**E-Commerce Security and Fraud Issues and Protections**

**Mục lục**

Tình huống mở đầu: Bệnh viện tim Kansas trở thành nạn nhân bị đòi tiền chuộc

11.1 Vấn đề về bảo mật thông tin

11.2 Tổng quan và các vấn đề bảo mật cơ bản trong thương mại điện tử

11.3 Các phương pháp tấn công kỹ thuật bằng phần mềm độc hại: Từ virus đến từ chối dịch vụ

11.4 Các phương pháp phi kỹ thuật: Từ tấn công giả mạo đến thư rác và lừa đảo

11.5 Mô hình đảm bảo thông tin và chiến lược phòng chống

11.6 Các hệ thống bảo vệ thông tin và thương mại điện tử

11.7 Bảo vệ người tiêu dung và người bán khỏi gian lận trực tuyến

11.8 Triển khai bảo mật thương mại điện tử toàn doanh nghiệp

Các vấn đề về quản lý

Tình huống kết thúc: Dyn bị tấn công theo hình thức DDOS như thế nào?

Tham khảo

**Mục tiêu**

Sau khi hoàn thành chương này, bạn có thể:

1. Hiểu được tầm quan trọng về việc bảo mật các hệ thống thông tin trong thương mại điện tử.
2. Mô tả được các khái niệm và thuật ngữ chính trong bảo mật thương mại điện tử.
3. Hiểu về các mối đe dọa an ninh chính của EC, các lỗ hổng bảo mật và các phương pháp tấn công kỹ thuật.
4. Hiểu được gian lận, lừa đảo và thư rác trên Internet.
5. Mô tả được các nguyên tắc bảo mật trong bảo vệ thông tin.
6. Mô tả các công nghệ chính để bảo vệ mạng lưới thương mại điện tử, bao gồm kiểm soát truy cập.
7. Mô tả nhiều loại hình kiểm soát và các cơ chế bảo vệ đặc biệt.
8. Mô tả bảo vệ người tiêu dùng và người bán khỏi gian lận.
9. Thảo luận về các vấn đề triển khai bảo mật thương mại điện tử trên toàn doanh nghiệp.
10. Hiểu được tại sao rất khó để có thể ngăn chặn các tội phạm máy tính.
11. Thảo luận về tương lai của thương mại điện tử.

**Tình huống mở đầu: Bệnh viện tim Kansas trở thành nạn nhân bị đòi tiền chuộc**

Bệnh viện tim Kansas thuộc Wichita, Kansas, cung cấp dịch vụ chăm sóc tim mạch toàn diện chuyên biệt cho cư dân Kansas tại bệnh viện và các dịch vụ lâm sàng. Bệnh viện được biết đến với các dịch vụ phẫu thuật chất lượng nên rất được tôn trọng, ngoại trừ những kẻ tấn công chuộc lợi.

**Sự cố**

Vào tháng 5 năm 2016, bệnh viện trở thành nạn nhân của các cuộc tấn công đòi tiền chuộc. Tin tặc yêu cầu một khoản tiền chuộc để tiết lộ những dữ liệu đã bị khóa sau khi chúng xâm nhập vào máy tính của bệnh viện (có thể từ bên ngoài Hoa Kỳ). Trong phần các phương pháp phi kỹ thuật 11.4, chúng ta sẽ đi sâu hơn và giải thích về vấn đề này.

Nói tóm lại, tin tặc đã khóa các tệp dữ liệu, từ chối cấp lại quyền truy cập trừ khi bệnh viện trả tiền chuộc bằng Bitcoin, để tránh bị theo dõi.

Bệnh viện thường là đích nhắm của các cuộc tấn công vì họ có dữ liệu nhạy cảm của bệnh nhân. Nếu tin tặc thành công, bệnh viện thường sẽ phải trả một khoản tiền chuộc.

(Năm 2016, Trung tâm Y tế Trưởng lão Hollywood ở Los Angeles, California, đã trả 17.000 đô la sau một cuộc đàm phán dài. Trong quá trình đàm phán, gần 1000 bệnh nhân đã phải gửi đến các bệnh viện gần đó.)

Vụ tấn công ở Kansas xảy ra lúc 9 giờ tối và trong vài phút, nhân viên bệnh viện đã mất quyền truy cập vào các tệp. Chỉ trong một thời gian ngắn, tấn công đã lan ra khắp bệnh viện.

Bệnh viện đã thương lượng và trả tiền chuộc nhưng tin tặc chỉ cung cấp quyền truy cập cho một số tệp, không phải tất cả, và chúng yêu cầu tiền chuộc nhiều hơn.

**Giải pháp**

Bệnh viện ngay lập tức kích hoạt một hệ thống bảo vệ có sẵn. Các tin tặc mã hóa dữ liệu trong tệp, kế hoạch đã sẵn sàng cho việc này và hệ thống bảo vệ có thể giảm thiểu thiệt hại mà tác nhân phần mềm độc hại được mã hóa gây ra.

**Kết quả**

Theo phía bệnh viên, không có thông tin bệnh nhân nào bị nguy hại. Vụ việc đã giúp bệnh viện cải thiện hệ thống bảo mật của mình tốt hơn.

**Bài học rút ra**

Các cuộc tấn công của tin tặc đang trở nên sáng tạo và tinh vi hơn rất nhiều. Gần đây, nhu cầu đòi tiền chuộc mọc lên như nấm và bệnh viện là mục tiêu chính của chúng. Tuy nhiên, quản trị viên của bệnh viện nhận thức được nguy cơ này và đã tìm cách để cố gắng bảo vệ thông tin của bệnh nhân. Tiền chuộc (ransomware) chỉ là một phương thức tấn công của hệ thống thông tin. Bên cạnh đó còn rất nhiều phương pháp khác được sử dụng. Nó tạo ra một cuộc chiến không hồi kết giữa những kẻ tấn công và những người bảo vệ. Một lĩnh vực đang phát triển liên quan chặt chẽ đến thương mại điện tử là gian lận. Chương này cung cấp tổng quan về bảo mật hệ thống thông tin, đặc biệt chú ý đến các chủ đề liên quan đến thương mại điện tử.

**11.1 Vấn đề về bảo mật thông tin**

Bảo mật thông tin, hay bảo mật hệ thống thông tin, đề cập đến nhiều hoạt động và phương pháp bảo vệ hệ thống thông tin, dữ liệu và quy trình khỏi mọi hành động được thiết kế để phá hủy, sửa đổi hoặc làm tổn hại hệ thống và hoạt động của chúng. Trong chương này, chúng tôi cung cấp tổng quan về một số vấn đề và giải pháp bảo mật thông tin chung vì chúng có liên quan đến thương mại điện tử. Trong phần này, chúng ta xem xét bản chất, mức độ của các vấn đề bảo mật và giới thiệu một số thuật ngữ thiết yếu của bảo mật thông tin.

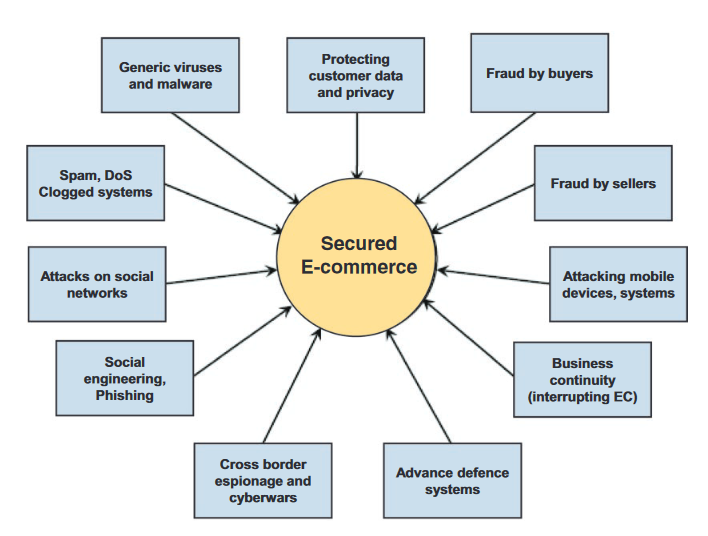
**Bảo mật thương mại điện tử là gì?**

Bảo mật máy tính nói chung đề cập đến các rủi ro và bảo vệ dữ liệu, mạng, chương trình máy tính cùng các thành phần khác của hệ thống thông tin máy tính. Đó là một lĩnh vực rất rộng do có nhiều phương thức tấn công cũng như nhiều phương thức để bảo vệ. Các cuộc tấn công và phòng thủ cho máy tính có thể ảnh hưởng đến các cá nhân, tổ chức, quốc gia hoặc toàn bộ Web. Bảo mật máy tính nhằm mục đích ngăn chặn, phục hồi hoặc ít nhất là giảm thiểu các cuộc tấn công. Bảo mật thông tin luôn được xếp hạng là một trong những mối quan tâm hàng đầu ở Hoa Kỳ và nhiều quốc gia khác. Hình 11.1 minh họa các chủ đề chính được trích dẫn trong các nghiên cứu khác nhau, được coi là quan trọng nhất trong bảo mật thông tin.

**Tình trạng bảo mật máy tính ở Hoa Kỳ**

Một số tổ chức tư nhân và chính phủ cố gắng đánh giá tình trạng bảo mật máy tính ở Hoa Kỳ một cách thường niên. Đáng chú ý là báo cáo CSI hàng năm, được mô tả trong mục tiếp theo.

Các khảo sát bảo mật toàn diện hàng năm được IBM, Symantec và các tổ chức khác công bố định kỳ. Ngoài các vấn đề bảo mật của tổ chức, còn có vấn đề về bảo mật cá nhân.



Hình 11.1 Các mối quan tâm chính về quản lý bảo mật thương mại điện tử

**Bảo mật cá nhân**

Gian lận (fraud) trên Web chủ yếu nhắm vào các cá nhân. Ngoài ra, bảo mật lỏng lẻo có thể dẫn đến nguy hiểm đối với sự an toàn cá nhân do những tội phạm tình dục tìm thấy nạn nhân của họ trên Internet.

**An ninh quốc gia**

Vấn đề bảo vệ mạng lưới máy tính của Hoa Kỳ được Bộ An ninh Nội địa (Department of Homeland Security) xử lý. Nó bao gồm các chương trình sau:

* **Cyber Security Preparedness and the National Cyber Alert.** Người sử dụng máy tính có thể cập nhật các mối đe dọa trên mạng thông qua chương trình này.
* **United States Computer Emergency Readiness Team (US-CERT Operations).** Cung cấp thông tin về các lỗ hổng và mối đe dọa bảo mật, chủ động quản lý rủi ro không gian mạng cho quốc gia và vận hành cơ sở dữ liệu để cung cấp các mô tả kỹ thuật về các lỗ hổng.
* **National Cyber Response Coordination Group (NCRCG).** Bao gồm các đại diện từ 13 cơ quan liên bang, họ xem xét các đánh giá mối đe dọa và khuyến nghị các hành động đối phó với sự cố, bao gồm phân bổ các nguồn lực liên bang.
* **CyberCop Portal.** Một cổng thông tin được thiết kế cho các quan chức chính phủ và người thực thi pháp luật sử dụng Internet để cộng tác và chia sẻ thông tin nhạy cảm với nhau trong một môi trường an toàn.

Tin tặc đang ngày càng tấn công các cơ sở hạ tầng quan trọng nhất của Hoa Kỳ (ví dụ: các cơ sở năng lượng, hạt nhân và nước). Chúng thậm chí đã cố gắng gây ảnh hưởng đến cuộc bầu cử tổng thống Mỹ.

Vào ngày 17 tháng 2 năm 2013, Tổng thống Obama đã ban hành một mệnh lệnh hành pháp đối với các cuộc tấn công mạng. Lệnh này đã cho các cơ quan liên bang có thẩm quyền lớn hơn để chia sẻ thông tin một cách công khai về “các mối đe dọa trên mạng”.

**Các rủi ro bảo mật năm 2017 và 2018**

Những rủi ro bảo mật chính trong tương lai gần là:

* Gián điệp mạng và các cuộc chiến tranh mạng, bao gồm các cuộc tấn công khủng bố, đang là mối đe dọa ngày càng tang.
* Các cuộc tấn công hiện cũng đang nhắm tới các thiết bị di động như điện thoại thông minh, máy tính bảng…
* Tấn công đòi tiền chuộc hiện đang phát triển rất nhanh.
* Tấn công trên các mạng xã hội và các công cụ phần mềm xã hội đang phát triển. Nội dung do người dùng tạo là một nguồn chính các mã độc.
* Các cuộc tấn công vào BYOD (“bring your own device”) và DOYA (“develop your own applications”) đang tăng lên.
* Trộm cắp danh tính đang bùng nổ, dẫn đến những hậu quả hình sự đối với những danh tính bị đánh cắp.
* Động cơ lợi nhuận - miễn là tội phạm mạng có thể kiếm tiền, các mối đe dọa bảo mật và các cuộc tấn công lừa đảo sẽ tiếp tục phát triển.
* Các công cụ kỹ thuật xã hội (social engineering tools) như lừa đảo qua tin nhắn, e-mail và nội dung web đang phát triển nhanh chóng.
* Sự hợp nhất của các bang nhóm tội phạm mạng đang nhân lên và ngày càng lớn hơn, đặc biệt là trong các cuộc chiến tranh mạng và lừa đảo trên Internet.
* Thư rác hướng kinh doanh (bao gồm cả thư rác dựa trên hình ảnh) đang gia tăng.
* Những kẻ tấn công đang sử dụng các công cụ phần mềm gián điệp tinh vi hơn.
* Tấn công vào các công nghệ mới như điện toán đám mây, IoT và ảo hóa đang phát triển.
* Tấn công vào các ứng dụng di động ngày càng phát triển nhanh chóng.
* Tin tức về sản phẩm và dịch vụ giả mọc lên như nấm.

Chúng ta sẽ xem xét tất cả các chủ đề chính trong danh sách trên trong phần còn lại của chương này. Các cuộc tấn công lớn vào các tập đoàn nhắm vào dữ liệu cá nhân của khách hàng hoặc nhân viên, các chiến lược và kế hoạch của công ty và các hoạt động kinh doanh có liên quan khác. Trong khi hầu hết các cuộc tấn công đều nhắm vào các doanh nghiệp lớn thì bên cạnh đó tin tặc cũng tấn công các doanh nghiệp vừa và nhỏ. Ngoài ra, 93% các công ty bị ảnh nằm trong các lĩnh vực như chăm sóc sức khỏe, bán lẻ, ngân hàng hay công nghệ thông tin.

**Rủi ro bảo mật trong các thiết bị di động**

Mối quan tâm bảo mật chính của thiết bị di động là mất các thiết bị bao gồm thông tin nhạy cảm, rò rỉ dữ liệu, thiết bị di động bị nhiễm phần mềm độc hại, đánh cắp dữ liệu từ thiết bị, người dùng tải xuống ứng dụng độc hại, đánh cắp danh tính và mất các thông tin cá nhân khác. Để biết thêm rủi ro bảo mật các thiết bị di động, đọc thêm bài viết tại đây (https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store#.WKsaeG\_yvIU). Ngay cả chiếc điện thoại thông minh cũ được Tổng thống Trump sử dụng để tweet cũng có thể là một mở đầu cho các mối đe dọa về bảo mật.

**Chiến tranh và gián điệp mạng trên khắp biên giới**