiết với Qdata vì vậy Qdata sẵn sàng thương lượng lại hợp đồng trong thời gian tới.

Cuộc tấn công vào iPremier

- 4:31 sáng, ngày 12 tháng 1 năm 2001

Giám đốc của iPremier được một nhân viên trong công ty thông báo về việc website của công ty đã bị tấn công. Website công ty đã bị khoá. Nhân viên công ty đã thử ba phần mềm duyệt web nhưng không thể mở nó ra được. Khách hàng của công ty cũng không thể mở được. Dịch vụ hỗ trợ khách hàng đang ngập tràn trong điện thoại và mỗi giây công ty lại nhận được một e-mail với nội dung chỉ có từ " Ha". Các e-mail liên tiếp tạo thành Ha ha ha...Hầu hết các email bắt nguồn từ Châu Á và Châu Âu. Chính vì vậy để lần ra ai là người đã tiến hành tấn công vào website của công ty sẽ phải mất rất nhiều thời gian. Theo nhận định của nhân viên công ty có thể mất khoảng 18 tháng mới tìm ra người khởi tạo email. Nếu email được gửi từ một nơi công cộng thì thời gian để tìm ra sẽ còn lâu hơn nữa.

Ngay sau khi vụ tấn công diễn ra nhân viên kỹ thuật của công ty đã kết hợp với Qdata để tìm ra lý do sinh sôi các email này. Cuối cùng họ phát hiện ra rằng kẻ chủ mưu vụ tấn công đã sử dụng virus zombies có tên " Bình minh của cái chết" để tấn công vào hệ thống cơ sở dữ liệu của công ty. Mỗi lần công ty cố

shutdown một IP truy cập vào thì mấy con virus sẽ tự động khởi động tấn công từ hai IP khác. Tuy nhiên vụ tấn công bằng virus này vẫn còn non chưa thể vượt qua bức tường lửa do hệ thống kỹ thuật xây lên; chính vì vậy cuộc tấn công nhanh chóng chấm dứt vào lúc 5:46 sáng. Kẻ tấn công vẫn chưa hack được vào trong hệ thống của công ty.

Câu hỏi ôn tập

1. Hãy cho biết một số rủi ro thường gặp trong thương mại điện tử
2. Hãy cho biệt một số vấn đề về an ninh mà các doanh nghiệp gặp phải khi tiến hành hoạt động thương mại điện tử.
3. Phishing là gì? Hãy cho biết một vài ví dụ về phishing trên thế giới và tại Việt Nam
4. DDoS là gì? Hãy cho biết một vài ví dụ về DDoS trên thế giới và tại Việt Nam trong một vài năm gần đây.
5. Hãy cho biết một số biện pháp doanh nghiệp thường tiến hành để đảm bảo an toàn cho các giao dịch thương mại điện tử.

Thuật ngữ

Nội dung động (active content) : những chương trình được gắn liền vào các trang web và sẽ hoạt động tùy theo hành vi tác động từ người sử dụng.

Tiêu chuẩn mã hóa cấp cao (advanced encryption standard): Tiểu chuẩn mã hóa mới thường được sử dụng để bảo mật các thông tin của chính phủ sử dụng thuật toán mã hóa của Rijndael. Thuật toán này được Viện tiêu chuẩn và công nghệ quốc gia (NITS) giới thiệu năm 2001.

Phần mềm chống virus (antivirus software): những phần mềm giúp phát hiện virus và sâu sau đó có thể xóa hoặc tách những phần mềm nguy hại này khỏi các dữ liệu khác để chúng không thể hoạt động gây hại được.

Mã hóa không đối xứng (asymmetric encryption): đồng nghĩa với mã hóa công khai, đây là công nghệ mã hóa các thông điệp dữ liệu, sử dụng hai khóa riêng biệt nhưng có quan hệ một một với nhau.

Cửa hậu (back door): những lỗ hổng trên các phần mềm thương mại điện tử được tạo ra vô tình hay cố ý.

Thiết bị an ninh sinh học (biometric security device): một thiết bị an ninh sử dụng các đặc điểm sinh học của con người để xác thực. Các thiết bị này có thể là máy kiểm tra chữ ký, máy quét võng mạc, máy đọc vân tay, đọc chi tiết bàn tay...

Bộ đệm (buffer): một phần của bộ nhớ máy tính được dành riêng lưu trữ các dữ liệu do máy tính đọc từ các file hay cơ sở dữ liệu.

Cơ quan chứng thực (CA-certificate authority): một công ty hay tổ chức cung cấp chữ ký điện tử và chứng thực điện tử cho các tổ chức và cá nhân

Mã hóa (Cryptography): công nghệ để giấu các thông tin để chỉ những người được phép mới có thể đọc được.

Chương trình giải mã (Decrypted program): một phần mềm giúp đảo ngược quá trình mã hóa, kết quả là khôi phục lại thông điệp ban đầu từ thông điệp đã được mã hóa.

Chứng chỉ số (Digital certificate): phần gắn kèm theo một thông điệp dữ liệu hoặc tích hợp trong trang web để xác thực người gửi hay website.

Chữ ký số (Digital signature): thông điệp điện tử được tạo ra nhờ việc sử dụng phần mềm ký điện tử mã hóa phần rút gọn của các văn bản điện tử.

Máy chủ quản lý tên miền (Domain name server): một máy tính trên Internet lưu trữ các danh bạ cho phép liên kết tên miền với các địa chỉ IP.

Thuật toán mã hóa (Encryption algorithm): logic cho phép tiến hành các chương trình mã hóa.

Chương trình mã hóa (Encryption program): chương trình cho phép chuyển các văn bản sang dạng mã hóa.

Tường lửa (firewall): Một máy tính cung cấp hàng rào bảo vệ giữa mạng bên trong tường lửa với các mạng bên ngoài tường lửa để tránh các rủi ro, nguy cơ cho mạng bên trong. Tất cả các luồng thông tin đến và đi từ mạng bên trong đều phải chạy qua tường lửa. Chỉ những luồng thông tin được phép theo quy định được đặt ra cho tường lửa mới được truyền qua.

Thuật toán "băm"/thuật toán rút gọn (hash function): một thuật toán cho phép phối hợp tất cả các ký tự trong một văn bản để tạo ra một con số với độ dài cố định (thường là 128 bit) được coi là bản rút gọn đại diện cho văn bản gốc, bản rút gọn này quan hệ một một với bản gốc, tương tự như vai trò của vân tay với người có vân tay đó.

Virus macro (macro virus): virus được truyền tải hay giấu trong các file đính kèm, có thể làm hỏng các chương trình khác trên máy tính hoặc làm lộ các thông tin bí mật.

Bom thư (mail bomb): hành động tấn công bằng cách gửi hàng loạt thư điện tử đến một địa chỉ cụ thể, vượt quá khả năng tiếp nhận của địa chỉ đó làm địa chỉ đó hoặc toàn bộ hệ thống ngừng hoạt động.

Lừa đảo qua mạng (phishing): gửi hàng loạt thư điện tử giả danh từ một địa chỉ đáng tin cậy đến các khách hàng của địa chỉ đó. Thư điện tử có đường link đến một trang web có giao diện giống hệt giao diện của công ty có uy tín. Nạn nhân được đề nghị nhập vào tên, mã bí mật, thông tin thẻ tín dụng để được cập nhật và ngay lập tức những thông tin này bị đánh cắp.

Khóa bí mật (private key): là một phần mềm giúp mã hóa và giải mã các thông điệp, chủ sở hữu giữ bí mật để sử dụng xác thực vào các thông điệp dữ liệu họ gửi qua mạng.

Khóa công khai (public key): là khóa có quan hệ một một với khóa bí mật, được dùng để mã hóa và giải mã các thông điệp đã được mã hóa bằng khóa bí mật, khóa này được công bố cho mọi người liên quan biết để sử dụng nhằm xác thực thông điệp có được gửi bởi người nắm giữ khóa bí mật hay không.

Lớp khóa an toàn (Secure socket layer): một giao thức cho phép truyền tải thông tin trên mạng an toàn

Mã hóa đối xứng (Symmetric encryption): công nghệ mã hóa sử dụng một khóa trong cả hai quá trình mã hóa và giải mã.

Tiêu chuẩn mã hóa dữ liệu 3 (Triple DES, 3 DES – triple data encryption standard) : một tiêu chuẩn mã hóa do chính phủ Mỹ xây dựng và các máy tính mạnh nhất hiện nay vẫn chưa thể phá mã được.

Con ngựa thành trojan (Trojan horse) : một chương trình nấp bên trong một chương trình khác hay một trang web khác để che giấu các hành vi của nó, thường là mang tính phá hoạt.

Sâu (worm) : một dạng virus tự nhân bản.

Zombie : một dạng virus chiếm quyền kiểm soát các máy tính với mục đích tấn công một máy tính nhất định. Tấn công theo kiểu này thường rất khó truy tìm người chủ m