**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.

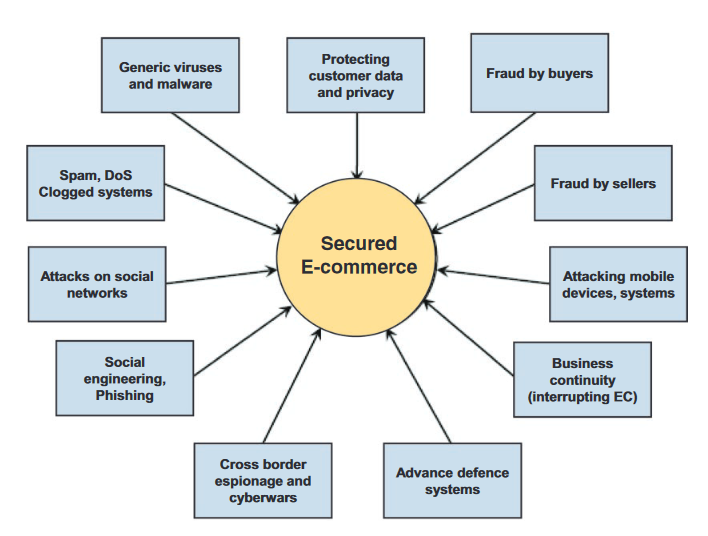
**Bảo mật thương mại điện tử là gì?**

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 hoạt động gián điệp mạng trên khắp biên giới**

Sử dụng máy tính như một công cụ để tấn công các hệ thống thông tin và máy tính khác đang phát triển nhanh chóng và ngày càng trở nên nguy hiểm hơn.

***Chiến tranh mạng***

Theo Viện nghiên cứu tội phạm và tư pháp của Liên hợp quốc (UNICRI), chiến tranh mạng là nói đến bất kỳ hành động của một quốc gia, tiểu bang hoặc tổ chức quốc tế nào nhằm xâm nhập vào mạng máy tính quốc gia khác với mục đích phá vỡ hoặc gây thiệt hại. Tuy nhiên, các định nghĩa rộng hơn cho rằng chiến tranh mạng cũng bao gồm các hành vi của chủ nghĩa tội phạm mạng và khủng bố không gian mạng. Cuộc tấn công thường được thực hiện thông qua virus, DoS hoặc botnet. Theo Laudicina (2016), năm 2017 sẽ là năm của chiến tranh mạng.

* Chiến tranh mạng, một hoạt động bất hợp pháp ở hầu hết các quốc gia, bao gồm các mối đe dọa chính sau đây: sự vi phạm các hành vi gián điệp và bảo mật trực tuyến, được thực hiện để có được tài liệu và thông tin quốc gia có tính chất nhạy cảm hoặc được phân loại thông qua việc khai thác Internet (ví dụ: khai thác lỗi mạng thông qua phần mềm độc hại).
* Phá hoại - việc sử dụng Internet để phá vỡ truyền thông trực tuyến với mục đích gây ra thiệt hại.
* Tấn công vào mạng SCADA (kiểm soát giám sát và thu thập dữ liệu) và NCIs (Cơ sở hạ tầng tính toán quốc gia). Chẳng hạn, năm 2015, tin tặc đã tấn công mạng máy tính của Quốc hội Đức.

***Hoạt động gián điệp mạng***

Hoạt động gián điệp mạng đề cập đến gián điệp trái phép sử dụng hệ thống máy tính. Gián điệp liên quan đến việc lấy được bí mật mà không có sự cho phép của người nắm giữ thông tin (cá nhân, nhóm hoặc tổ chức). Gián điệp mạng là một hoạt động bất hợp pháp ở hầu hết các quốc gia. Đối với các cuộc tấn công mạng vào các công ty Hoa Kỳ của người Trung Quốc, tham khảo bài viết sau (<https://money.cnn.com/2016/03/24/technology/china-cyber-espionage-military/>).

**Tấn công các hệ thống thông tin**

Cuộc tấn công GhostNet không phải là một trường hợp cá biệt của các cuộc tấn công mạng xuyên biên giới. Quốc hội Hoa Kỳ đang nghiên cứu luật pháp để bảo vệ đất nước khỏi những gì mà một số người gọi là cuộc tấn công “Cyber Pearl Harbor”. Vào tháng 5 năm 2014, chính phủ Hoa Kỳ đã chỉ ra năm tin tặc quân sự Trung Quốc đánh cắp dữ liệu và gián điệp hàng ngàn công ty ở Hoa Kỳ, đồng thời đánh cắp bí mật thương mại (nguồn: <https://arstechnica.com/tech-policy/2014/05/how-chinas-army-hacked-american-companies/>).

**Các loại hình tấn công chiến tranh mạng**

Tấn công mạng có thể được phân thành hai loại chính có liên quan đến nhau:

1. **Coporate espionage (gián điệp công ty).** Nhiều cuộc tấn công nhắm vào các công ty liên quan đến năng lượng vì có nhiều thông tin bên trong giá trị. Gần một nửa trong số tất cả các nhà máy điện và các cơ sở hạ tầng khác được khảo sát đã bị xâm nhập bởi những kẻ thù tinh vi, với việc rút tiền là một động lực chung. Tin tặc nước ngoài nhắm vào một hệ thống kiểm soát nhà máy nước ở Illinois, khiến máy bơm bị hỏng. Những kẻ tấn công cũng có được quyền truy cập trái phép vào cơ sở dữ liệu hệ thống.  
   Vào năm 2011, những tên trộm trên mạng (được gọi là nhóm Rove) có trụ sở tại Đông Âu đã chiếm đoạt ít nhất bốn triệu máy tính tại hơn 100 quốc gia trước khi chúng bị bắt. Những kẻ tấn công đã sử dụng phần mềm độc hại và định tuyến lại lưu lượng truy cập Internet một cách bất hợp pháp. Chúng đã đánh cắp 14 triệu đô la trước khi bị bắt. Các tin tặc cũng tấn công các cơ quan chính phủ Hoa Kỳ và các tập đoàn lớn.  
   Vào năm 2013, các tin tặc Trung Quốc bị cáo buộc đã tấn công các máy tính của New York Times để đe dọa các phương tiện truyền thông Mỹ không đưa tin về hình ảnh tiêu cực của Trung Quốc.
2. **Political espionage and warfare (liên quan đến hoạt động gián điệp chính trị).** Hoạt động gián điệp chính trị và chiến tranh mạng đang gia tăng một cách cường độ. Đôi khi, những điều này có liên quan đến gián điệp công ty. Năm 2014, tin tặc Mỹ ở Illinois đã sử dụng phần mềm độc hại DDoS để tấn công trang web chính thức của cuộc trưng cầu dân ý Crimea. Vài ngày sau, các tài nguyên web và trang web truyền thông nhà nước lớn của chính phủ Nga cũng bị tấn công bởi phần mềm độc hại DDoS.

**Ví dụ 1**

Theo Báo cáo Tình báo Hoa Kỳ, người Nga đã tích cực tham gia vào việc hack email của Đảng Dân chủ Hoa Kỳ (ví dụ: e-mail DNC) trong cuộc bầu cử tổng thống năm 2016. Có một sự nỗ lực rõ ràng để tác động đến kết quả của cuộc bầu cử (tham khảo: <https://www.inquisitr.com/3804493/cyber-war-us-russia-obama-putin-hacking/>).

**Ví dụ 2**

Một mạng lưới gián điệp mạng bị tình nghi, được gọi là GhostNet, đã xâm phạm hệ thống máy tính ở 103 quốc gia, bao gồm các hệ thống máy tính thuộc mạng lưới lưu vong, đại sứ quán và các bộ ngoại giao. Các cuộc tấn công được cho là đến từ Trung Quốc.

**Ví dụ 3**

Một trong những sự cố gián điệp mạng phức tạp nhất từng xảy ra là phần mềm gián điệp bị nghi ngờ Turla của Nga, được sử dụng để tấn công hàng trăm máy tính của chính phủ ở Hoa Kỳ và Tây Âu. Các sự cố trên cho thấy sự kém hiệu quả của một số hệ thống bảo mật thông tin. Để biết tổng quan về cách hoạt động của chiến tranh mạng, tham khảo thêm <https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#2d32151d44ce>

**Thúc đẩy dẫn đến các vấn đề về bảo mật thương mại điện tử**

Có nhiều nguyên nhân có thể gây ra vấn đề bảo mật cho thương mại điện tử. Ở đây chúng ta xem xét một số vấn đề chính: thiết kế dễ bị tấn công của Internet, sự thay đổi sang các tội phạm sinh lợi nhuận, cuộc cách mạng không dây, nền kinh tế Internet ngầm, tính chất động của các hệ thống thương mại điện tử và sự tinh vi của các cuộc tấn công…

**Thiết kế dễ bị tấn công của Internet**

Internet và các giao thức mạng đi kèm chưa bao giờ có ý định bảo vệ để chống lại tội phạm mạng. Chúng được thiết kế để cung cấp như phương tiện liên lạc dựa trên máy tính trong một cộng đồng tin cậy. Tuy nhiên, Internet hiện là một nơi để liên lạc, tìm kiếm và giao dịch toàn cầu. Hơn nữa, Internet được thiết kế để đạt hiệu quả tối đa mà không liên quan đến vấn đề bảo mật. Mặc dù đưa ra những giải pháp và cải thiện nhưng về cơ bản Internet vẫn không an toàn.

**Các tội phạm sinh lợi nhuận**

Có một sự thay đổi rõ ràng trong bản chất hoạt động của tội phạm máy tính. Trong những ngày đầu của thương mại điện tử, nhiều tin tặc chỉ muốn đạt được danh tiếng bằng cách phá hoại các trang web. Càng ngày càng có nhiều tội phạm tinh vi, và chúng chuyển sang việc sinh lợi nhuận. Phổ biến nhất là đánh cắp thông tin cá nhân như số thẻ tín dụng, tài khoản ngân hàng, ID và mật khẩu. Theo Cơ quan bảo vệ quyền riêng tư (Privacyrights.org), hàng triệu hồ sơ liên quan đến thông tin cá nhân bị vi phạm hàng năm. Năm 2016, Yahoo! thừa nhận rằng tin tặc đã đánh cắp dữ liệu liên quan đến 1 tỷ tài khoản người dùng của họ. Dữ liệu bị đánh cắp sau đó được bán để kiếm lời.

**Máy tính khắp mọi nơi**

Máy tính ở khắp mọi nơi, từ trong nhà cho đến nơi làm việc, nơi học tập, khu giải trí... Ngay cả xe của bạn cũng có thể bị hack (nguồn: <https://money.cnn.com/2014/06/01/technology/security/car-hack/index.html>).

**Sự gia tăng của các hoạt động không dây (wireless activities) và số lượng các thiết bị di động**

Mạng không dây thường khó bảo vệ hơn mạng hữu tuyến. Ví dụ: nhiều điện thoại thông minh được trang bị chip giao tiếp trường gần (NFC), cần thiết cho thanh toán di động. Ngoài ra, tin tặc có thể khai thác các tính năng của điện thoại thông minh và các thiết bị liên quan (ví dụ: Bluetooth) một cách dễ dàng.

**Sự toàn cầu hoá của kẻ tấn công**

Nhiều quốc gia có những kẻ tấn công mạng (ví dụ: Trung Quốc, Nga, Nigeria, Iran và Ấn Độ). Để biết ví dụ về các cuộc tấn công của Iran vào các ngân hàng Mỹ, tham khảo bài viết <https://www.heritage.org/military-strength-topical-essays/2018-essays/national-defense-and-the-cyber-domain>.

**Sự bùng nổ của mạng xã hội**

Sự phát triển vượt bậc của mạng xã hội cũng như sự phát triển của các nền tảng và công cụ khiến việc bảo vệ chống lại tin tặc trở nên khó khăn hơn. Mạng xã hội là mục tiêu dễ dàng để thực hiện hình thức lừa đảo và các cuộc tấn công kỹ thuật xã hội (social engineering) khác.

**Tính chất động của hệ thống thương mại điện tử**

Các hệ thống thương mại điện tử liên tục thay đổi cùng với những đổi mới. Vấn đề bảo mật do đó cũng đi kèm với thay đổi. Trong những năm gần đây, chúng ta đã gặp nhiều vấn đề về bảo mật trong các lĩnh vực mới của mạng xã hội, thương mại di động và hệ thống không dây. Một điều lưu ý rằng những người trong cuộc (những người làm việc cho các tổ chức bị tấn công) phải chịu trách nhiệm cho gần một nửa các vấn đề bảo mật. Nhân viên mới được bổ sung thường xuyên cho các tổ chức và họ có thể mang theo các mối đe dọa bảo mật.

**Sự tinh vi của các cuộc tấn công**

Tội phạm mạng đang liên tục mài giũa “vũ khí”, sử dụng các sáng tạo về công nghệ. Ngoài ra, chúng còn được tổ chức thành các nhóm rất mạnh, như LulzSec và Anonymous. Tội phạm mạng thay đổi chiến thuật của họ vì an ninh đang được cải thiện (nghĩa là, họ đang thích nghi nhanh chóng với sự thay đổi của môi trường).

**Darknet và nền kinh tế ngầm**

Darknet được xem như một mạng Internet riêng biệt có thể được truy cập thông qua Internet thông thường và một kết nối với mạng TOR (TOR là một mạng VPN cho phép bảo mật trên Internet). Darknet đã hạn chế quyền truy cập tới những người đáng tin cậy (“bạn bè”) bằng cách sử dụng các giao thức phi chuẩn. Darknet cho phép lướt web ẩn danh. Nội dung trên darknet không thể tìm thấy thông qua Google hoặc các công cụ tìm kiếm khác. Công nghệ TOR được sử dụng trong việc chia sẻ tệp (ví dụ như Pirate Bay: https://thepirate-bay.org/home87). Darknet thường được sử dụng cho việc bất đồng chính trị và thực hiện các giao dịch bất hợp pháp, chẳng hạn như mua bán ma túy và vi phạm bản quyền sở hữu trí tuệ thông qua chia sẻ tệp tin. Hoạt động thứ hai được gọi là nền kinh tế Internet ngầm. Vào tháng 11 năm 2014, các cơ quan thực thi pháp luật ở Châu Âu và Hoa Kỳ đã đóng cửa nhiều trang web của TOR. Tuy nhiên, có vẻ như họ cũng chưa bẻ khóa được mã hóa TOR. Năm 2015, chính phủ Mỹ đã đóng cửa một thị trường các dữ liệu cá nhân bị đánh cắp có tên là Darkode.

***Nền kinh tế Internet ngầm***

Nền kinh tế Internet ngầm ám chỉ đến các thị trường điện tử các thông tin bị đánh cắp. Những thị trường này bao gồm hàng ngàn trang web giao bán số thẻ tín dụng, số căn cước công dân, địa chỉ email, số tài khoản ngân hàng, ID mạng xã hội và mật khẩu... Dữ liệu bị đánh cắp được bán cho những kẻ gửi thư rác hoặc cho bọn tội phạm, từ ít hơn một đô la đến vài trăm đô la mỗi lần. Người mua sử dụng chúng để gửi thư rác hoặc thực hiện các giao dịch tài chính bất hợp pháp như chuyển tiền của người khác vào tài khoản của chính họ hoặc thanh toán các hóa đơn khác. Người ta ước tính rằng khoảng 30% tất cả các giao dịch trong thị trường ngầm liên quan đến thẻ tín dụng bị đánh cắp. Symantec ước tính giá trị tiềm năng cho mỗi việc mua bán chỉ thẻ tín dụng và thông tin ngân hàng là khoảng một tỷ đô mỗi năm. Bốn mươi mốt phần trăm nền kinh tế ngầm là ở Hoa Kỳ, trong khi 13% là ở Rumani. Nguồn tham khảo thêm: <https://www.amazon.com/Future-Crimes-Digital-Underground-Connected/dp/0804171459>.

***“Con đường tơ lụa” Internet***

Đây là một trong những địa điểm ngầm nơi hàng trăm người buôn bán ma túy và các thương nhân khác ở các thị trường chợ đen thực hiện công việc kinh doanh. Vào tháng 10 năm 2013, các cơ quan thực thi pháp luật tại Hoa Kỳ đã đóng cửa trang web và bắt giữ người sáng lập, kết án hơn 20 năm tù. Tuy nhiên, ngay sau đó, con đường tơ lụa đã được hồi sinh lại với tên Silk Road 2.0. Các giao dịch trên con đường tơ lụa chỉ thanh toán duy nhất bằng Bitcoin (một loại tiền điện tử). Vào tháng 2 năm 2014, tin tặc đã đánh cắp hơn 4400 Bitcoin được giữ trong ký quỹ (giữa người mua và người bán); hơn 2,7 triệu đô la giá trị Bitcoin biến mất vĩnh viễn (nguồn: https://money.cnn.com/2014/02/14/technology/security/silk-road-bitcoin/). Chủ sở hữu của trang Silk Road tuyên bố phá sản. Tuy nhiên, đến tháng 5 năm 2014, trang web đã hoạt động trở lại với tên Silk Road 2.0 và trở lại trực tuyến vào tháng 5 năm 2016 với tên Silk Road 3.0.

***Chí phí của tội phạm mạng***

Hiện vẫn chưa rõ chi phí tội phạm mạng gây ra là bao nhiêu. Nhiều công ty không tiết lộ khoản lỗ của họ. Tuy nhiên, theo báo cáo toàn cầu nghiên cứu về tội phạm mạng năm 2013 của HP Enterprise Security, nhận thấy rằng chi phí trung bình hàng năm của tội phạm mạng gây ra cho mỗi công ty được khảo sát là 7,2 triệu đô la mỗi năm, tăng 30% so với nghiên cứu chi phí mạng toàn cầu năm trước. Lỗ hổng về dữ liệu có thể là cái giá rất lớn cho các tổ chức.

**Phần 11.1 Câu hỏi ôn tập**

1. Định nghĩa bảo mật máy tính.
2. Liệt kê các rủi ro bảo mật chính hiện nay.
3. Mô tả thiết kế dễ bị tấn công của Internet.
4. Mô tả một số tội phạm máy tính sinh lợi nhuận.
5. Mô tả bản chất động của hệ thống thương mại điện tử.
6. Mô tả nền kinh tế Internet ngầm và darknet.
   1. **Khái quát về các vấn đề bảo mật cơ bản trong thương mại điện tử**

Để hiểu rõ hơn các vấn đề về bảo mật, chúng ta cần nắm được một số khái niệm thường được sử dụng trong bảo mật thương mại điện tử nói riêng và công nghệ thông tin nói chung. Chúng ta bắt đầu với thuật ngữ cơ bản.

**Thuật ngữ bảo mật cơ bản**

* Business continuity plan (kế hoạch kinh doanh liên tục): Một kế hoạch giúp doanh nghiệp hoạt động sau khi có sự cố xảy ra. Mỗi chức năng trong doanh nghiệp nên có một kế hoạch phục hồi hợp lý.
* Cybercrime: Sự phạm tội có chủ đích được thực hiện trên Internet.
* Cybercriminal: Một người cố tình phạm tội trên Internet.
* Exposure: Một trường hợp bị phơi bày tổn thất từ một cuộc tấn công khai thác lỗ hổng (bao gồm ước tính thiệt hại).
* Fraud (gian lận): Bất kỳ hoạt động kinh doanh nào sử dụng các hành vi hoặc thiết bị gian dối để tước đoạt tài sản hoặc các quyền khác.

**Kết luận**

Tội phạm mạng là một hiện tượng đa dạng với nhiều phương pháp và gây thiệt hại đáng kể. Nó liên tục thay đổi vì bọn tội phạm ngày càng sáng tạo và tinh vi hơn. Đối với tình trạng tội phạm mạng năm 2016, thao khảo <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf>.

* Malware (malicious software): Thuật ngữ chung cho phần mềm độc hại.
* Phishing (lừa đảo): Một quá trình gian lận nhằm cố gắng thu thập thông tin nhạy cảm bằng cách giả mạo như một thực thể đáng tin cậy.
* Ransomware: Một phương thức tấn công trong đó kẻ tấn công mã hóa các tệp để nạn nhân không thể mở chúng trừ khi họ trả tiền chuộc.
* Risk (rủi ro): Xác suất mà một lỗ hổng sẽ được biết và khai thác.
* Social engineering (kỹ nghệ xã hội): Một loại tấn công phi kỹ thuật sử dụng một số mưu mẹo để lừa người dùng tiết lộ thông tin hoặc thực hiện một hành động xâm phạm đến máy tính hoặc mạng.
* Spam: thư rác điện tử.
* Vulnerability (lỗ hổng): Điểm yếu trong phần mềm hoặc các cơ chế khác đe dọa tính bảo mật, tính toàn vẹn hoặc tính sẵn sàng của một tài sản. Nó là cơ hội trực tiếp để tin tặc có thể có quyền truy cập vào hệ thống hoặc mạng.
* Zombie: Máy tính bị nhiễm phần mềm độc hại và nằm dưới sự kiểm soát của các tội phạm mạng.