**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.

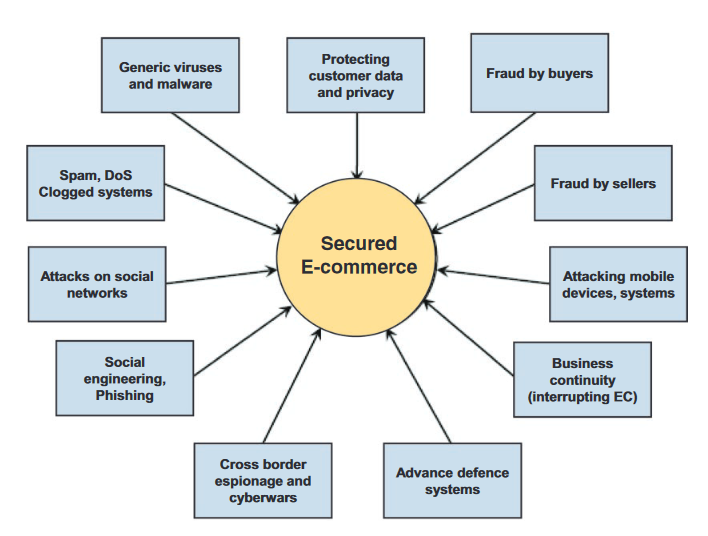
**Bảo mật thương mại điện tử là gì?**

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](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%23.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.
2. 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.
3. 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.
4. **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.

**“Chiến trường” an ninh thương mại điện tử**

Bản chất của bảo mật thương mại điện tử có thể được xem là một chiến trường giữa những kẻ tấn công và những người bảo vệ hệ thống. Chiến trường này bao gồm các thành phần sau, như trong Hình.11.2:

* Các cuộc tấn công, những kẻ tấn công và chiến lược của họ.
* Các tài sản đang bị tấn công (các mục tiêu) trong các hệ thống.
* Bên phòng thủ chống lại các cuộc tấn công và các phương pháp chiến lược của họ.

**Các mối đe dọa và những kẻ tấn công**

Các hệ thống thông tin, bao gồm cả thương mại điện tử, dễ bị tấn công trước các mối đe dọa vô ý và cố ý.

A screenshot of a cell phone

Description automatically generated

*Hình 11.2 “Chiến trường” an ninh thương mại điện tử*

**Đe dọa vô ý (unintentional threat)**

Các mối đe dọa vô ý rơi vào ba loại chính: lỗi do con người, các mối nguy hiểm xung quanh môi trường và các sự cố trong hệ thống máy tính.

* Lỗi do con người: Lỗi của con người có thể xảy ra trong thiết kế phần cứng, phần mềm hoặc các hệ thống thông tin. Nó cũng có thể xảy ra trong lúc lập trình (ví dụ: quên xử lý trong năm nhuận), kiểm thử, thu thập dữ liệu, nhập dữ liệu, vận hành hệ thống... Lỗi có thể xảy ra do sơ suất, quy trình bảo mật lỗi thời, đào tạo nhân viên không đến nơi đến chốn hoặc do mật khẩu không được thay đổi hoặc được chia sẻ với những người khác.
* Mối nguy hiểm môi trường: Bao gồm thiên tai và các điều kiện môi trường khác ngoài tầm kiểm soát của con người (ví dụ: các tai nạn như động đất, bão lớn, bão tuyết hoặc bão cát), lũ lụt, mất điện hoặc biến động mạnh, hỏa hoạn (mối nguy hiểm phổ biến nhất), các vụ nổ, bụi phóng xạ và sự cố hệ thống làm mát nước. Tài nguyên máy tính cũng có thể bị hỏng do tác dụng phụ như khói và nước.
* Trục trặc trong hệ thống máy tính: Sai sot có thể đến từ việc sản xuất kém, vật liệu bị lỗi, rò rỉ bộ nhớ và mạng đã lỗi thời hoặc bảo trì kém. Sự cố vô ý cũng có thể xảy ra vì các nguyên nhân khác, từ thiếu kinh nghiệm người dùng đến việc kiểm thử không đầy đủ. Vào ngày 29 tháng 1 năm 2017, một máy tính bị mất liên kết các chuyến bay của Delta Airline tại Hoa Kỳ. Một trăm năm mươi chuyến bay đã bị hủy (theo CNN News, ngày 29 tháng 1 năm 2017). Một ví dụ khác là Amazon Cloud (EC2), nơi lưu trữ nhiều trang web lớn (ví dụ: Reddit, Airbnb, Foursquare). Trước đây, dịch vụ lưu trữ đám mây đã bị sập do sự cố với các trung tâm dữ liệu của công ty. Sự cố đã làm sập Netflix, Foursquare, Dropbox, Instagram và Pinterest do thời tiết khắc nghiệt tấn công trung tâm dữ liệu ở Bắc Virginia. Những vấn đề này đã được khắc phục sau vài giờ.

**Các cuộc tấn công có chủ ý và tội ác**

Các cuộc tấn công có chủ ý được thực hiện bởi các tội phạm mạng. Các loại tấn công có chủ ý bao gồm đánh cắp dữ liệu, sử dụng dữ liệu không phù hợp (ví dụ: thay đổi hoặc sử dụng nó nhằm mục đích lừa đảo), đánh cắp máy tính xách tay và các thiết bị khác, chèn các chương trình máy tính để đánh cắp dữ liệu, phá hoại hoặc làm hỏng máy tính hoặc hệ thống thông tin, làm hỏng tài nguyên máy tính, tạo và phân phối virus... Các tình huống mở đầu và kết thúc của chương này cung cấp các ví dụ về các cuộc tấn công có chủ ý.

**Tội phạm và phương pháp của họ**

Tội phạm mạng bao gồm hacker và cracker. Một hacker mô tả ai đó có quyền truy cập trái phép vào hệ thống máy tính. Một cracker (còn được gọi là hacker mũ đen) là một hacker với nhiều kinh nghiệm về máy tính và có thể gây hại nhiều hơn. Một số nhóm tin tặc (như nhóm quốc tế Anonymous) được coi là không thể ngăn chặn trong việc xâm nhập vào các tổ chức thuộc mọi loại (nhiều cơ quan chính phủ Hoa Kỳ, bao gồm Quân đội Hoa Kỳ và Bộ Năng lượng). Điều nguy hiểm là một số công ty có thể không thực hiện các biện pháp phòng ngừa tối thiểu để bảo vệ thông tin khách hàng của họ, đổ lỗi cho các cuộc tấn công vào tội phạm mạng. Tội phạm sử dụng nhiều phương pháp cho các cuộc tấn công. Để biết thêm lịch sử hacking tham khảo --------------------- i-programmer.info/news/149-security/3972-a-short-history-of-hacking.html.

**Ví dụ: Ngân hàng Bangladesh**

Một số tin tặc đã cài đặt phần mềm độc hại trong hệ thống máy tính của Ngân hàng Trung ương Bangladesh cho phép chúng xem, trong nhiều tuần, cách rút tiền từ tài khoản ngân hàng US. Các tin tặc sau đó đã cố gắng đánh cắp khoảng 1 tỷ đô la nhưng đã bị chặn lại sau khi đánh cắp 80 triệu đô la từ dự trữ của Bangladesh tại Ngân hàng Dự trữ Liên bang NewYork.

**Mục tiêu của các cuộc tấn công ở các khu vực dễ bị tổn thương**

Như đã thấy trong hình 11.2, các mục tiêu có thể là con người, máy tính hoặc hệ thống thông tin. Gian lận thường nhằm mục đích ăn cắp tiền hoặc các tài sản khác như bất động sản. Máy tính cũng được sử dụng để quấy rối mọi người (ví dụ: đe doạ trực tuyến), làm tổn hại danh tiếng của họ, vi phạm quyền riêng tư của họ, v.v.

**Khu vực dễ bị tổn thương đang bị tấn công**

Bất kỳ phần nào của một hệ thống thông tin cũng có thể bị tấn công. PC, máy tính bảng hoặc điện thoại thông minh có thể dễ dàng bị đánh cắp hoặc tấn công bởi virus và phần mềm độc hại. Người dùng có thể trở thành nạn nhân của một loạt các hành động lừa đảo. Cơ sở dữ liệu có thể bị tấn công bởi những kẻ xâm nhập trái phép và dữ liệu rất dễ bị tổn thương ở nhiều nơi trong một hệ thống máy tính. Ví dụ, dữ liệu có thể được sao chép, thay đổi hoặc đánh cắp. Mạng có thể bị tấn công và luồng thông tin có thể bị dừng hoặc thay đổi. Thiết bị đầu cuối máy tính, máy in và bất kỳ phần thiết bị nào khác có thể bị hỏng theo những cách khác nhau. Chương trình phần mềm có thể bị điều khiển. Các thủ tục và chính sách có thể bị sửa đổi... Các khu vực dễ bị tổn thương thường xuyên bị tấn công.

**Lỗ hổng thông tin**

Một lỗ hổng là nơi kẻ tấn công tìm thấy điểm yếu trong hệ thống và sau đó khai thác điểm yếu đó. Lỗ hổng tạo cơ hội cho kẻ tấn công làm hỏng hệ thống thông tin. MITER Corporation xuất bản một từ điển các lỗ hổng bảo mật được biết đến công khai được gọi là các lỗ hổng và sự cố phổ biến (cve.mitre.org). Tham khảo hướng dẫn của Microsoft về các mối đe dọa và lỗ hổng bảo mật tại <https://technet.microsoft.com/en-us/library/dd159785.aspx>.

**Tấn công điện thoại thông minh và hệ thống không dây**

Vì các thiết bị di động dễ bị tấn công hơn các hệ thống có dây, tấn công điện thoại thông minh và máy tính bảng đang trở nên phổ biến do sự phát triển bùng nổ của điện toán di động. Theo Fink (2014), tin tặc thậm chí có thể đánh cắp mật khẩu điện thoại của bạn bằng kính kỹ thuật số.

**Lỗ hổng của chip RFID**

Những con chip này được nhúng ở mọi nơi, kể cả trong thẻ tín dụng và hộ chiếu của Hoa Kỳ. Thẻ được thiết kế để đọc từ một khoảng cách nhất định (không tiếp xúc), điều này cũng tạo ra một lỗ hổng. Khi bạn mang theo thẻ tín dụng trong ví hoặc túi của mình, bất kỳ ai có đầu đọc RFID đủ gần bạn đều có thể đọc thông tin RFID trên thẻ của bạn. Tham khảo thêm cách thức hoạt động tại <https://www.youtube.com/watch?v=vmajlKJlT3U>.

**Các lỗ hổng trong hệ thống CNTT và thương mại điện tử**

Các lỗ hổng có thể về mặt kỹ thuật (ví dụ: truyền thông không được mã hóa, thiếu các chương trình bảo mật và tường lửa) hoặc chúng có thể về các điểm yếu của tổ chức (ví dụ: thiếu trong đào tạo người dùng và nhận thức về bảo mật, người trong nội bộ đánh cắp dữ liệu và sử dụng máy tính không đúng cách).

**Tài nguyên vi phạm bản quyền**

Việc tải xuống, sao chép hoặc phân phối nhạc, video, sách, phần mềm lậu và các tài sản trí tuệ khác tương đối dễ dàng khi nó có trên Web. Ví dụ: vi phạm bản quyền trực tuyến xảy ra khi phần mềm lậu được tải xuống trái phép từ mạng ngang hàng. Một ví dụ khác là vi phạm bản quyền các sự kiện thể thao trực tiếp. Hậu quả là hàng triệu đô la doanh thu bị tổn thất. Các tổ chức này đang tham gia lực lượng vận động hành lang cho luật bản quyền mạnh mẽ hơn và bằng cách đệ đơn kiện chống lại những người vi phạm. Để biết thông tin và số liệu thống kê về vi phạm bản quyền trực tuyến trên toàn cầu, tham khảo <https://torrentfreak.com/europe-has-the-highest-online-piracy-rates-by-far-160801/>.

**Yêu cầu bảo mật thương mại điện tử**

Bảo mật tốt chính là yếu tố thành công quan trọng trong thương mại điện tử. Tập hợp các yêu cầu bảo mật sau đây được sử dụng để đảm bảo thành công và giảm thiểu rủi ro giao dịch thương mại điện tử:

* **Authentication (xác thực):** Xác thực là một quy trình được sử dụng để xác minh (đảm bảo) danh tính thực sự của một thực thể thương mại điện tử, có thể là một cá nhân, tác nhân phần mềm, chương trình máy tính hoặc trang web thương mại điện tử. Đối với thông báo điện tử, xác thực xác minh rằng người gửi / người nhận tin nhắn là người hoặc tổ chức đúng với những gì họ khai báo.
* **Authorization (ủy quyền):** Ủy quyền là việc cung cấp quyền cho người đã được xác thực truy cập hệ thống và thực hiện các hoạt động nhất định trong các hệ thống cụ thể đó.
* **Auditing (kiểm toán):** Khi một người hoặc chương trình truy cập một trang web hoặc truy vấn cơ sở dữ liệu, nhiều mẩu thông tin khác nhau được ghi lại vào một tệp. Quá trình duy trì hoặc xem xét lại chuỗi sự kiện trong quá trình giao dịch, khi nào và bởi ai, được gọi là kiểm toán.
* **Availability (khả dụng):** Mọi hệ thống thông tin đều phục vụ mục đích riêng của nó và thông tin phải luôn luôn sẵn sàng khi cần thiết. Điều đó có nghĩa rằng hệ thống tính toán sử dụng để lưu trữ và xử lý thông tin, có một hệ thống điều khiển bảo mật sử dụng để bảo vệ nó, và kênh kết nối sử dụng để truy cập nó phải luôn hoạt động chính xác. Hệ thống có tính sẵn sàng cao hướng đến sự sẵn sàng ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: sự cố mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống… đảm bảo tính sẵn sàng cũng có nghĩa là tránh được tấn công từ chối dịch vụ.
* **Nonrepudiation (chống chối bỏ):** Chống chối bỏ có nghĩa rằng một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác. Ví dụ: trong khi giao dịch mua hàng qua mạng, khi khách hàng đã gửi số thẻ tín dụng cho bên bán, đã thanh toán thành công, thì bên bán không thể phủ nhận việc họ đã nhận được tiền, (trừ trường hợp hệ thống không đảm bảo tính an toàn thông tin trong giao dịch).

Tính xác thực và chống chối bỏ là các biện pháp phòng chống hiệu quả lừa đảo và đánh cắp danh tính. Để bảo vệ và đảm bảo sự tin cậy trong các giao dịch thương mại điện tử, chữ ký số, hoặc các chứng nhận số, thường được thêm vào để xác nhận người gửi và thời gian của các giao dịch nên người mua không thể phủ nhận rằng giao dịch không xảy ra.

**Bên phòng vệ và những phương pháp, chiến lược**

Chiến lược bảo mật thương mại điện tử bao gồm nhiều lớp phòng thủ gồm một số phương pháp. Bảo vệ này nhằm mục đích cản trở, ngăn chặn và phát hiện sự xâm nhập trái phép vào máy tính của tổ chức và các hệ thống thông tin). Các biện pháp phòng ngừa giúp ngăn chặn những người không được phép truy cập vào hệ thống thương mại điện tử (ví dụ: bằng cách sử dụng các thiết bị xác thực, tường lửa…). Các biện pháp phát hiện giúp tìm ra các vi phạm an ninh trong các hệ thống máy tính. Thông thường, điều này có nghĩa là tìm hiểu xem những kẻ xâm nhập đang cố gắng (hoặc đã cố gắng) đột nhập vào hệ thống thương mại điện tử, liệu chúng có thành công hay không, liệu chúng có còn làm hỏng hệ thống hay không và chúng có thể gây ra thiệt hại gì không.

**Đảm bảo thông tin**

Đảm bảo rằng khách hàng mua sắm trực tuyến an toàn và bảo mật là một phần quan trọng trong việc cải thiện trải nghiệm người dùng trực tuyến. Đảm bảo thông tin (IA) là các biện pháp được thực hiện để bảo vệ các hệ thống thông tin và các quy trình của chúng chống lại mọi rủi ro.

**Hình phạt có thể có**

Một phần của phòng thủ là để ngăn chặn tội phạm bằng cách trừng phạt họ nặng nề nếu họ bị bắt. Các thẩm phán hiện đang đưa ra các hình phạt nặng nề và khắc nghiệt hơn một thập kỷ trước. Ví dụ, vào tháng 3 năm 2010, một thẩm phán liên bang đã kết án hacker TJX 28 tuổi Albert Gonzalez 20 năm tù vì vai trò của anh ta trong việc đánh cắp hàng triệu số thẻ tín dụng và thẻ ghi nợ rồi bán chúng. Những bản án nghiêm khắc như vậy sẽ gửi một thông điệp mạnh mẽ tới tin tặc và răn đe họ. Thật không may, trong nhiều trường hợp, hình phạt là quá nhẹ để răn đe tội phạm mạng.

**Phục hồi (recovery)**

Phục hồi là rất quan trọng đặc biệt sau khi xảy ra các cuộc tấn công trái phép. Nó phải được thực hiện một cách nhanh chóng bởi vì doanh nghiệp vẫn cần tiếp tục kinh doanh cho đến khi hệ thống thông tin được khôi phục hoàn toàn.

**Phần 11.2 Câu hỏi ôn tập**

1. Liệt kê năm điều khoản bảo mật chính của thương mại điện tử.
2. Mô tả các mối nguy hiểm an ninh không chủ ý.
3. Liệt kê năm ví dụ về tội phạm bảo mật thương mại điện tử có chủ ý.
4. Mô tả cuộc chiến an ninh, những người tham gia và hình thức diễn ra. Các kết quả có thể là gì?
5. Định nghĩa hacker và cracker.
6. Liệt kê tất cả các yêu cầu về bảo mật, định nghĩa các yêu cầu xác thực và ủy quyền.
7. Tính chống chối bỏ là gì?
8. Mô tả một vài lỗ hổng và cách thức tấn công có thể.
9. Mô tả hình thức răn đe, ngăn chặn và phát hiện trong các hệ thống bảo mật thương mại điện tử.
10. Chiến lược bảo mật là gì và tại sao lại cần thiết?

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

Có nhiều cách bọn tội phạm tấn công thông tin hệ thống EC và người dùng. Ở đây, chúng tôi chỉ bao gồm các phương pháp đại diện chính.

Để biết ví dụ từ Ấn Độ (32 slide), xem Singh (2016).

Rất hữu ích để phân biệt giữa hai loại tấn công phổ biến – **kỹ thuật** (mà chúng ta sẽ thảo luận trong phần này) và **phi kỹ thuật** mà chúng tôi thảo luận trong phần: “**Phương pháp phi kỹ thuật: Từ lừa đảo đến thư rác và gian lận**”.

**Tấn công kỹ thuật và phi kỹ thuật: Tổng quan**

Kiến thức phần mềm và hệ thống được sử dụng để duy trì các cuộc tấn công kỹ thuật. Sử dụng không đủ các phần mềm chống virus và tường lửa cá nhân và giao tiếp không được mã hóa là những lý do chính cho các lỗ hổng kỹ thuật.

Các cuộc tấn công tổ chức phi kỹ thuật là những cuộc tấn công mà bảo mật của mạng hoặc máy tính bị xâm phạm (ví dụ: thiếu đào tạo nâng cao nhận thức an ninh thích hợp). Chúng tôi coi gian lận tài chính, thư rác, kỹ thuật xã hội, bao gồm lừa đảo, ransomware và các phương thức gian lận khác, là phi kỹ thuật. Nhiều phương pháp phi kỹ thuật cũng sử dụng một số phần mềm độc hại trong các cuộc tấn công của họ. Các mục tiêu của kỹ thuật xã hội là giành quyền truy cập trái phép vào các hệ thống hoặc thông tin bằng cách thuyết phục những người không bị nghi ngờ tiết lộ thông tin cá nhân được sử dụng bởi bọn tội phạm để lừa đảo và các tội phạm khác. Các phương pháp phi kỹ thuật chính được mô tả trong phần “**Phương pháp phi kỹ thuật: Từ lừa đảo đến thư rác và gian lận**”. Đối với danh sách 10 cuộc tấn công hàng đầu theo thể loại, xem [www.secpoint.com](file:///C:\Users\QUANGTHAI\Desktop\www.secpoint.com). Sau đó, tìm kiếm về virus, phần mềm gián điệp, vv

**Các phương pháp tấn công kỹ thuật chính**

Tin tặc thường sử dụng một số công cụ phần mềm (không may là có sẵn và miễn phí trên Internet cùng với hướng dẫn về cách sử dụng chúng) để tìm hiểu về các lỗ hổng cũng như các thủ tục tấn công. Cuộc tấn công kỹ thuật lớn các phương pháp được minh họa trong hình 11.3 và được mô tả ngắn gọn tiếp theo. Lưu ý rằng có nhiều phương thức khác, chẳng hạn như “mass SQL injection” các cuộc tấn công có thể rất nguy hiểm.

**Phần mềm độc hại: Virus, Sâu và Ngựa Trojan**

Phần mềm độc hại là một chương trình phần mềm, khi lan truyền, được thiết kế để lây nhiễm, thay đổi, làm hỏng, xóa hoặc thay thế dữ liệu hoặc hệ thống thông tin mà không có sự hiểu biết hoặc chấp thuận của chủ sở hữu. Phần mềm độc hại là một thuật ngữ toàn diện mô tả bất kỳ chương trình hoặc phần mềm độc hại nào (ví dụ: virus là một tập hợp con của chương trình phần mềm độc hại). Các cuộc tấn công bằng phần mềm độc hại là hành vi xam phạm bảo an ninh phổ biến nhất. Các hệ thống máy tính bị nhiễm phần mềm độc hại nhận lệnh từ bọn tội phạm và thực hiện những việc như gửi thư rác hoặc đánh cắp mật khẩu được lưu trữ của người dùng.

|  |  |
| --- | --- |
| *Hình 11.3 Các phương pháp tấn công an ninh kỹ thuật chính*  *(theo thứ tự quan trọng giảm dần)* |  |

Phần mềm độc hại bao gồm virus máy tính, sâu, botnet, ngựa Trojan, công cụ lừa đảo, công cụ phần mềm gián điệp và các phần mềm độc hại và không mong muốn khác. Theo Harrison và Pagliery (2015), gần một triệu mối đe dọa phần mềm độc hại mới được phát hành trên toàn thế giới mỗi ngày.

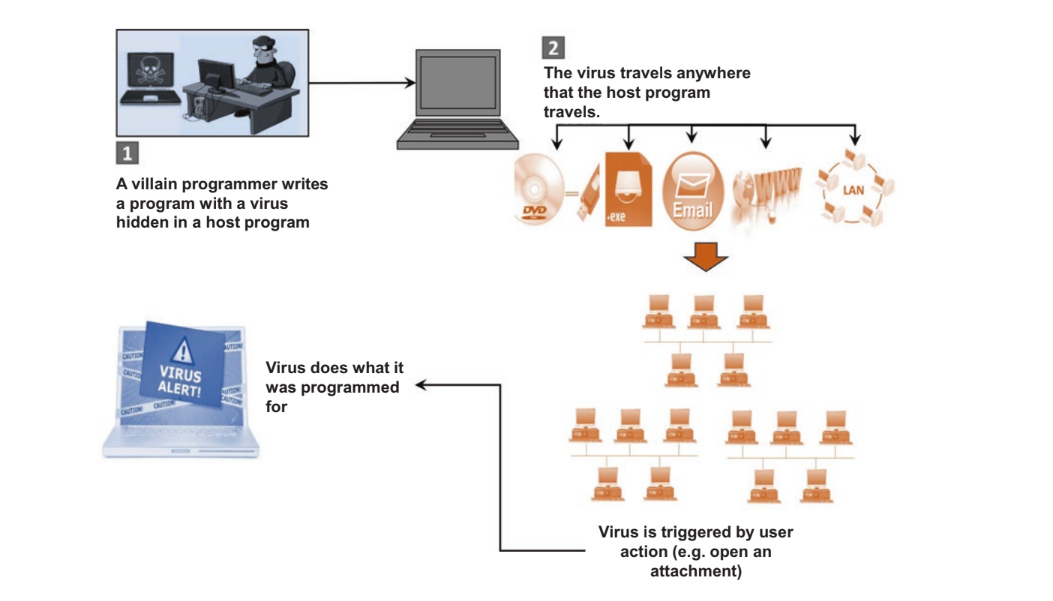
Theo Adhikari (2016), một phần mềm độc hại Android có tên Gooligan đã vi phạm hơn một triệu tài khoản Google. Phần mềm độc hại ảnh hưởng đến thiết bị chạy Android 4 và 5.

**Viruses**

Một virus được lập trình phần mềm được bọn tội phạm chèn vào máy tính để làm hỏng hệ thống; chạy chương trình máy chủ bị nhiễm kích hoạt virus. Một virus có hai khả năng cơ bản. Đầu tiên, nó có một cơ chế mà cho phép nó lây lan. Thứ hai, nó có thể thực hiện các hoạt động gây hại sau khi được kích hoạt. Đôi khi một sự kiện cụ thể kích hoạt việc thực thi virus Virus. Vấn đề là các hệ thống chống vi-rút hiện tại có thể không hoạt động chống lại virus mới và thật không may, vi-rút mới được tạo ra mọi lúc. Chẳng hạn, ngày sinh của Michelangelo đã kích hoạt virus Michelangelo khét tiếng. Vào ngày 1 tháng 4 năm 2009, cả thế giới đang chờ đợi một loại virus có tên Conficker. Vào năm 2014, một loại virus có tên là “Pony”, đã lây nhiễm hàng trăm nghìn máy tính để đánh cắp Bitcoin và các loại tiền ảo khác (xem Finkle 2014). Cuối cùng, Finkle báo cáo rằng một loại virus có tên Agent BTZ đã tấn công hơn 400.000 máy tính ở Nga, Hoa Kỳ và Châu Âu. Cuộc tấn công lớn này đã không thành công, nhưng virus vẫn tiếp tục lây lan mọi lúc.

***Virus ILOVEYOU***

Virus ILOVEYOU là một trong những loại virus gây hại nhất trong lịch sử. Nó được gửi qua một email ghi chú với dòng chữ “I LOVE YOU” trong dòng chủ đề và nó chứa một tệp đính kèm mà khi mở ra, kết quả là tin nhắn được gửi đến mọi người trong sổ địa chỉ Microsoft Outlook của người nhận và có lẽ nghiêm trọng hơn, dẫn đến mất mọi JPEG, MP3 và một vài tệp khác trên ổ cứng người nhận.



*Hình 11.4 Làm thế nào một virus máy tính có thể lây lan*

Do đó, nó đã có thể lan truyền nhanh chóng từ người dùng sang người dùng trong một nhóm. Vào ngày 4 tháng 5 năm 2000, khi virus lần đầu tiên xuất hiện, nó đã lan truyền nhanh đến mức e-mail phải ngừng hoạt động ở một số doanh nghiệp lớn. Virus đã lan ra khoảng 45 triệu người dùng trong một ngày.

Một trong những bước đầu tiên mà các công ty sử dụng để tránh virus ILOVEYOU là sàng lọc các ghi chú với ILOVEYOU trong dòng chủ đề. Tuy nhiên, các tin tặc đã nhanh chóng giới thiệu các biến thể copycat. Tổng thiệt hại ước tính lên tới 10 tỷ USD. Các loại virus/sâu gây hại khác là Code Red, Melissa và Sasser.

**Sâu**

Không giống như virus, một con sâu có thể tự sao chép một cách tự động (như là một trò chơi độc lập trên phạm vi trực tuyến của bất kỳ máy chủ hoặc người nào). Sâu sử dụng mạng để truyền bá và lây nhiễm máy tính hoặc thiết bị cầm tay và thậm chí có thể lây lan qua tin nhắn tức thời hoặc e-mail. Ngoài ra, không giống như các loại virus thường bị giới hạn trong một máy tính mục tiêu, một con sâu có thể lây nhiễm nhiều thiết bị trong mạng cũng như làm giảm hiệu suất của mạng. Theo Cisco, sâu có thể khai thác lỗ hổng trên hệ thống đích hoặc sử dụng một số loại kỹ thuật xã hội để lừa người dùng thực thi chúng. Vì sâu lây lan nhanh hơn nhiều so với virus, nên chúng có thể nguy hiểm hơn.

***Macro Virus và Micro Worms***

Macro virus (macro worm) là mã phần mềm độc hại được đính kèm vào tệp dữ liệu thay vì chương trình thực thi (ví dụ: tệp Word). Theo Microsoft, virus macro có thể tấn công các tệp Word cũng như bất kỳ ứng dụng nào khác sử dụng ngôn ngữ lập trình. Khi tài liệu được mở hoặc đóng, virus có thể lây lan sang các tài liệu khác trên hệ thống máy tính. Để biết thông tin về Word macro virus, hãy xem Microsoft Support tại support.microsoft.com/kb/187243/en. Các chương trình máy tính rất giống với virus là sâu và ngựa Trojan.

***Ngựa Trojan***

Một con ngựa thành Troia là một chương trình có vẻ vô hại hoặc thậm chí trông có vẻ hữu ích nhưng thực sự có chứa một mã độc ẩn. Người dùng bị lừa thực thi một tệp bị nhiễm, nơi nó tấn công máy chủ, bất cứ nơi nào từ việc chèn các cửa sổ bật lên đến làm hỏng máy chủ bằng cách xóa các tệp, phát tán phần mềm độc hại, v.v. Tên này bắt nguồn từ con ngựa thành Trojan trong thần thoại Hy Lạp. Truyền thuyết kể rằng trong cuộc chiến thành Trojan, thành phố Troy đã được tặng một con ngựa gỗ lớn làm quà tặng cho nữ thần Athena. Trojans kéo con ngựa bên trong cổng thành. Trong đêm, những người lính Hy Lạp đang ẩn náu trong con ngựa rỗng đã mở cổng thành Troy và cho quân đội Hy Lạp vào. Quân đội đã có thể chiếm thành phố và chiến thắng trong cuộc chiến. Trojan chỉ được lan truyền bởi sự tương tác của người dùng (ví dụ: chẳng hạn như hoạt động dưới vỏ bọc của một email được cho là của Verizon) và có nhiều biến thể của Trojan (ví dụ: Zeus, W32).

**Ví dụ 1: Trojan-Phisher-Rebery**

Năm 2006, một biến thể của chương trình ngựa thành Trojan có tên là Trojan-Phisher-Rebery đã được sử dụng để đánh cắp hàng chục ngàn danh tính từ những người ở 125 quốc gia khác nhau. Phần mềm độc hại Rebery là một ví dụ về banking Trojan, được lập trình để tạo ra thiệt hại khi người dùng truy cập vào một số trang web ngân hàng trực tuyến hoặc thương mại điện tử. Để biết bức tranh thông tin mô tả trạng thái của financial Trojans, xem Wueest (2013).

**Ví dụ 2: Tấn công DDOS trên WordPress Corporation**

Vào tháng 3 năm 2014, tin tặc đã sử dụng botnet để tấn công hơn 162.000 trang web WordPress. Cho biết WordPress có khoảng 17% các trang web viết blog trên thế giới, bất kỳ cuộc tấn công nào cũng có thể gây ra tổn thất lớn.

**Một số lỗi bảo mật: Heartbleed và CryptoLocker**

Hai lỗi máy tính nguy hiểm được phát hiện vào năm 2013 và 2014.

**Heartbleed**

Theo Russell (2014), “Heartbleed là một lỗ hổng trong OpenSSL, tiêu chuẩn mã hóa nguồn mở được sử dụng bởi phần lớn các trang web cần truyền dữ liệu mà người dùng muốn giữ an toàn. Về cơ bản, nó cung cấp cho bạn một dòng an toàn khi bạn gửi e-mail hoặc trò chuyện trên IM”.

Thiệt hại tiềm tàng có thể lớn. Về lý thuyết, bất kỳ dữ liệu nào được lưu trong bộ nhớ hoạt động đều có thể bị bug lấy ra. Tin tặc thậm chí có thể đánh cắp các khóa mã hóa cho phép chúng đọc các tin nhắn được mã hóa. Khoảng 650 triệu trang web có thể bị ảnh hưởng. Lời khuyên duy nhất được cung cấp bởi các chuyên gia là thay đổi mật khẩu trực tuyến.

**CryptoLocker**

Được phát hiện vào tháng 9 năm 2013, CryptoLocker là một lỗi Trojan ransomware. Phần mềm độc hại này có thể đến từ nhiều nguồn bao gồm tệp đính kèm e-mail và có thể mã hóa các tệp trên máy tính của bạn, do đó bạn không thể đọc các tệp này. Chủ sở hữu phần mềm độc hại sau đó đề nghị giải mã dữ liệu để đổi lấy Bitcoin hoặc hệ thống thanh toán không thể truy xuất tương tự.

Để biết thông tin về những việc cần làm nếu bạn bị tống tiền và cách tự bảo vệ mình, xem Cannell (2013).

**Mirai (Phần mềm độc hại)**

Theo Wikipedia, thì Mirai (tiếng Nhật nghĩa là “tương lai”) là phần mềm độc hại biến các hệ thống máy tính chạy Linux thành các “bot” điều khiển từ xa có thể được sử dụng như một phần của mạng botnet trong các cuộc tấn công mạng quy mô lớn. Nó chủ yếu nhắm vào các thiết bị tiêu dùng trực tuyến như máy ảnh từ xa và bộ định tuyến gia đình ... Mạng botnet Mirai đã được sử dụng trong một số cuộc tấn công từ chối dịch vụ phân tán (DDoS) lớn nhất và gây gián đoạn nhất, bao gồm cả cuộc tấn công vào ngày 20 tháng 9 năm 2016 đối với trang web của nhà báo bảo mật máy tính Brian Krebs, ... và cuộc tấn công mạng Dyn tháng 10 năm 2016 .... ”.

**Từ chối dịch vụ (DoS và DDoS)**

Theo Incapsula, Inc., một cuộc tấn công từ chối dịch vụ (DoS) là một nỗ lực độc hại để làm cho một máy chủ hoặc tài nguyên mạng không có sẵn cho người dùng, thường bằng cách tạm thời gián đoạn hoặc tạm dừng các dịch vụ của máy chủ được kết nối với Internet. Điều này khiến hệ thống gặp sự cố hoặc không thể phản hồi kịp thời, do đó trang web trở nên không khả dụng. Một trong những kiểu tấn công DoS phổ biến nhất xảy ra khi tin tặc tấn công vào hệ thống bằng cách làm quá tải hệ thống với lưu lượng truy cập vô dụng, vì vậy người dùng không được truy cập vào e-mail, trang web, v.v.

Lưu ý: Tấn công DoS là một cuộc tấn công độc hại gây ra bởi một máy tính và một kết nối Internet trái ngược với cuộc tấn công từ chối dịch vụ phân tán (DDoS), mà liên quan đến nhiều thiết bị và nhiều kết nối Internet. Ví dụ, cuộc tấn công vào Dyn (trường hợp đóng cửa) được thực hiện bởi hàng ngàn máy tính bị tin tặc bắt làm con tin. Tin tặc cũng sử dụng IoT (Chương 7) để bắt giữ máy tính và bắn phá các nạn nhân; xem Mello Jr. (2016). Kẻ tấn công cũng có thể sử dụng tin nhắn e-mail spam để khởi động một cuộc tấn công tương tự vào tài khoản e-mail của bạn. Một phương pháp phổ biến để khởi động các cuộc tấn công DoS là sử dụng máy tính zombie (bị cướp), cho phép máy tính bị cướp bị điều khiển từ xa bởi tin tặc mà không có sự nhận biết của chủ sở hữu máy tính. Máy tính zombie (còn được gọi là botnet trực tuyến) đưa ra vô số yêu cầu đối với một trang web bị tấn công, tạo ra DoS. Ví dụ, những kẻ tấn công DoS nhắm vào các mạng xã hội, đặc biệt là Facebook và Twitter.

**Ví dụ**

Vào ngày 22 tháng 10 năm 2016, trong cuộc tấn công vào Dyn, một số mạng xã hội đã sập trong hơn một giờ. Chúng bao gồm Twitter, Spotify và Reddit; xem Lake (2016).

Các cuộc tấn công DoS có thể khó dừng lại. May mắn thay, cộng đồng bảo mật đã phát triển các công cụ để chống lại chúng. Để có cái nhìn bao quát, hãy xem us-cert.gov/ncas/tips/ST04-015.

Lưu ý: Vào năm 2014, một nhóm hack có tên Lizard Stresser đã đề xuất gỡ bỏ bất kỳ trang web nào bằng cách sử dụng DoS, với mức phí 3 đô la (xem Goldman 2014a).

**Máy chủ web và Chiếm quyền điều khiển trang web**

Đánh cắp trang *hay pagejacking* là sao chép bất hợp pháp nội dung trang web để người dùng có thể bị chuyển hướng sai sang một trang web khác. Các tài khoản truyền thông xã hội đôi khi bị tấn công nhằm mục đích đánh cắp thông tin cá nhân của chủ tài khoản. Ví dụ, 50 triệu người theo dõi Justin Bieber đã trở thành nạn nhân của phương pháp này khi tài khoản Twitter của Bieber bị tấn công vào tháng 3 năm 2014. Tài khoản được nhúng với một liên kết độc hại đến một ứng dụng được sử dụng để đánh cắp tài khoản được chuyển tiếp tới nhiều bạn bè hơn.

**Botnets**

Theo Trung tâm an toàn và bảo mật của Microsoft, botnet (còn được gọi là quân đội zombie zombie) là một phần mềm độc hại mà bọn tội phạm phân phối để lây nhiễm một số lượng lớn máy tính kết nối Internet bị tấn công bởi tin tặc. Những máy tính bị nhiễm này sau đó tạo thành một mạng botnet, mạng khiến cho máy tính cá nhân thực hiện các cuộc tấn công trái phép trên Internet mà không có sự nhận biết của người dùng. Các tác vụ trái phép bao gồm gửi thư rác và e-mail, tấn công máy tính và máy chủ và thực hiện các loại lừa đảo khác, khiến máy tính của người dùng chậm lại (microsoft.com/security/resource/botnet-whatis.aspx).

Mỗi máy tính tấn công được coi là robot máy tính. Một mạng botnet được tạo thành từ 75.000 hệ thống bị nhiễm, vào năm 2010, với các máy tính bị nhiễm Zeus Trojan. Botnet được sử dụng trong các trò gian lận, spam và lừa đảo hoặc chỉ để làm hỏng hệ thống. Botnet xuất hiện ở các dạng khác nhau và có thể bao gồm sâu hoặc virus. Các botnet nổi tiếng bao gồm Zeus, Srizbi, Pushdo / Cutwail, Torpig và Conficker.

**Ví dụ**

Rustock là một mạng botnet được tạo thành từ khoảng một triệu máy tính bị tấn công, mà đã trốn tránh sự phát giác trong nhiều năm. Mạng botnet, đã gửi tới 30 tỷ tin nhắn rác mỗi ngày, đã đặt các quảng cáo “booby-traped”và liên kết trên các trang web mà các nạn nhân truy cập. Những kẻ gửi thư rác đã ngụy trang các bản cập nhật cho PC để trông giống như các bình luận trong các bảng thảo luận, khiến chúng khó tìm thấy bằng phần mềm bảo mật. Microsoft là một trong những công ty đã giúp đánh sập Rustock. Vào năm 2013, Microsoft và FBI đã “phá hủy” hơn 1000 botnet được sử dụng để đánh cắp thông tin và danh tính ngân hàng. Cả Microsoft và FBI đều đã cố gắng hạ gục phần mềm độc hại “Citadel”, thứ đã ảnh hưởng đến hàng triệu người ở hơn 90 quốc gia. Để phân tích các cuộc tấn công botnet độc hại, xem Katz (2014).

***Thiết bị gia dụng “Botnet”***

Internet của vạn vật (IoT) cũng có thể bị hack. Kể từ khi các thiết bị gia dụng thông minh (Chương 7) có kết nối với Internet, chúng có thể trở thành máy tính có thể bị hack và kiểm soát. Vụ tấn công tại nhà đầu tiên, liên quan đến bộ máy truyền hình và ít nhất một tủ lạnh, xảy ra trong khoảng thời gian từ tháng 12 năm 2013 đến tháng 1 năm 2014 và được gọi là “Thiết bị gia dụng ‘botnet’ đầu tiên và cuộc tấn công mạng đầu tiên từ Internet of Things”. Tin tặc đã đột nhập vào hơn 100.000 thiết bị gia dụng được kết nối và sử dụng chúng để gửi hơn 750.000 e-mail độc hại cho các doanh nghiệp và cá nhân trên toàn thế giới (xem Bort 2014).

Đối với các cuộc tấn công hình sự bằng cách sử dụng botnet, xem Mello, Jr. (2016).

**Quảng cáo độc hại**

Theo Techopedia, quảng cáo độc hại là “một dạng quảng cáo Internet độc hại được sử dụng để phát tán phần mềm độc hại”. Quảng cáo độc hại được thực hiện bằng cách ẩn mã độc hại trong các quảng cáo trực tuyến tương đối an toàn (xem techopedia.com/definition/4016/malvertising).

Lưu ý rằng tin tặc đang nhắm mục tiêu quảng cáo để ẩn phần mềm độc hại gia tăng nhanh chóng. Ví dụ: vào năm 2013, Google đã vô hiệu hóa quảng cáo từ hơn 400.000 trang web đang ẩn phần mềm độc hại (xem Yadron 2014). Lời cuối cùng: Nếu bạn nhận được một e-mail chúc mừng bạn vì đã giành được một số tiền lớn và yêu cầu bạn “Xin vui lòng xem tệp đính kèm”, đừng làm theo!

### Keystroke Logging trong nền kinh tế ngầm

**Keystroke logging (keylogging)** là quá trình sử dụng thiết bị hoặc chương trình phần mềm theo dõi và ghi lại hoạt động của một người dùng trong thời gian thực (không có nhận biết hoặc sự đồng ý của người dùng) bằng các phím bàn phím họ nhấn. Vì thông tin cá nhân chẳng hạn như mật khẩu và tên người dùng được nhập trên bàn phím, keylogger có thể sử dụng tổ hợp phím để lấy chúng.

**11.4 Các phương pháp phi kỹ thuật: Từ tấn công giả mạo (Phishing) đến thư rác (Spam) và lừa đảo (Fraud)**

Như đã đề cập trong phần “Vấn đề bảo mật thông tin”, đã có một sự thay đổi liên quan đến lợi nhuận của các tội phạm Internet. Những tên tội phạm này được thực hiện với sự trợ giúp của cả 2 công cụ kỹ thuật, như mã độc, cái có thể truy cập vào các thông tin bí mật có thể được sử dụng để lấy cắp tiền từ tài khoản ngân hàng trực tuyến của bạn, và các phương pháp phi kỹ thuật, như tấn công phi kỹ thuật.

Chú ý: Hầu hết các phương pháp phi kỹ thuật được liệt kê trong phần này sử dụng một vài phần mềm kỹ thuật độc hại (ví dụ như vi-rút). Sau đó, bọn tội phạm sử dụng một số cách tiếp cận phi kỹ thuật (ví dụ như áp lực về tâm lý). Lừa đảo có thể dưới nhiều hình thức. Những nội dung chính sẽ được đề cập trong chương này. Một số phương pháp khác là sự kết hợp giữa kỹ thuật và phi kỹ thuật (ví dụ như mã độc tống tiền). Đối với các xu hướng lừa đảo phạm tội về kinh tế toàn cầu, tham khảo Altshull (2017). Đối với các tác động nghiệp vụ và giải pháp, tham khảo Perret (2016).

**Kỹ thuật tấn công xã hội (Social Engineering) và lừa đảo (Fraud)**

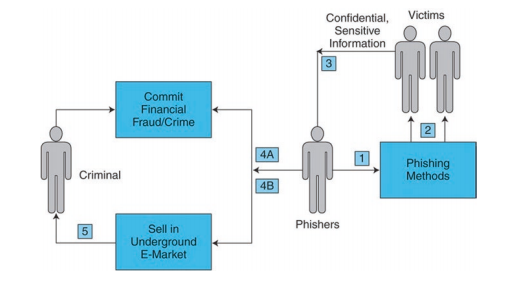
Kỹ thuật tấn công xã hội đề cập đến một tập hợp các phương pháp mà tội phạm sử dụng tâm lý của con người để thuyết phục hoặc thao túng mọi người tiết lộ thông tin cá nhân của họ, hoặc thông tin về việc làm của họ, để chúng có thể thu thập thông tin cho các hoạt động bất hợp pháp. Tin tặc cũng có thể cố gắng truy cập vào máy tính của người dùng để cài đặt phần mềm độc hại, thứ sẽ cung cấp cho tin tặc quyền kiểm soát máy tính cá nhân. Các cuộc tấn công kỹ thuật xã hội chủ yếu là *tấn công giả mạo* (một số phương pháp: thông thường, một kẻ lừa đảo gửi một e-mail trông giống như là đến từ một nguồn đáng tin cậy), *mạo danh* (ví dụ: một e-mail được gửi từ một người mạo danh bạn bè để hỏi vay tiền) và *diversion theft* (khi một kỹ sư xã hội thuyết phục một công ty chuyển phát nhanh rằng hắn ta thật sự là người nhận gói hàng nhưng nó được sửa lại thành một địa chỉ khác, nơi hắn có thể lấy được gói hàng. Khi thông tin được lấy từ một nạn nhân (ví dụ: thông qua lừa đảo), nó được sử dụng để thực hiện hành vi phạm tội, chủ yếu là để thu lợi tài chính, như thể hiện trong hình 11.5. Tốc độ tăng trưởng của các lỗ hổng chưa được vá và khối lượng các e-mail, văn bản hoặc các hoạt động lừa đảo trên các Website đang tăng nhanh (để dự đoán, tham khảo Damri 2016).

Như bạn có thể thấy trên hình, những kẻ lừa đảo có được thông tin bí mật bằng cách sử dụng các phương pháp từ các kỹ thuật tấn công xã hội để trộm cắp. Thông tin bị đánh cắp (ví dụ: số thẻ tín dụng, danh tính người dùng) được kẻ trộm sử dụng để lừa đảo lợi ích tài chính, hoặc nó được bán trên thị trường Internet ngầm cho các nhóm tội phạm khác, những kẻ sau đó sẽ sử dụng thông tin để thực hiện hành vi phạm tội tài chính. Để biết thêm chi tiết, tham khảo Wallen (2016). Trong phần này, chúng tôi sẽ mô tả phishing, một phần nhỏ của kỹ thuật xã hội, được sử dụng.

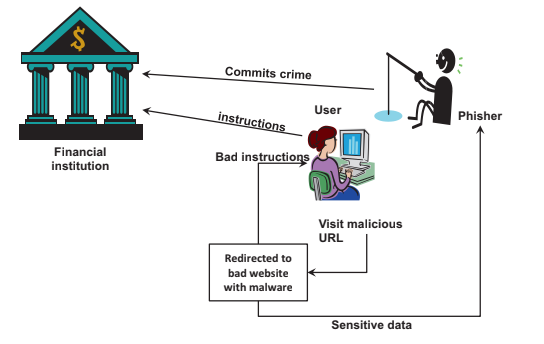
Tin tặc khét tiếng Kevin Mitnick, người đã phải ngồi tù vì hack, đã sử dụng kỹ thuật tấn công xã hội làm phương pháp chính để giành được quyền truy cập vào các hệ thống máy tính.

**Tấn công giả mạo mang tính xã hội (Social Phishing)**

Trong lĩnh vực bảo mật máy tính, tấn công giả mạo là một quá trình gian lận để có được thông tin bí mật, chẳng hạn như thẻ tín dụng hoặc thông tin về ngân hàng, từ người dùng máy tính. Kẻ lừa đảo gửi thư điện tử, IM, bình luận hoặc tin nhắn văn bản đến từ một công ty, ngân hàng, trường học hay một tổ chức công khai đáng tin cậy, nổi tiếng. Người dùng được hướng dẫn truy cập vào 1 trang web hỏng, nơi người dùng có thể bị lừa gửi thông tin bí mật (ví dụ: được yêu cầu cập nhật thông tin). Đôi khi những tên lừa đảo cài đặt các phần mềm độc hại để tạo điều kiện cho việc trích xuất thông tin. Tham khảo cuốn “Marlins Cry A Phishing Story” của Swann (2012), một cuốn tiểu thuyết thú vị tiếng kêu báo động về an ninh mạng. Quá trình lừa đảo dựa trên nền tảng Web được minh họa trong hình 11.6. Tham khảo APWG (2016) để xem các báo cáo hàng quý.



*Hình 11.5 Từ lừa đảo đến gian lận phạm tội tài chính*



*Hình 11.6 Mô tả việc lừa đảo hoàn thành*

**Ví dụ: Lừa đảo giả mạo Amazon 2016**

Theo ngài Jones, “Ngay trong mùa lễ hội mua sắm, một email lừa đảo giả mạo khổng lồ đang được lây lan. Bạn thực sự cần phải coi chừng email giả mạo Amazon này. Những gì đang xảy ra là mọi người nhận được email tự nhận là tự Amazon, nhưng chúng thực ra là những kẻ lừa đảo. Các email cảnh bảo người nhận rằng có một vấn đề khi xử lý đơn đặt hàng mà họ đã đặt và nó sẽ không được chuyển đi. Nó còn nói rằng bạn sẽ không thể truy cập vào tài khoản của bạn hoặc đặt hàng với Amazon cho đến khi thông tin của bạn được xác nhận. Bên trong email là một liên kết độc hại đưa bạn đến trang Amazon giả mạo nơi bạn cần xác nhận thông tin của mình. Nó hỏi tên, địa chỉ và tất cả thông tin thẻ tín dụng của bạn”. Jones đề nghị gửi e-mail khả nghi để dừng việc giả mạo@amazon.com.

Theo Shepard (2017), lừa đảo trực tuyến ở Amazon đang gia tăng.

Để thảo luận về tấn công giả mạo là gì và cách nhận biết nó, truy cập ehow.com/how\_2003277\_yahoo-mesbah-scam.html. Xem thêm www.phishing.org/phishing- techniques để biết cách hoạt động của tấn công giả mạo. Các công ty chống tấn công giả mạo cung cấp các báo cáo (xem APWG 2016). Các báo cáo hàng quý bao gồm tổng thể về tấn công giả mạo với các số liệu thống kê và các dự báo. Casti (2014) mô tả một trò lừa đảo tấn công giả mạo trên Netflix nơi người dùng bị lừa liên hệ với đại diện của một dịch vụ khách hàng giả mạo và bàn giao dữ liệu tài khoản cá nhân. Những kẻ lừa đảo hiện đã nhắm mục tiêu vào nhiều công ty khác, chẳng hạn như AT & T và Comcast, bằng cách thu hút người dùng đến các trang web giả mạo thông qua quảng cáo được tài trợ. Đối với các cuộc tấn công lừa đảo năm 2015, xem Lemos (2016). Xem thêm Forrest (2016) để biết lý do tại sao tấn công giả mạo ngày càng nguy hiểm.

Bán thông tin bị đánh cắp, như bán bất kỳ hàng hóa bị đánh cắp, có thể sinh lợi ích xấu và không thể bị ngăn chặn.

**Ví dụ: Vi phạm an ninh mục tiêu**

Vi phạm bảo mật Target Corp 2013, nơi hàng triệu khách hàng bị đánh cắp dữ liệu thẻ ghi nợ và thẻ tín dụng, được bắt đầu như một cuộc tấn công giả mạo (xem Schwartz 2014). Các tin tặc đã sử dụng thông tin đăng nhập của một nhân viên của một trong những nhà cung cấp Target, để có quyền truy cập vào hệ thống bảo mật Target, và cài đặt phần mềm độc hại cho mục đích truy cập dữ liệu của mỗi thẻ được sử dụng. Một nhân viên Target sẽ quẹt thẻ khách hàng và phần mềm độc hại đã cài đặt sẽ lấy được số thẻ tín dụng của người mua sắm. Khi tin tặc có được quyền truy cập vào dữ liệu, chúng có thể đánh cắp 40 triệu số thẻ tín dụng và thẻ ghi nợ, và 70 triệu địa chỉ, số điện thoại và các thông tin cá nhân khác. Để xem tổng quan về cách các tin tặc đột nhập và làm thế nào Target có thể ngăn chặn vụ hack, xem Smith (2014).

**Spear phishing**

**Spear phishing** là một biến thể của tấn công giả mạo nhắm vào các nạn nhân bằng e-mail đến từ đồng nghiệp, hoặc thành viên gia đình hoặc bạn bè. Ví dụ, một vụ spear phishing nổi tiếng là một vụ bạn nhận được từ một người bạn nói với bạn rằng cô ấy đang ở một quốc gia khác và cô ấy đã bị cướp ví. Sau đó, cô ấy ngỏ ý nhờ bạn mua hộ một vé để cô ấy có thể trở về nhà và sẽ trả lại tiền cho bạn sau. Theo Perret (2016), có sự gia tăng đáng kể trong các cuộc tấn công như vậy, đặc biệt là đối với các doanh nghiệp. Một ví dụ khác là bạn có thể nhận được một e-mail, được cho là từ sếp của bạn, người đang đi du lịch, để chuyển tiền cho một “khách hàng” ở Hàn Quốc hoặc gửi cho sếp của họ danh sách khách hàng qua e-mail. Perret (2016) trình bày các giải pháp khả thi cho cả phishing và spear phishing. Để biết 10 vụ tấn công giả mạo hàng đầu, hãy xem secpoint.com/top-10-spam-attacks.html. Jones (2016c) báo cáo rằng Fancy Bear của Nga đã nhắm vào Ủy ban Quốc gia Dân chủ, đã phát động một cuộc tấn công spear phsshing và khai thác lỗ hổng trong Adobe Flash và Microsoft Windows.

***Các phương pháp tấn công giả mạo khác***

Bisson (2016) liệt kê thêm một số phương pháp tấn công sau: deceptive phishing, CEO fraud, Dropbox phishing, Google Docs phishing. Bisson cũng cung cấp các biện pháp bảo vệ.

***Pharming***

Giống như phishing, pharming là một hình thức lừa đảo qua mạng trong đó mã độc được cài đặt trên máy tính được sử dụng để chuyển hướng nạn nhân đến các trang web không có thật mà không có sự hiểu biết hoặc mong muốn của nạn nhân. Pharming có thể nguy hiểm hơn phishing vì người dùng không biết họ đã được chuyển đến một trang web giả mạo. Pharming được hướng tới các nhóm lớn người dùng cùng một lúc thông qua việc giả mạo tên miền. Pharming có thể được sử dụng để lừa đảo nhận dạng (thảo luận trong phần sau). Để biết thêm chi tiết, xem en.wikipedia.org/wiki/Pharming.

**Lừa đảo (Fraud) và các hình thức lừa đảo trực tuyến (Scams)**

Các khách hàng tiềm năng liệt kê “Các rủi ro ngầm của lừa đảo trực tuyến” và “Sự nghi ngờ của các thương nhân trực tuyến mà bạn không biết” là những lý do chính khiến họ không mua sắm trực tuyến.

Tấn công giả mạo (phishing) có thể dẫn đến nhiều hình thức lừa đảo trực tuyến. Thị trường EC, nơi mà người mua và người bán không thể nhìn thấy nhau, tạo điều kiện cho lừa đảo trực tuyến. Có nhiều hình thức lừa đảo trên mạng (xem fbi.gov/scams-and-safe/common-fraud-scheme/iNET-fraud). Lừa đảo là một vấn đề đối với các nhà bán lẻ và các khách hàng trực tuyến. May mắn thay, mặc dù thiệt hại thực tế trên mỗi sự cố đang tăng lên nhưng đã có ít sự cố hơn xảy ra, do đó tổng thiệt hại có lẽ sẽ giảm. Truy cập dmoz.org/Society/Issues/Fraud/Internet để có một cái nhìn toàn diện về các nguồn lừa đảo trực tuyến. Các cuộ tấn lông lừa đảo trực tuyến trên các thiết bị di động đang phát triển khá nhanh; xem Damri (2016). Để thảo luận, xem phần “Consumer and Seller Protection from Online Fraud”.

**Ví dụ về tấn công lừa đảo trực tuyến thông thường**

Sau đây là một số cuộc tấn công lừa đảo qua mạng đặc trưng xảy ra trên Internet.

* Khi một trong những tác giả của cuốn sách này quảng cáo trực tuyến rằng anh ta có một căn nhà để cho thuê, một số “bác sĩ” và “y tá” giả vờ đến từ Vương quốc Anh và Nam Mỹ đã áp dụng. Họ đồng ý trả giá cao cho một hợp đồng thuê ngắn hạn và nói họ sẽ trả bằng séc thu ngân. Họ hỏi liệu tác giả có chấp nhận ghi tiền trả từ

$ 6000 đến $ 10.000 và gửi lại cho họ số dư $ 4000 đến $ 8000 hay không. Khi biết rằng không có vấn đề gì, nhưng số dư sẽ chỉ được trả lại ngay khi séc của họ bị xóa, không ai trong số những người thuê nhà sẽ theo dõi.

* Các tổ chức tống tiền ở Anh và Nga đã tống tiền hàng trăm ngàn đô la từ các trang web cá cược thể thao trực tuyến. Một vài trang web đã từ chối thanh toán phí bảo kê của thành phố đã bị đe dọa bởi các cuộc tấn công DoS.

Xem video “Cách tin tặc xâm nhập vào ngôi nhà của bạn” (2:26), truy cập money.cnn.com/video/technology/2013/08/14/t-hack-my-baby-monitor-and house.cnnmoney.

Để thảo luận về social engineering, tấn công giả mạo phishing và các phương pháp lừa đảo lấy cắp thông tin trực tuyến khác, xem Pontrioli (2013).

**Các kiểu lừa đảo trực tuyến**

Dưới đây là một số hình thức tiêu biểu của lừa đảo trực tuyến (theo Spamlaws, xem spamlaws.com/scams.html): lừa đảo bằng bài viết, lừa đảo thuế, lừa đảo qua thư điện tử, lừa đảo xổ số, lừa đảo người Negiria (hay lừa đảo “419”), lừa đảo thẻ tín dụng (nhiều loại), lừa đảo giúp việc tại nhà, lừa đảo email IRS, và lừa đảo các dịp miễn phí. Truy cập fbi.gov/scams-safe/fraud/iNET\_fraud để biết thêm.

**Lừa đảo trực tuyến qua thư điện tử**

Lừa đảo qua email là một kiểu lừa đảo phổ biến vì email rất dễ để mắc bẫy. Trung tâm thông tin về các giống chó đăng các ví dụ phổ biến tại (dogbreedinfo.com/iNETfraud/scamemailexamples.html). Các ví dụ vừa mang tính giáo dục vừa mang tính giải trí. Nguy hiểm nhất là các email lừa đảo trông giống như chúng đến từ các tổ chức nổi tiếng (ngân hàng, công ty viễn thông) cho bạn biết rằng bạn phải cung cấp thông tin để giữ cho tài khoản của bạn hoạt động. Một ví dụ về e-mail được gửi bởi Yahoo! được cung cấp dưới đây.

**TÀI KHOẢN YAHOO**

Thông báo xác minh !!! (KMM69467VL55834KM)

Kính gửi thành viên

Do sự tắc nghẽn trong tất cả các tài khoản Yahoo, Yahoo sẽ tắt tất cả các tài khoản không sử dụng. Bạn cần xác nhận e-mail của bạn bằng cách điền thông tin đăng nhập của bạn bên dưới sau khi nhấp vào nút trả lời, hoặc tài khoản của bạn sẽ bị đình chỉ trong vòng 24 h vì lý do an ninh.

**Yahoo! ID**

Tên:.........................................

Yahoo! ID:..................................

Địa chỉ thư Yahoo!:..................

Mật khẩu:....................................

Thông tin thành viên

Giới tính: .......................................

Ngày sinh:..................................

Nghề nghiệp: .................................

Quốc gia:......................................

Nếu bạn là một thuê bao tài khoản Yahoo! Premium, chúng tôi sẽ hoàn trả phần chưa sử dụng của thuê bao Premium của bạn. Các hoàn trả sẽ xuất hiện dưới dạng tín dụng thông qua phương thức thanh toán mà chúng tôi cung cấp trong hồ sơ cho bạn. Vì vậy, hãy chắc chắn rằng thông tin thnh toán của bạn là chính xác và mới nhất. Để biết thêm thông tin, vui lòng truy cập Payment.mail.yahoo.com.

Sau khi làm theo hướng dẫn trên đây, tài khoản của bạn sẽ không bị gián đoạn và sẽ tiếp tục như bình thường.

Chúng tôi quan tâm tài khoản Yahoo! của bạn.

Trân trọng,

Hỗ trợ khách hàng Yahoo!

Bất kỳ e-mail nào bạn nhận được yêu cầu thông tin cá nhân rất có thể là một sự xâm nhập hoặc lừa đảo vì một tổ chức hợp pháp sẽ có tất cả thông tin cá nhân của bạn. Đối với lời khuyên từ Yahoo! về cách tự bảo vệ mình trực tuyến, xem Yahoo! Safety (safe.yahoo.com).

**Top 10 cuộc tấn công và các biện pháp khắc phục**

Trang web bảo mật CNTT SecPoint.com cung cấp danh sách top 10 cuộc tấn công liên quan đến bảo mật theo các chủ đề sau: virus, phần mềm gián điệp, thư rác, sâu, lừa đảo trực tuyến, tin tặc tấn công, và tin tặc và các chiến thuật kỹ thuật xã hội. Ngoài ra, trang này cung cấp các trang liên quan về tài nguyên bảo mật CNTT như 10 tin tặc hàng đầu; mười mẹo và công cụ bảo mật hàng đầu; các trang liên quan đến chống lừa đảo, chống DoS, chống thư rác, v.v. Để biết các tài nguyên CNTT của Secpoint cho 10 cuộc tấn công thư rác hàng đầu, hãy xem secpoint.com/Top-10-Spam-Attacks.html.

**Ăn cắp danh tính và gian lận danh tính**

**Ăn cắp danh tính**, theo trang web của Bộ Tư pháp Hoa Kỳ, là một hành vi phạm pháp. Nó đề cập đến việc lấy và sử dụng sai danh tính của người khác theo một cách nào đó để thực hiện các tội ác liên quan đến gian lận hoặc lừa đảo (ví dụ: vì lợi ích kinh tế). Nạn nhân có thể bị thiệt hại nghiêm trọng. Ở nhiều quốc gia, việc giả mạo danh tính người khác là phạm pháp. Theo Ủy ban Thương mại Liên bang Hoa Kỳ (ftc.gov), hành vi trộm cắp danh tính là một trong những mối quan tâm chính của người mua sắm trực tuyến. Theo thống kê của Safe Smart Living, hành vi trộm cắp danh tính ảnh hưởng đến hơn 12 triệu người Mỹ mỗi năm, (2015) vì mất hơn 55 tỷ USD và đang tăng khoảng 20% mỗi năm. Theo Alt (2016), hơn 1 tỷ hồ sơ bị rò rỉ đã ảnh hưởng đến 500.000 nạn nhân vào tháng 6 năm 2014. Kẻ trộm danh tính thu về 5,8 tỷ USD mỗi năm. Ngoài ra, có 19 người trở thành nạn nhân của hành vi trộm cắp danh tính mỗi phút. Cuối cùng, trẻ con là con mồi dễ dàng. Để xem một bộ phim hài giải trí, hãy xem “Kẻ trộm danh tính năm 2013”.

**Ví dụ**

Theo Constantin (2016a), vào tháng 1 năm 2016, những kẻ trộm danh tính đã đánh cắp 100.000 số an sinh xã hội và các dữ liệu cá nhân khác từ các tập tin IRS của Hoa Kỳ.

**Gian lận danh tính**

Gian lận danh tính đề cập đến việc giả mạo danh tính của người khác hoặc tạo ra một người hư cấu và sau đó sử dụng danh tính bất hợp pháp để phạm tội. Các hoạt động tiêu biểu bao gồm:

* Mở tài khoản thẻ tín dụng bằng tên nạn nhân
* Mua hàng bằng cách sử dụng danh tính giả (ví dụ: sử dụng danh tính khác để mua hàng hóa)
* Những kẻ trộm cắp danh tính doanh nghiệp đang sử dụng một tên doanh nghiệp khác để lấy tín dụng hoặc tham gia vào quan hệ đối tác
* Đóng giả làm người khác để phạm tội
* Tiến hành rửa tiền (ví dụ: tội phạm có tổ chức) bằng cách sử dụng danh tính giả.

**Cướp ngân hàng điện tử**

Tấn công mạng có thể xảy ra với các cá nhân và các tổ chức, bao gồm cả những ngân hàng.

**Ví dụ**

Secureworks.com đã phát hiện ra các hoạt động gian lận kiểm tra sau: Tội phạm mạng Nga đã sử dụng “những con lừa” (những người nghĩ rằng họ đang làm một công việc hợp pháp), 2000 máy tính và các phương pháp hack tinh vi để đánh cắp hình ảnh kiểm tra lưu trữ từ năm công ty và thu thập hình ảnh tiền ở nước ngoài.

Tiếp theo, những kẻ lừa đảo đã in séc giả, mà các con lừa sẽ gửi tiền vào tài khoản của chính họ. Sau đó, các con lừa được lệnh chuyển tiền đến một ngân hàng ở Nga. Những “con lừa”, như thường lệ, là những người vô tội được thuê và trả tiền để thực hiện việc chuyển nhượng. Một số con lừa đã trở nên nghi ngờ và đã báo cáo vụ lừa đảo cho chính quyền.

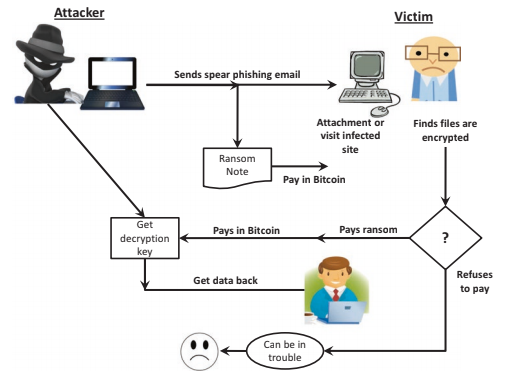
**Mã độc tống tiền**

Các chương trình mã độc mã hóa tập tin đã trở thành một trong những mối đe dọa lớn nhất đối với các tổ chức mạng. Thật không may, các chương trình mã độc liên tục phát triển và ngày càng tinh vi hơn. Một số người tin rằng mã độc tống tiền đang trở thành một dịch bệnh (Greengard 2016b). Trường hợp mở đầu là một ví dụ về một cuộc tấn công. Theo Fitzpatrick và Griffin (2016), FBI đã nhận được 2453 khiếu nại trong năm 2015, trong đó các nạn nhân đã trả 24 triệu đô la tiền chuộc. Năm 2016/2017, mức độ nghiêm trọng của vấn đề còn lớn hơn nhiều. Ví dụ, công ty bảo mật Malwarebytes đã kiểm tra hơn 50.000 sự cố và thấy rằng Las Vegas là khu vực bị tấn công nhiều nhất ở Hoa Kỳ (tính theo đầu người).

**Mã độc là gì?**

Một cách tổng quát, bọn tội phạm mã hóa và khóa các tệp kỹ thuật số bằng cách sử dụng phần mềm độc hại và yêu cầu tiền chuộc trước khi hệ thống được mở khóa.

Quá trình của cài đặt mã độc được minh họa trong hình 11.7.



*Hình 11.7 Quá trình xâm nhập bằng mã độc*

Các tin tặc có thể gửi cho nạn nhân e-mail với tệp được đính kèm. Sử dụng spear phishing hoặc các kỹ thuật lừa đảo xã hội khác, họ thuyết phục người dùng mở tệp đính kèm có virus đó. Vài giờ sau, tất cả các tệp được bảo vệ lỏng lẻo sẽ bị mã hóa. Dữ liệu trong các tệp sau đó bị bắt làm con tin và yêu cầu tiền chuộc được đưa ra.

Giá giải mã được yêu cầu bởi kẻ đã cài mã độc được tính trên mỗi hệ thống bị khóa. Thanh toán thường được thực hiện bằng Bitcoin (Chương 12). Các nạn nhân cần lấy khóa giải mã cho các hệ thống bị xâm nhập. Nếu không, các phần mềm mã độc có thể lây lan rộng hơn nữa. Do đó, cần phải phát hiện phần mềm độc hại càng sớm càng tốt trước khi nó phát tán bên trong mạng, ảnh hưởng đến nhiều hệ thống khác.

**Các biện pháp khả thi**

Các biện pháp rõ ràng nhất là có một gói phần mềm chống vi-rút tốt, sao lưu dữ liệu tốt và người dùng được đào tạo tốt. Những giải pháp này là tốt, nhưng chúng có thể không ngăn chặn được tất cả các tin tặc. Hầu hết các nhà cung cấp bảo mật cung cấp giải pháp bổ sung và lời khuyên bảo mật. Ví dụ: Tripwire cung cấp 22 mẹo phòng ngừa ransomware tại [tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevent-tips](file:///C:\Users\QUANGTHAI\Desktop\tripwire.com\state-of-security\security-data-protection\cyber-security\22-ransomware-prevent-tips).

Mello Jr. (2017) cung cấp tổng quan về vấn đề và thảo luận về các giải pháp. Để có sách điện tử miễn phí năm 2016, xem Staff (2016b).

Hassell (2016) cũng gợi ý một số phương pháp để chống lại mã độc. Tương lai có vẻ tươi sáng hơn. Ngành công nghiệp bảo mật đang tìm những cách mới để chặn các phần mềm mã độc. Ví dụ, theo Constantin (2016b), học máy (Chương 7) có thể giúp các công ty phản ứng nhanh hơn với mã độc. Phương pháp AI này có thể cải thiện đáng kể thời gian phát hiện và phản ứng của mã độc, cho phép ngăn chặn sự lây lan nhanh chóng của phần mềm độc hại trong các tổ chức.

Một cuốn sách điện tử đặc biệt toàn diện (2016) được miễn phí từ Symantec. Bạn có thể nhận nó từ symantec.com/content/en/us/enterprise/media/security\_response/whitepapers/ISTR2016\_Ransomware\_and\_Businesses.pdf.

**Ví dụ 1**

Ngay cả Tổng thống Hoa Kỳ cũng có thể bị ảnh hưởng bởi mã độc. Theo Constantin (2017), thì khoảng 70% trong số các máy ảnh được nối với hệ thống mạch kín (CCTV) của cảnh sát ở Washington D.C. được cho là không thể ghi lại cảnh quay trong vài ngày trước khi Tổng thống Donald Trump nhậm chức vì một cuộc tấn công của mã độc.

Vụ tấn công đã ảnh hưởng đến 123 trong số 187 máy quay video tạo thành hệ thống mạng camera quan sát thành phố. Mỗi thiết bị này được sử dụng để lưu trữ các cảnh quay video được ghi lại bởi tối đa bốn camera được cài đặt trong khu vực công cộng.

Vụ việc xảy ra vào ngày 12 tháng 1 năm 2017, tám ngày trước khi Tổng thống Trump nhậm chức và phải mất ba ngày để khôi phục hệ thống. Thành phố đã từ chối trả tiền chuộc và gửi các đội đến mỗi trang web để lấy các thiết bị bị ảnh hưởng, thay thế phần mềm của họ và khởi động lại chúng. Nếu tên tội phạm đủ thông minh và bắt đầu vụ việc 1 ngày trước khi khánh thành, thành phố sẽ có rất ít sự lựa chọn ngoài việc trả tiền chuộc hoặc khiến Tổng thống gặp rủi ro về an ninh.

**Ví dụ 2**

Ngay cả một công ty nhỏ cũng có thể bị tấn công. Bolton (2016) cung cấp một ví dụ về một hãng taxi nhỏ với 12 máy tính được nối mạng ở Đông London (Anh). Phần mềm độc hại xâm nhập hệ thống thông qua tệp đính kèm trong e-mail. Một nỗ lực để loại bỏ thủ phạm của Spy Hunter đã thất bại. Một khoản tiền chuộc 1,2 Bitcoin đã được yêu cầu. May mắn thay, công ty đang trong quá trình thay thế các PC cũ, vì vậy họ đã làm điều này và không trả tiền chuộc. Các đề xuất của Bolton cho các doanh nghiệp nhỏ là (1) có một máy quét e-mail và (2) sao lưu dữ liệu thường xuyên.

**Tấn công bằng thư rác**

Thư rác điện tử, còn được gọi là các mảnh thư điện tử hay chỉ đơn giản là thư rác, xảy ra khi các email gần như giống hệt nhau được gửi qua thư điện tử cho 1 số lượng lớn người nhận (đôi khi là hàng triệu email không được yêu cầu). Theo Symantec, hầu hết các tin nhắn trên một quy mô network lớn đều là thư rác. Gần 58% thư rác đến từ các con bot; con bot tồi tệ nhất được gọi là Dotnet. Ngày nay (2017) tình hình đã tốt hơn do việc lọc thư rác được cải thiện. Kẻ gửi thư rác có thể mua hàng triệu địa chỉ email và sau đó định dạng địa chỉ, cắt và dán thư và nhấn Gửi. Phần mềm e-mail tạo hàng loạt, gửi và tự động gửi thư rác được gọi là Ratware. Các tin nhắn có thể là quảng cáo (để mua sản phẩm), ý định lừa đảo hoặc chỉ là vi-rút gây phiền nhiễu. Để biết số liệu thống kê hiện tại về thư rác, hãy truy cập securelist.com/statistic. Securelist là một trang web toàn diện cũng cung cấp các mô tả về thư rác và vi-rút, bảng chú giải và thông tin về các mối đe dọa. Hơn 130 tỷ thư rác được gửi mỗi ngày vào năm 2013, nhưng tốc độ tăng trưởng này đã ổn định. Lưu ý rằng khoảng 80% tất cả thư rác được gửi bởi ít hơn 200 người gửi thư rác. Những kẻ gửi thư rác này đang sử dụng phần mềm gián điệp và các công cụ khác chủ yếu để gửi quảng cáo không mong muốn. Những kẻ gửi thư rác ngày càng thông minh và tinh vi hơn (ví dụ: xem Lệnh cấm 2015 để phân tích các trường hợp). Kỹ thuật thư rác thông minh đòi hỏi các công nghệ chống thư rác tiên tiến (Lệnh cấm 2015).

**Một vài ví dụ tiêu biểu về thư rác**

Mỗi tháng, Symantec cung cấp một báo cáo có tiêu đề là “Tình hình về thư rác: Một báo cáo hàng tháng”. Báo cáo cung cấp các ví dụ về các trò gian lận phổ biến hiện tại, các loại thư rác, quốc gia có nguồn gốc, khối lượng và nhiều hơn nữa.

**Phần mềm gián điệp**

**Phần mềm gián điệp** là phần mềm theo dõi được cài đặt bởi bọn tội phạm, không có sự đồng ý của người dùng, nhằm thu thập thông tin về người dùng và chuyển trực tiếp đến nhà quảng cáo hoặc các bên thứ ba khác. Sau khi cài đặt chương trình phần mềm gián điệp theo dõi và ghi lại các hoạt động của người dùng trên Internet. Phần mềm gián điệp có thể chứa mã độc chuyển hướng hoạt động trên trình duyệt Web. Phần mềm gián điệp cũng có thể làm chậm tốc độ lướt web và làm hỏng các chức năng của chương trình. Phần mềm gián điệp thường được cài đặt khi bạn tải xuống phần mềm miễn phí hoặc phần mềm chia sẻ. Để theo dõi tin tức và video có tiêu đề “Chính phủ Ethiopia cài gián điệp trong các tòa báo có trụ sở tại Hoa Kỳ (2:23 phút) về cách một số chế độ sử dụng phần mềm gián điệp chống lại các nhà báo, xem Timberg (2014).

**Mạng xã hội khiến tấn công bằng kỹ thuật xã hội dễ dàng hơn**

Theo một nghiên cứu của công ty bảo mật CNTT thuộc sở hữu của Đan Mạch, CSIS cho biết, các trang web mạng xã hội là khu vực dễ bị xâm nhập và “màu mỡ” để tin tặc chiếm được sự tin tưởng của người dùng.

**Cách tin tặc tấn công mạng xã hội**

Tin tặc đang khai thác môi trường đáng tin cậy của các mạng xã hội có chứa thông tin cá nhân (đặc biệt là Facebook) để khởi động các cuộc tấn công kỹ thuật xã hội khác nhau. Thật không may, nhiều trang mạng xã hội có các biện pháp kiểm soát bảo mật kém. Xu hướng sử dụng các trang web mạng xã hội ngày càng tăng chính là nền tảng cho việc đánh cắp dữ liệu cá nhân của người dùng.

**Ví dụ**

Dưới đây là một số ví dụ trong vấn đề bảo mật của các trang mạng xã hội:

* Người dùng có thể vô tình chèn mã độc vào trang hồ sơ cá nhân hoặc thậm chí là danh sách bạn bè của họ.
* Hầu hết các biện pháp chống thư rác không thể phân biệt giữa các yêu cầu thực tế và yêu cầu phạm tội để kết nối với mạng. Điều này cho phép bọn tội phạm có được thông tin cá nhân về các thành viên trong mạng.
* Facebook và các trang mạng xã hội phổ biến khác cung cấp các ứng dụng miễn phí, hữu ích, hấp dẫn. Những ứng dụng này có thể đã được xây dựng bởi các nhà phát triển sử dụng bảo mật yếu.
* Kẻ lừa đảo có thể tạo hồ sơ giả và sử dụng nó trong một vụ tấn công giả mạo trực tuyến.

**Thư rác trong mạng xã hội và trong môi trường web 2.0**

Mạng xã hội thu hút những nguồn gửi thư rác do số lượng lớn người nhận tiềm năng và nền tảng mạng xã hội và Internet kém an toàn hơn. Kẻ gửi thư rác thích tấn công Facebook nói riêng. Một vấn đề khác là các bình luận rác trong các blog (blog spam).

***Blog spam tự động***

Các blogger bị spam bởi các quảng cáo được tạo tự động (một số là thật và một số là giả) cho các mặt hàng từ thảo dược Viagra đến các nhà cung cấp cờ bạc. Người viết blog có thể sử dụng các công cụ để đảm bảo rằng con người chứ không phải một hệ thống tự động đăng bài đã bình luận các vấn đề trên blog của họ.

**Kết quả rác từ các công cụ tìm kiếm và bình luận rác của các blog**

Công cụ tìm kiếm spam là một công nghệ cho phép tạo ra các trang được gọi là trang spam để lừa các công cụ tìm kiếm cung cấp kết quả tìm kiếm sai lệch để xếp hạng của các trang nhất định bị thổi phồng. Một chiến thuật tương tự liên quan đến việc sử dụng các splog (viết tắt của các trang blog spam), đó là các blog được tạo bởi những kẻ gửi thư rác chỉ để quảng cáo. Kẻ gửi thư rác tạo ra nhiều splog và liên kết chúng với các trang web của những người trả tiền cho anh ta (cô ta) để tăng thứ hạng trang nhất định. Như bạn có thể nhớ lại từ chương 10, các công ty đang tìm kiếm tối ưu hóa công cụ tìm kiếm (SEO), được thực hiện một cách phi đạo đức bằng các kỹ thuật trên.

**Ví dụ**

Một vài ví dụ về tấn công bằng thư rác trong mạng xã hội là:

* Tin nhắn khẩn cấp trong các mạng xã hội thường dễ bị tấn công bởi thư rác.
* King (2016) mô tả các cuộc tấn công lừa đảo trên các mạng xã hội lớn (Facebook, Twitter, LinkedIn). Những cuộc tấn công này đã tăng 150% trong 1 năm.

King đã liệt kê 5 ví dụ sau đây:

1. Dịch vụ tài khoản khách hàng giả trên Twitter
2. Bình luận giả trên các bài đăng phổ biến
3. Video livestream giả
4. Giảm giá trực tuyến giả
5. Khảo sát và các cuộc thi trực tuyến giả

**Vi phạm dữ liệu (rò rỉ)**

**Vi phạm dữ liệu** (còn được gọi là rò rỉ dữ liệu hoặc mất dữ liệu) là một sự cố bảo mật trong đó dữ liệu được lấy bất hợp pháp và sau đó được công bố hoặc xử lý. Có nhiều mục đích cho các vi phạm dữ liệu. Chẳng hạn, một người trong quân đội Hoa Kỳ đã sử dụng USB để tải thông tin mật và sau đó đăng thông tin bị đánh cắp lên Internet. Để biết các trình điều khiển vi phạm dữ liệu và cách tự bảo vệ bản thân, hãy xem Goldman (2014b). Đối với các vi phạm dữ liệu đáng sợ nhất, xem TechRepublic Staff (2015).

Các cuộc thảo luận cho đến nay đã tập trung vào các cuộc tấn công. Các cơ chế bảo vệ, bao gồm cả các cơ chế liên quan đến thư rác và các tội phạm mạng khác, được cung cấp trong phần “Defending Information Systems and E-Commerce Including Mobile Systems”. Đầu tiên, chúng ta hãy kiểm tra những gì liên quan đến việc đảm bảo an toàn thông tin.

**Phần 11.4 Câu hỏi ôn tập**

1. Định nghĩa tấn công giả mạo (phishing).
2. Mô tả mối quan hệ của tấn công giả mạo với lừa đảo tài chính.
3. Mô tả ngắn gọn một số chiến thuật tấn công giả mạo.
4. Định nghĩa pharming.
5. Định nghĩa thư rác và các phương pháp của nó.
6. Định nghĩa splog và giải thích cách các splogger kiếm tiền.
7. Tại sao và làm thế nào các mạng xã hội bị tấn công?
8. Mô tả vi phạm dữ liệu (rò rỉ dữ liệu).
9. Mô tả quá trình xâm nhập bằng mã độc tống tiền.

**11.5 Mô hình đảm bảo thông tin và chiến luợc phòng chống**

Mô hình đảm bảo thông tin (IA), được gọi là bộ ba bảo mật CIA, là một điểm tham chiếu được sử dụng để xác định vấn đề các lĩnh vực và đánh giá an ninh thông tin của một tổ chức. Việc sử dụng mô hình bao gồm ba thuộc tính cần thiết: bảo mật, toàn vẹn và tính khả dụng, Mô hình này được mô tả tiếp theo. (Để thảo luận, hãy xem  [whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA](file:///C:\Users\QUANGTHAI\Desktop\whatis.techtarget.com\definition\Confidentiality-integrity-and-availability-CIA))

Lưu ý: Mô hình đảm bảo có thể được điều chỉnh phù hợp với một số hoạt động EC. Ví dụ: đảm bảo chuỗi cung ứng EC là quan trọng.

**Bảo mật, toàn vẹn và tính khả dụng**

Sự thành công và bảo mật của EC có thể được đo lường bằng các thuộc tính sau:

1. Bảo mật là sự đảm bảo bí mật dữ liệu và quyền riêng tư. Cụ thể, dữ liệu chỉ được tiết lộ cho những người được ủy quyền. Bảo mật đạt được bằng cách sử dụng một số phương pháp, chẳng hạn như mã hóa và mật khẩu.
2. Tính toàn vẹn là sự đảm bảo rằng dữ liệu là chính xác và chúng không thể bị thay đổi. Thuộc tính toàn vẹn cần phải là có thể phát hiện và ngăn chặn việc tạo, sửa đổi hoặc xóa dữ liệu hoặc tin nhắn trái phép trong quá trình.
3. Tính khả dụng là sự đảm bảo rằng quyền truy cập vào bất kỳ dữ liệu, trang web thông tin hoặc các dịch vụ EC khác có liên quan sử dụng có sẵn trong thời gian thực, bất cứ khi nào và bất cứ nơi nào cần thiết. Các thông tin phải đáng tin cậy.

**Xác thực, ủy quyền và không bác bỏ**

Ba khái niệm có liên quan đến mô hình IA: xác thực, ủy quyền và không tính toán. Những khái niệm quan trọng là:

* Xác thực là một biện pháp bảo mật đảm bảo rằng thông tin dữ liệu, người tham gia và giao dịch ECD và tất cả các đối tượng liên quan đến EC khác là hợp lệ. Xác thực yêu cầu xác minh. Ví dụ, một người có thể được xác thực bởi một cái gì đó anh ta biết (ví dụ: mật khẩu), thứ gì đó anh ta sở hữu (ví dụ: mã thông báo nhập cảnh) hoặc thứ gì đó duy nhất để người đó (ví dụ: dấu vân tay).
* Ủy quyền yêu cầu so sánh thông tin được cung cấp bởi một người hoặc một chương trình trong khi đăng nhập với thông tin được lưu trữ liên quan đến quyền truy cập được yêu cầu.
* Không bác bỏ là khái niệm đảm bảo rằng một bên trong giao dịch EC không thể từ chối (hoặc bác bỏ) tính hợp lệ của một hợp đồng EC và cô ấy hoặc anh ấy sẽ thực hiện nghĩa vụ của họ trong các giao dịch.Theo bảng chú giải thuật ngữ của hệ thống bảo mật thông tin quốc gia (INFOSEC), không bác bỏ là “sự bảo đảm của người gửi dữ liệu được cung cấp bằng chứng giao hàng và người nhận được cung cấp bằng chứng về danh tính người gửi, để sau này không thể từ chối xử lý dữ liệu.”

**Lưu ý**: Xem danh sách các thuật ngữ chính trong phần “Các vấn đề và cảnh quan an ninh thương mại điện tử cơ bản”. Một số nguồn liệt kê thêm các khái niệm (ví dụ: Techopedia).

Để đảm bảo các thuộc tính này, thương mại điện tử áp dụng các công nghệ như mã hóa, chữ ký số và chứng nhận. Ví dụ, việc sử dụng chữ ký số khiến mọi người khó từ chối sự tham gia của họ trong giao dịch EC. Trong thương mại điện tử, các phương pháp mới hoặc cải tiến để đảm bảo tính bảo mật của số thẻ tín dụng, tính toàn vẹn của các tin nhắn liên quan đến giao dịch, xác thực người mua và người bán và các giao dịch không bác bỏ cần được cập nhật liên tục khi các phương thức cũ trở nên lỗi thời.

**Chiến lược an ninh thương mại điện tử**

Bảo mật EC cần giải quyết mô hình IA và các thành phần của nó. Trong hình 11.7, một khung bảo mật EC xác định các loại đảm bảo mức cao và các điều khiển của chúng được trình bày. Các danh mục chính là các hoạt dộng quy định, tài chính và tiếp thị. Chỉ các khu vực chính được liệt kê trong hình.

**Bảo vệ các hệ thống EC**

Chúng tôi tổ chức bảo vệ thành tám loại:

1. Bảo vệ quyền truy cập vào hệ thống máy tính, luồng dữ liệu và giao dịch EC. Điều này bao gồm ba chủ đề: Truy cập kiểm soát (bao gồm sinh trắc học), mã hóa nội dung và cơ sở hạ tầng khóa công khai (PKI). Dòng bảo vệ này cung cấp bảo vệ toàn diện khi áp dụng cùng nhau. Kẻ xâm nhập phá vỡ kiểm soát truy cập sẽ đối mặt với tài liệu được mã hóa ngay cả khi chúng vượt qua tường lửa.
2. Mạng EC bảo vệ. Điều này bao gồm chủ yếu bảo vệ bởi tường lửa. Tường lửa cô lập mạng công ty và các thiết bị điện toán từ Internet được bảo mật kém. Để làm cho Internet an toàn hơn, chúng ta có thể sử dụng mạng riêng ảo. Ngoài các biện pháp này, nên sử dụng các hệ thống phát hiện xâm nhập. Một bảo vệ mạng có nghĩa là bảo mật e-mail đến, thường không được mã hóa. Nó cũng là cần thiết để bảo vệ chống lại virus và phần mềm độc hại khác được truyền qua mạng.
3. Điều khiển chung, hành chính và ứng dụng. Đây là một loạt các biện pháp bảo vệ nhằm bảo vệ tính toán tài sản bằng cách thiết lập các hướng dẫn, kiểm tra thủ tục, v.v.
4. Bảo vệ chống lại kỹ thuật xã hội và gian lận. Một số phương pháp bảo vệ được sử dụng để chống spam, lừa đảo và phần mềm gián điệp.
5. Chuẩn bị cho thiên tai, kinh doanh liên tục và quản lý rủi ro. Những chủ đề này là vấn đề quản lý được hỗ trợ bởi phần mềm.
6. Thực hiện các chương trình bảo mật toàn doanh nghiệp. Để triển khai các phương pháp phòng thủ nói trên, người ta cần phải sử dụng chiến lược thực hiện phù hợp.
7. Tiến hành đánh giá lỗ hổng và kiểm tra thâm nhập. (Xem văn bản sau.)
8. Sao lưu dữ liệu.

Để có phạm vi bảo hiểm toàn diện về tất cả các khía cạnh của bảo vệ thông tin, xem Harwood (2015).

Để thực hiện bảo vệ trên, trước tiên hãy tiến hành một số đánh giá và sau đó lập kế hoạch và thực hiện. Hai hoạt động có thể là đánh giá lỗ hổng và kiểm tra thâm nhập.

**Đánh giá lỗ hổng và nhu cầu bảo mật**

Một nhiệm vụ chính trong chiến lược bảo mật là tìm ra những điểm yếu và điểm mạnh của các chiến lược và giải pháp bảo mật hiện có. Điều này là một phần của đánh giá rủi ro và có thể được thực hiện theo những cách khác nhau. Đây là hai gợi ý đại diện:

1. Tiến hành đánh giá lỗ hổng của hệ thống EC của bạn. Đánh giá lỗ hổng là một quá trình xác định và đánh giá các khu vực có vấn đề dễ bị tấn công trên hệ thống máy tính. Hệ thống EC bao gồm đặt hàng trực tuyến, mạng truyền thông, cổng thanh toán, cơ sở dữ liệu sản phẩm, chống gian lận, v.v. Các lỗ hổng nghiêm trọng nhất là những lỗ hổng có thể làm gián đoạn hoặc đóng cửa doanh nghiệp. Ví dụ, một DoS có thể ngăn chặn việc lấy đơn hàng; một cuộc tấn công virus có thể ngăn chặn giao tiếp. Việc đánh giá sẽ xác định sự cần thiết và ưu tiên của các cơ chế phòng thủ. Cho một tổng quan về đánh giá lỗ hổng bao gồm cả quá trình, [searchmidmarketsecurity.techtarget.com/definition/ vulnerability-analysis.](file:///C:\Users\QUANGTHAI\Desktop\searchmidmarketsecurity.techtarget.com\definition\%20vulnerability-analysis)
2. Tiến hành kiểm tra thâm nhập (pen) (có thể được thực hiện bằng cách thuê các hacker) để tìm các lỗ hổng và bảo mật điểm yếu của một hệ thống. Các thử nghiệm này được thiết kế để mô phỏng các cuộc tấn công bên ngoài. Điều này cũng được gọi là kiểm thử hộp đen. Ngược lại, các công ty phát triển phần mềm tiến hành thử nghiệm chuyên sâu về hộp trắng, có liên quan đến việc cẩn thận kiểm tra hệ thống của cả hai phần cứng và phần mềm. Các loại thử nghiệm thâm nhập khác bao gồm nhắn tin mục tiêu, kiểm thử mù, kiểm thử mù đôi.

**Kiểm tra sự xâm nhập**

Một bài kiểm tra thâm nhập (pen test)là một phương pháp đánh giá lỗ hổng của hệ thống máy tính. Nó có thể được thực hiện bằng tay, bởi cho phép các chuyên gia hoạt động như tin tặc để mô phỏng các cuộc tấn công độc hại. Quá trình kiểm tra các điểm yếu (dễ bị tổn thương) mà kẻ tấn công có thể tìm và khai thác. Bất kỳ điểm yếu nào được phát hiện đều được trình bày cho quản lý, cùng với tiềm năng tác động và một giải pháp đề xuất. Một bài kiểm tra bút có thể là một bước trong kiểm toán bảo mật toàn diện. Một số phương pháp có thể được sử dụng để thực hiện kiểm tra bút (ví dụ: quy trình tự động). Ngoài ra, nhiều công cụ phần mềm có sẵn vì mục đích này. Để xem xét và hướng dẫn, hãy xem [pen-tests.com](file:///C:\Users\QUANGTHAI\Desktop\pen-tests.com) và [coresecurity.com/penetration-testing-overview](file:///C:\Users\QUANGTHAI\Desktop\coresecurity.com\penetration-testing-overview).Thông tin thêm về các bài kiểm tra thâm nhập, xem Maxwell (2016).

**PHẦN 11.5 CÂU HỎI THƯỜNG GẶP**

1. Đảm bảo thông tin là gì? Liệt kê các thành phần chính của nó.
2. Xác định tính bảo mật, tính toàn vẹn và tính sẵn sàng.
3. Xác định xác thực, ủy quyền và không bác bỏ.
4. Liệt kê các mục tiêu của chiến lược EC.
5. Liệt kê tám loại bảo vệ trong các hệ thống EC.
6. Mô tả đánh giá lỗ hổng.
7. Kiểm tra thâm nhập là gì?

**11.6 CÁC HỆ THỐNG KHAI THÁC THÔNG TIN VÀ THƯƠNG MẠI ĐIỆN TỬ**

Hệ thống thông tin bảo vệ bất kể bản chất của chúng là tương tự nhau và được mô tả trong các cuốn sách CNTT chung (ví dụ: bởi Kim và Sa-lô-môn 2016).

Chúng tôi chỉ cung cấp những điểm nổi bật về bảo mật này, chia nó thành ba loại: (1) kiểm soát truy cập, mã hóa và PKI; (2) mạng lưới thương mại điện tử an ninh;(3) kiểm soát chung, spam, cửa sổ bật lên và kỹ thuật xã hội. Trong phần ”Bảo vệ người tiêu dùng và người bán khỏi gian lận trực tuyến” , chúng tôi mô tả sự bảo vệ gian lận.

Thông tin toàn diện về các mối đe dọa và phòng thủ an ninh mạng được Scott cung cấp trong một số tập có tiêu đề An ninh mạng 101. Tập 1 (Scott 2016a) bao gồm hầu hết các lĩnh vực phi kỹ thuật, trong khi Tập 2 (Scott 2016b) bao gồm hầu hết các lĩnh vực kỹ thuật.

Một cuốn sách toàn diện về phòng thủ chống lại các cuộc tấn công trên Web được cung cấp bởi Harwood (2015).

**Bảo vệ I: Kiểm soát truy cập, mã hóa và PKI**

Trong phần này, chúng tôi mô tả các chủ đề sau: phương pháp kiểm soát truy cập, hệ thống sinh trắc học, mã hóa và mã hóa PKI. Để biết tổng quan về khu vực phòng thủ này, hãy xem Cloud (2015).

**Kiểm soát truy cập**

Kiểm soát truy cập xác định ai (người, chương trình hoặc máy) có thể sử dụng hợp pháp tài nguyên điện toán của tổ chức (tài nguyên nào, khi nào và như thế nào).

***Ủy quyền và Xác thực***

Kiểm soát truy cập liên quan đến ủy quyền (có quyền truy cập) và xác thực, còn được gọi là nhận dạng người dùng (ID người dùng), tức là, chứng minh rằng người dùng là người mà họ tuyên bố là. Mỗi người dùng có một nhận dạng riêng biệt khác nhau nó từ những người dùng khác. Thông thường, nhận dạng người dùng được sử dụng cùng với mật khẩu.

***Xác thực***

Sau khi người dùng đã được xác định, người dùng phải được xác thực. Xác thực là quá trình xác minh danh tính người dùng và quyền truy cập. Việc xác minh danh tính người dùng thường dựa trên một hoặc nhiều đặc điểm để phân biệt cá nhân này với cá nhân khác.

***Bảo vệ chống vi-rút***

Một số lượng lớn các công ty cung cấp cơ bản để siêu bảo vệ. Một số là miễn phí. Tên đại diện là McAfee, Norton, và Kaspersky (từ Symantec), Webroot, và Bitdefender, và Tạp chí PC và các ấn phẩm kỹ thuật khác xem xét các sản phẩm khác nhau. Đối với tốt nhất của năm 2017, xem Rubenking (2017).

**Hệ thống sinh trắc học**

Xác thực sinh trắc học là một công nghệ đo lường và phân tích danh tính của con người dựa trên các đặc điểm sinh học hoặc hành vi có thể đo lường được hoặc các tín hiệu sinh lý.

Các hệ thống sinh trắc học có thể xác định một người đã đăng ký trước đó bằng cách tìm kiếm thông qua cơ sở dữ liệu để tìm sự phù hợp có thể dựa trên trên người mà quan sát thấy các đặc điểm vật lý, sinh học hoặc hành vi hoặc hệ thống có thể xác minh danh tính của một người bằng cách khớp một cá nhân đã đo các đặc điểm sinh trắc học so với phiên bản được lưu trữ trước đó.

Ví dụ về các tính năng sinh trắc học bao gồm dấu vân tay, nhận dạng khuôn mặt, DNA, in lòng bàn tay, hình học bàn tay, nhận dạng mống mắt,và thậm chí mùi / mùi hương. Các đặc điểm hành vi bao gồm ID giọng nói, nhịp gõ (động lực gõ phím) và xác minh chữ ký.

Một mô tả ngắn gọn về một số trong những điều sau đây:

* **Dấu ngón cái hoặc dấu vân tay**. Một ngón tay cái hoặc dấu vân tay (quét ngón tay) của người dùng yêu cầu quyền truy cập được khớp với mẫu có chứa dấu vân tay của người được ủy quyền (ví dụ: được Apple Pay sử dụng).
* **Quét võng mạc.**  Một trùng khớp được tìm kiếm giữa các mô hình của các mạch máu trong võng mạc của những người tìm kiếm truy cập chống lại hình ảnh võng mạc của những người được ủy quyền được lưu trữ trong cơ sở dữ liệu nguồn.
* **ID giọng nói** (**xác thực giọng nói**). Một trùng khớp được tìm kiếm giữa mẫu giọng nói của người tìm kiếm truy cập và được lưu trữ mẫu giọng nói của người được ủy quyền.
* **Nhận dạng khuôn mặt**. Phần mềm máy tính xem hình ảnh hoặc video của một người và so sánh nó với hình ảnh được lưu trữ trong cơ sở dữ liệu (được sử dụng bởi Amazon.com và Alibaba).
* **Nhận dạng chữ ký**. Chữ ký của người tìm kiếm truy cập được khớp với chữ ký xác thực được lưu trữ.

Năm 2017, Apple đã khám phá ID cảm ứng hai bước và nhận dạng khuôn mặt cho iPhone; xem Hardwick (2017).

Lưu ý rằng Alibaba đang sử dụng nhận dạng khuôn mặt để thanh toán trực tuyến. Bạn quét khuôn mặt trước camera trên điện thoại thông minh của bạn (xem Kan 2015 để biết chi tiết). Amazon đang sử dụng một hệ thống tương tự (Hinckley 2016).

Các loại sinh trắc học khác là nhận dạng khuôn mặt hồng ngoại nhiệt, hình học tay và tĩnh mạch tay. Để biết chi tiết, so sánh với liên quan đến đặc điểm của con người và phân tích lợi ích của chi phí, xem [findbiometrics.com/solutions.](file:///C:\Users\QUANGTHAI\Desktop\findbiometrics.com\solutions) Để biết thêm về sinh trắc học, xem

[biometricsociety.org](file:///C:\Users\QUANGTHAI\Desktop\biometricsociety.org)

**Mã hóa và hệ thống một khóa (đối xứng)**

Mã hóa là quá trình mã hóa dữ liệu thành một hình thức (được gọi là *bản mã*) sẽ khó khăn, tốn kém hoặc tốn thời gian cho người không phải tác giả hiểu được. Tất cả các phương thức mã hóa có năm thành phần cơ bản: *bản rõ, bản mã, một thuật toán mã hóa, khóa* và *không gian khóa*. **Bản rõ** là một văn bản hoặc tin nhắn có thể đọc được. Mật mã là một mã hóa văn bản thô. Thuật toán mã hóa là tập hợp các thủ tục hoặc thuật toán toán học được sử dụng để mã hóa hoặc giải mã tin nhắn. Thông thường, thuật toán không phải là phần bí mật của quá trình mã hóa. **Khóa** (**giá trị khóa**) là phần bí mật được sử dụng với thuật toán mã hóa (hoặc giải mã) tin nhắn. Để biết cách mã hóa hoạt động, hãy xem [computer.how wareworks.com/encryption.htm.](file:///C:\Users\QUANGTHAI\Desktop\computer.how%20wareworks.com\encryption.htm)

Những lợi ích chính của mã hóa là:

* Cho phép người dùng mang dữ liệu trên máy tính xách tay, thiết bị di động và thiết bị lưu trữ của họ (ví dụ: ổ flash USB)
* Bảo vệ phương tiện sao lưu trong khi mọi người và dữ liệu ở ngoài cơ sở.
* Cho phép các mạng riêng ảo an toàn cao (VPN; xem phần “Chiến lược quảng cáo và khuyến mãi”).
* Thực thi các chính sách liên quan đến người được ủy quyền xử lý dữ liệu cụ thể của công ty.
* Đảm bảo tuân thủ luật riêng tư và các quy định của chính phủ và giảm rủi ro kiện cáo.
* Bảo vệ danh tiếng và bí mật của tổ chức.

Mã hóa có hai tùy chọn cơ bản: hệ thống đối xứng, với một khóa bí mật và hệ thống bất đối xứng, có hai khóa.

**Mã hóa khóa đối xứng (riêng tư)**

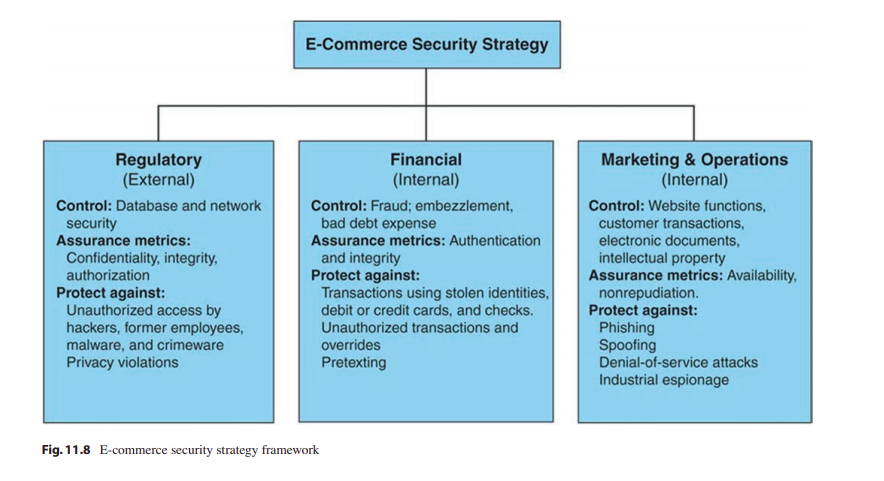
Trong mã hóa khóa đối xứng (riêng tư), cùng một khóa được sử dụng để mã hóa và giải mã bản rõ (xem Hình 11.8). Các người gửi và người nhận văn bản phải chia sẻ cùng một khóa mà không tiết lộ cho bất kỳ ai khác về việc biến nó thành cái gọi là riêng tư hệ thống.

Một chìa khóa mạnh chỉ là một yêu cầu. Chuyển chìa khóa giữa các cá nhân và tổ chức có thể làm cho nó không an toàn. Do đó, trong EC, một hệ thống PKI được sử dụng.

**Cơ sở hạ tầng khóa công khai**

**Cơ sở hạ tầng khóa công khai** (**PKI**) là một khung toàn diện để đảm bảo luồng dữ liệu và trao đổi thông tin khắc phục một số thiếu sót của hệ thống một khóa. Ví dụ, mã hóa một khóa đối xứng yêu cầu người viết một tin nhắn để tiết lộ chìa khóa cho người nhận tin nhắn. Một người đang gửi tin nhắn (ví dụ: nhà cung cấp) có thể cần để phân phối khóa cho hàng ngàn người nhận (ví dụ: người mua) và sau đó khóa có thể sẽ không được giữ bí mật. PKI

giải pháp là sử dụng hai khóa, công khai và riêng tư, cũng như các tính năng bổ sung tạo ra một hệ thống bảo mật cao. Ngoài ra đối với các khóa, PKI bao gồm chữ ký số, bản tóm tắt băm (chức năng) và chứng chỉ kỹ thuật số.



***Mã hóa khóa công khai (không đối xứng)***

**Mã hóa khóa công khai (không đối xứng)** sử dụng hai khóa- một khóa công khai được biết bởi tất cả và một khóa riêng chỉ có chủ sở hữu của nó biết. Hai khóa phải được sử dụng cùng nhau. Nếu một tin nhắn được mã hóa bằng khóa chung, thì chỉ có khóa riêng được liên kết có thể giải mã tin nhắn (và ngược lại). Ví dụ, nếu một người muốn gửi đơn đặt hàng đến nhà cung cấp và có Nội dung vẫn ở chế độ riêng tư, người gửi mã hóa tin nhắn bằng khóa công khai của người mua. Khi nhà cung cấp, ai là người duy nhất có thể đọc đơn đặt hàng, nhận đơn đặt hàng, nhà cung cấp giải mã nó với khóa riêng được liên kết.

***Quy trình PKI: Chữ ký số và Cơ quan cấp chứng chỉ***

Chữ ký số là tương đương điện tử của chữ ký cá nhân trên giấy. Họ rất khó giả mạo vì họ xác thực danh tính của người gửi sử dụng khóa chung. Chữ ký số được coi là hợp pháp như chữ ký trên giấy. Nhìn làm thế nào một chữ ký số hoạt động , đi tới [searchsecurity.techtarget.com/definition/digital-signature](file:///C:\Users\QUANGTHAI\Desktop\searchsecurity.techtarget.com\definition\digital-signature)

***Cơ quan cấp chứng chỉ***

Các cơ quan độc lập được gọi là **các cơ quan cấp chứng chỉ (CAs)** cấp chứng chỉ kỹ thuật số hoặc chứng chỉ SSL, là điện tử các tệp xác định duy nhất các cá nhân và trang web và cho phép giao tiếp được mã hóa. Giấy chứng nhận chứa thống tin cá nhân và các thông tin khác liên quan đến khóa chung và phương thức mã hóa, cũng như hàm băm có chữ ký của dữ liệu chứng chỉ.

***Lớp cổng bảo mật (SSL)***

Các hệ thống PKI được bảo mật hơn nữa với SSL -giao thức cho thương mại điện tử. PKI với SSL làm cho thương mại điện tử rất an toàn nhưng cồng kềnh cho người dùng. Một trong những giao thức chính được sử dụng hiện nay là Lớp cổng bảo mật (SSL). SSL đã thành công bởi Transport Layer Security (TLS), dựa trên SSL. Để biết thêm chi tiết, hãy xem

[searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS.](file:///C:\Users\QUANGTHAI\Desktop\searchsecurity.techtarget.com\definition\Transport-Layer-Security-TLS)

**Các điều khiển khác**

Một số phương pháp khác được sử dụng để kiểm soát truy cập. Ví dụ, Shipley (2017) cung cấp danh sách các dịch vụ DDos tốt nhất của 2017 (ví dụ: f5, Arbor Network, Akamai và Incapsula). Một số là miễn phí. Trong phần tiếp theo, trọng tâm là công ty kỹ thuật số chu vi kỹ thuật số của các mạng.

**Bảo vệ II: Đảm bảo mạng lưới thương mại điện tử**

Một số công nghệ tồn tại để đảm bảo rằng một ranh giới mạng của tổ chức được bảo mật khỏi sự tấn công hoặc xâm nhập không gian mạng và rằng nếu ranh giới của tổ chức bị xâm phạm, sự xâm nhập sẽ được phát hiện nhanh chóng và được chống lại.

**Tường lửa**

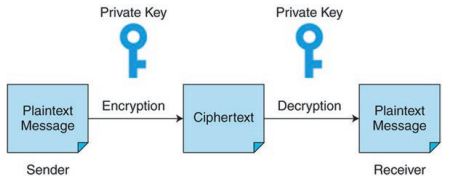
Tường lửa là rào cản giữa một mạng đáng tin cậy nội bộ (hoặc PC) và Internet không đáng tin cậy. Một tường lửa được thiết kế để ngăn chặn truy cập trái phép vào và từ các mạng riêng, chẳng hạn như mạng nội bộ. Về mặt kỹ thuật, tường lửa bao gồm phần cứng và gói phần mềm tách mạng máy tính riêng (ví dụ: mạng LAN của bạn) khỏi mạng công cộng (Internet). Tường lửa được thiết kế chủ yếu để bảo vệ chống lại mọi đăng nhập từ xa, truy cập của những kẻ xâm nhập thông qua các cửa hậu, thư rác và khác nhau

các loại phần mềm độc hại (ví dụ: vi-rút hoặc macro). Tường lửa có nhiều hình dạng và định dạng. Một hệ thống phòng thủ phổ biến là một DMZ. DMZ có thể được thiết kế theo hai cách khác nhau, sử dụng một tường lửa duy nhất hoặc với tường lửa kép. Đối với tường lửa thông minh, xem Tèo (2016)

***Kiến trúc tường lửa kép: DMZ***

Trong kiến trúc DMZ (DMZ là viết tắt của khu phi quân sự), có hai tường lửa giữa Internet và nội bộ  người dùng. Một tường lửa nằm giữa Internet và DMZ (tường lửa biên giới) và một tường lửa khác nằm giữa DMZ và mạng nội bộ (xem hình 11.9). Tất cả các máy chủ công khai được đặt trong DMZ (tức là, giữa hai tường lửa). Với thiết lập này, có thể có các quy tắc tường lửa cho phép các đối tác đáng tin cậy truy cập vào các máy chủ công khai, nhưng tường lửa bên trong có thể hạn chế tất cả các kết nối đến.

Để biết thêm về DMZ và lợi ích của nó, xem Mitchell (2016)



**Mạng riêng ảo (VPN)**

Giả sử một công ty muốn thiết lập ứng dụng B2B, cung cấp cho nhà cung cấp, đối tác và những người khác không chỉ truy cập vào dữ liệu cư trú trên trang web nội bộ của mình nhưng cũng để dữ liệu chứa trong các tệp khác (ví dụ: tài liệu Word) hoặc trong các hệ thống cũ (ví dụ: lớn Cơ sở dữ liệu quan hệ). Theo truyền thống, thông tin liên lạc với công ty sẽ diễn ra trong một an toàn nhưng đắt tiền đường dây thuê riêng giá trị gia tăng hoặc thông qua đường quay số được kết nối với modem hoặc máy chủ truy cập từ xa (RAS). Không may, sử dụng Internet thay thế, miễn phí, có thể không an toàn. Việc sử dụng Internet an toàn hơn được cung cấp bằng cách sử dụng VPN.

Mạng riêng ảo (VPN) đề cập đến việc sử dụng Internet để truyền thông tin nhưng theo cách an toàn hơn. VPN hoạt động như một mạng riêng bằng cách sử dụng mã hóa và các tính năng bảo mật khác để giữ an toàn cho thông tin. Ví dụ: VPN xác minh danh tính của bất kỳ ai sử dụng mạng. Để biết chi tiết về VPN, hãy xem [searchenterprisewan.techtarget.com/defTHER/virtual-private-network](file:///C:\Users\QUANGTHAI\Desktop\searchenterprisewan.techtarget.com\defTHER\virtual-private-network), xem [pcmag.com/article2/0,2817,2403388,00.asp.](file:///C:\Users\QUANGTHAI\Desktop\pcmag.com\article2\0,2817,2403388,00.asp)

**Hệ thống phát hiện xâm nhập (IDS)**

Cho dù tổ chức được bảo vệ như thế nào, nó vẫn có thể là mục tiêu cho các cuộc tấn công bảo mật đã cố gắng. Ví dụ, hầu hết các tổ chức đều có phần mềm chống vi-rút, tuy nhiên họ phải chịu sự tấn công của vi-rút bởi vi-rút mới. Đây là lý do tại sao một tổ chức phải liên tục theo dõi các nỗ lực vi phạm an ninh cũng như thực tế. Việc giám sát có thể được thực hiện bằng cách sử dụng các máy dò xâm nhập. Hệ thống phát hiện xâm nhập (IDS) là một thiết bị bao gồm phần mềm và / hoặc phần cứng được thiết kế để giám sát các hoạt động của mạng máy tính và hệ thống máy tính để phát hiện và xác định các nỗ lực truy cập trái phép và độc hại, thao tác và / hoặc vô hiệu hóa các mạng và hệ thống này. Để biết chi tiết, công nghệ, lợi ích và hạn chế, xem Parker II (2016) và [searchsecurity.techtarget.com/guides/Intributiontion-to-IDS-IPS-Network-intrusion-detection-system-basics.](file:///C:\Users\QUANGTHAI\Desktop\searchsecurity.techtarget.com\guides\Intributiontion-to-IDS-IPS-Network-intrusion-detection-system-basics)

**Xử lý các cuộc tấn công DoS**

Các cuộc tấn công DoS, như được mô tả trước đó, được thiết kế để bắn phá các trang web với tất cả các loại thông tin vô dụng, làm tắc nghẽn các trang web. Một cuộc tấn công DoS được phát hiện càng nhanh, thì việc phòng thủ càng dễ dàng. Các cuộc tấn công DoS phát triển nhanh chóng. Do đó, phát hiện sớm một sự xâm nhập có thể giúp đỡ. Vì có một số loại tấn công DoS (ví dụ: DDoS), nên có một số phương thức phòng thủ. Dành cho

ví dụ, xem [learn-networking.com/network-security/how-to-prevent-denial-of-service-attacks](file:///C:\Users\QUANGTHAI\Desktop\learn-networking.com\network-security\how-to-prevent-denial-of-service-attacks). Phát hiện xâm nhập phần mềm cũng xác định loại DoS, giúp cho việc phòng thủ dễ dàng và nhanh hơn. Để biết tương lai của IDS, xem Guri (2016). Để đánh bại các cuộc tấn công DDos, xem Cisco (2014).

**Bảo vệ III: Kiểm soát chung, Thư rác, Pop-up và Kiểm soát kỹ thuật xã hội**

Mục tiêu của thực tiễn quản lý bảo mật CNTT là bảo vệ hệ thống thông tin. Một chiến lược quốc phòng đòi hỏi một số kiểm soát.

Các loại điều khiển chính là (1) **kiểm soát chung**, được thiết kế để bảo vệ tất cả các ứng dụng hệ thống và (2) **các ứng dụng kiểm soát** để bảo vệ các ứng dụng. Trong phần này và sau đây, chúng tôi thảo luận về các loại đại diện của hai nhóm kiểm soát hệ thống thông tin. Sau đó trong phần này, chúng tôi đề cập đến thư rác và giảm thiểu gian lận.

**Kiểm soát chung, hành chính và kiểm soát khác**

Các loại chính của điều khiển chung là điều khiển vật lý, điều khiển quản trị và các điều khiển khác. Một mô tả ngắn gọn kiểm soát chung được cung cấp tiếp theo.

***Kiểm soát vật lý***

Kiểm soát vật lý bảo vệ các cơ sở và tài nguyên máy tính, bao gồm cả khu vực vật lý nơi các cơ sở tính toán nằm. Các biện pháp kiểm soát cung cấp bảo vệ chống lại các mối nguy hiểm tự nhiên, tấn công tội phạm và một số lỗi của con người.

Phần mềm kiểm soát truy cập mạng được cung cấp bởi tất cả các nhà cung cấp bảo mật lớn (xem [symantec.com/campaigns/endpoint-protection](file:///C:\Users\QUANGTHAI\Desktop\symantec.com\campaigns\endpoint-protection))

***Kiểm soát hành chính***

Kiểm soát hành chính được xác định bởi quản lý và hướng dẫn bao gồm và ban hành và giám sát tuân thủ.

**Bảo vệ chống thư rác**

Gửi thư rác bao gồm quảng cáo bán hàng và trông giống như email cá nhân, hợp pháp và có thể bỏ qua các bộ lọc là vi phạm

Đạo luật Hoa Kỳ kiểm soát hành vi tấn công khiêu dâm và tiếp thị không được mời (CAN-SPAM) năm 2003. Tuy nhiên, nhiều kẻ gửi thư rác che giấu danh tính của họ bằng cách sử dụng máy tính bị tấn công hoặc thư rác ma để tránh bị phát hiện và nhận dạng

**Bảo vệ máy tính của bạn khỏi quảng cáo bật lên**

Việc sử dụng cửa sổ bật lên và các phương thức quảng cáo tương tự đang phát triển nhanh chóng. Đôi khi rất khó để đóng những quảng cáo này khi chúng xuất hiện trên màn hình. Một số quảng cáo này có thể là một phần của thỏa thuận tiếp thị được phép của người tiêu dùng, nhưng hầu hết là không được yêu cầu Người dùng có thể làm gì về quảng cáo bật lên không mong muốn? Dưới đây là một số tài nguyên: Panicware, Inc. Phiên bản miễn phí Pop-Up stopper ([pop-up-stopper-free-edition.software.informer.com](file:///C:\Users\QUANGTHAI\Desktop\pop-up-stopper-free-edition.software.informer.com)), Softonic’s Pop up Blocker ([pop-up-blocker.en.softonic.com/doad](file:///C:\Users\QUANGTHAI\Desktop\pop-up-blocker.en.softonic.com\doad)) và AdFender ([adfender.com](file:///C:\Users\QUANGTHAI\Desktop\adfender.com)); những người khác có sẵn cho một khoản phí. Danh sách, xem [snapfiles.com](file:///C:\Users\QUANGTHAI\Desktop\%20snapfiles.com) và để biết danh sách các phần mềm chặn cho Windows, hãy xem [download.cnet.com/windows/popup-blockersoftware.](file:///C:\Users\QUANGTHAI\Desktop\download.cnet.com\windows\popup-blockersoftware) Nhiều ISP và các nhà sản xuất trình duyệt lớn (ví dụ: Google, Microsoft, Yahoo!, Mozilla) cung cấp các công cụ để ngăn chặn cửa sổ bật lên.

**Bảo vệ chống lại các cuộc tấn công kỹ thuật xã hội khác**

Với sự gia tăng số lượng các cuộc tấn công kỹ thuật xã hội thông qua các trang web và trong các mạng xã hội, cần phải được bảo vệ tốt hơn. Môi trường nguồn mở và bản chất tương tác của công nghệ cũng tạo ra rủi ro. Do đó, bảo mật EC trở thành một điều cần thiết cho bất kỳ sáng kiến mạng xã hội thành công.

Mangis (2016) cung cấp một ví dụ thú vị về nỗ lực tống tiền bằng cách sử dụng kỹ thuật xã hội và khóa một PC cá nhân. Đó là một lừa đảo thông minh, nhưng nó đã thất bại.

Mạng xã hội trải dài trên nhiều ứng dụng và dịch vụ khác nhau. Do đó, nhiều phương pháp và công cụ có sẵn để bảo vệ các hệ thống như vậy. Nhiều giải pháp có bản chất kỹ thuật và nằm ngoài phạm vi của cuốn sách này.

***Bảo vệ chống lừa đảo***

Bởi vì có nhiều phương thức lừa đảo, cũng có nhiều phương thức phòng thủ. Ví dụ minh họa được cung cấp bởi Symantec (2009) và Thông tin người tiêu dùng FTC tại [consumer.ftc.gov/articles/0003-phishing](file:///C:\Users\QUANGTHAI\Desktop\consumer.ftc.gov\articles\0003-phishing). Đối với rủi ro và gian lận thông tin chi tiết, xem sas.com/en\_us/insights/risk-fraud.html

***Bảo vệ chống lại quảng cáo độc hại***

Theo TechTarget, quảng cáo độc hại (quảng cáo độc hại) là một quảng cáo trên Internet có khả năng lây nhiễm cho người xem máy tính với phần mềm độc hại. Microsoft chống lại quảng cáo độc hại bằng cách thực hiện hành động pháp lý chống lại các nhà quảng cáo.

Bisson (2016) phân loại lừa đảo thành sáu loại và đề xuất giải pháp cho từng loại.

**Bảo vệ chống phần mềm gián điệp**

Để đối phó với sự xuất hiện của phần mềm gián điệp, rất nhiều phần mềm chống phần mềm độc hại tồn tại. Luật chống phần mềm gián điệp, có sẵn trong nhiều khu vực pháp lý, thường nhắm mục tiêu bất kỳ phần mềm độc hại được cài đặt mà không có kiến thức của người dùng. Ủy ban tư vấn Thương mại Liên bang Hoa Kỳ Ủy tư vấn cho người tiêu dùng về nhiễm phần mềm gián điệp. Để biết chi tiết và tài nguyên, hãy xem [ftc.gov/news-events/mediaresource/identity-theft-and-data-security/spyware-and-malware.](file:///C:\Users\QUANGTHAI\Desktop\ftc.gov\news-events\mediaresource\identity-theft-and-data-security\spyware-and-malware)

**Bảo vệ chống lại các cuộc chiến tranh mạng**

Đây là một nhiệm vụ khó khăn vì các cuộc tấn công này thường đến từ nước ngoài. Chính phủ Hoa Kỳ đang phát triển các công cụ sẽ khai thác các trang truyền thông xã hội để dự đoán các cuộc tấn công mạng. Các công cụ sẽ giám sát tất cả Facebook, Twitter và các mạng xã hội khác

các trang web để giải thích nội dung. Ý tưởng là để tự động hóa quá trình.

**Bảo vệ người dùng phương tiện truyền thông xã hội**

Như đã nêu trước đó, có một mối đe dọa gia tăng đối với người dùng phương tiện truyền thông xã hội và các thành viên của mạng xã hội. Nó có thể khó

để bảo vệ, đặc biệt chống lại những kẻ mạo danh truyền thông xã hội, những người cố gắng lừa đảo. Velasco (2016) gợi ý như sau:

* Sử dụng bất kỳ cài đặt bảo mật nào được cung cấp bởi các nền tảng truyền thông xã hội. Ví dụ về những điều này bao gồm các thiết lập quyền riêng tư, câu đố captcha và các trang cảnh báo cho bạn biết rằng bạn đang được chuyển hướng ra khỏi trang web.
* Không chia sẻ thông tin đăng nhập, ngay cả với những người bạn tin tưởng. Bạn bè thân thiết và gia đình vẫn có thể vô tình làm bạn dễ bị tổn thương nếu họ đang sử dụng tài khoản của bạn.
* Hãy cảnh giác với những thông tin bạn chia sẻ. Giữ thông tin cá nhân của bạn dưới khóa và chìa khóa, và không bao giờ cung cấp thông tin có độ nhạy cao như số xã hội hoặc số giấy phép lái xe của bạn.
* Không sử dụng lại mật khẩu. Có một mật khẩu duy nhất cho mọi tài khoản bạn giữ.
* Xem xét thay đổi thông tin không cần thiết. Bạn không cần phải đưa ngày sinh nhật thật của mình lên Facebook.
* Chỉ chấp nhận yêu cầu kết bạn từ những người có vẻ quen thuộc.

**Hoạt động kinh doanh liên tục và khắc phục thảm họa**

Thảm họa có thể xảy ra mà không có cảnh báo. Một biện pháp phòng thủ thận trọng là có một kế hoạch kinh doanh liên tục, chủ yếu bao gồm một thảm họa kế hoạch phục hồi. Kế hoạch như vậy mô tả chi tiết về quá trình phục hồi từ các thảm họa lớn như mất tất cả (hoặc hầu hết) các cơ sở tính toán hoặc dữ liệu.

**Ví dụ: Bệnh viện trả tiền chuộc sau khi tấn công phần mềm độc hại vì họ không có kế hoạch khắc phục thảm họa.**

Trung tâm Y tế Presbyterian Hollywood đã trả khoản tiền chuộc 17.000 đô la Bitcoin (vì vậy không thể xác định được kẻ tống tiền / tin tặc; xem chương 12 về Bitcoin). Tin tặc đã mã hóa dữ liệu không được sao lưu. Bệnh viện thất bại với thảm họa và kế hoạch phục hồi, vì vậy không có sự lựa chọn (theo quản lý bệnh viện) mà phải trả tiền chuộc. Để biết chi tiết, xem Jennings (2016).Trường hợp này tương tự như trường hợp mở.

**Kiểm soát an ninh quan trọng Sans Sans CIS**

Học viện Sans là một công ty chuyên về bảo mật thông tin. Công ty nổi tiếng về đào tạo, giáo dục, và các chương trình chứng nhận. Một trong những dự án được biết đến nhiều nhất của công ty là Công cụ giám sát và đo lường quan trọng của CIS Bảo vệ. " 20 điều khiển này là cốt lõi của cấu hình bảo mật được khuyến nghị của cơ sở hạ tầng mạng máy tính.Chúng được khuyến nghị để phòng thủ không gian mạng hiệu quả. Sans cung cấp một poster miễn phí bao gồm những điểm nổi bật của các điều khiển; xem [sans.org/media/critical-security-controls/SANS\_CSC\_Poster.pdf](file:///C:\Users\QUANGTHAI\Desktop\sans.org\media\critical-security-controls\SANS_CSC_Poster.pdf). 20 mặt hàng là mặt hàng ưu tiên đầu tiên. Poster bao gồm các nhà cung cấp chính và các sản phẩm của họ, cùng với một ma trận cho thấy mức độ mà các sản phẩm có thể đáp ứng mỗi trong số 20 mặt hàng. Một mô tả về 20 mặt hàng có sẵn trên poster cũng như tại [sans.org/criticalsecurity-controls](file:///C:\Users\QUANGTHAI\Desktop\sans.org\criticalsecurity-controls). Greene (2015) cung cấp thảo luận bổ sung. Sans cung cấp nghiên cứu trường hợp, hệ thống giám sát Internet nhân viên của các chuyên gia toàn cầu, tài liệu nghiên cứu và tin tức. Một sự phát triển đáng chú ý là NetWars, một bộ học tập tương tác các công cụ để mô phỏng các kịch bản như tấn công mạng. NetWars được sử dụng bởi Không quân Hoa Kỳ và Quân đội Hoa Kỳ.

Một số điều khiển quan trọng (ví dụ: kiểm soát truy cập, bảo vệ dữ liệu, phục hồi dữ liệu, tường lửa và kiểm tra thâm nhập) là thảo luận trong chương này.

**PHẦN 11.6 CÂU HỎI THƯỜNG GẶP**

1. Xác định kiểm soát truy cập.
2. Các yếu tố cơ bản của một hệ thống xác thực là gì?
3. Xác định hệ thống sinh trắc học và liệt kê năm phương pháp của nó.
4. Xác định mã hóa đối xứng (một khóa).
5. Liệt kê một số nhược điểm của hệ thống đối xứng.
6. Các thành phần chính của PKI là gì?
7. Mô tả quá trình PKI.
8. Chữ ký số hoạt động như thế nào?
9. Mô tả chứng nhận kỹ thuật số.
10. Liệt kê các loại tường lửa cơ bản và mô tả ngắn gọn từng loại.
11. VPN hoạt động như thế nào và nó mang lại lợi ích gì cho người dùng?
12. Mô tả ngắn gọn các loại IDS chính.
13. Điều khiển chung là gì? Liệt kê các loại khác nhau.
14. Làm thế nào để bảo vệ chống thư rác?
15. Làm thế nào để bảo vệ chống lại cửa sổ bật lên?
16. Làm thế nào để bảo vệ chống lừa đảo, phần mềm gián điệp và quảng cáo độc hại?
17. Làm thế nào để bảo vệ chống lại tấn công đòi tiền chuộc?

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

Gian lận Internet là một vấn đề lớn trong thương mại điện tử và nó đang phát triển nhanh chóng. Sự gian lận chủ yếu là chống lại người tiêu dùng, nhưng có một số chống lại người bán và thương nhân. Chính phủ đặc biệt mong muốn giáo dục công chúng về nhiều loại lừa đảo, đặc biệt nhắm vào công dân cao cấp. Thông tin chung về các gian lận phổ biến được cung cấp bởi các cơ quan như FBI (xem [**fbi.gov/scams-and-safe/common-fraud-scheme/iNET-fraud**](http://fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud) ). FBI cũng vận hành Trung tâm Khiếu nại Tội phạm Internet, IC3 tại [**ic3.gov**](http://ic3.gov/) . Gian lận Internet là một vấn đề đang gia tăng (khoảng 25% tất cả người tiêu dùng là nạn nhân). Vấn đề đang gia tăng do sự pha trộn giữa thương mại xã hội và thương mại điện tử và sự gia tăng sử dụng thương mại điện tử (xem Frenkel[2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR32)). Để biết tổng quan, hãy xem [**paypal.com/us/webapps/mpp/paypal-safe-and-securance**](http://paypal.com/us/webapps/mpp/paypal-safety-and-security) . Các cuộc tấn công lừa đảo trực tuyến đang gia tăng ở mức đáng báo động ở Hoa Kỳ, theo Meola ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR80)). Các hoạt động gian lận tồn tại ở nhiều định dạng, như được thảo luận trong phần [Phương pháp phi kỹ thuật: Từ lừa đảo đến thư rác và gian lận](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#Sec79) . Xem thêm Lonergan ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR73)). Để biết xu hướng gian lận thương mại điện tử toàn cầu, xem Khaitan ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR60)).

Để biết 20 mẹo để bảo vệ trang web EC của bạn khỏi bị hack và lừa đảo, hãy xem Karol ([2017](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR58)).

Cần phải bảo vệ người tiêu dùng EC, điều mà IC3 cố gắng thực hiện, bằng cách thông báo cho công chúng về các trò gian lận trên Internet và bằng cách xuất bản các thông báo dịch vụ công cộng.

**Bảo vệ người tiêu dùng (người mua)**

Bảo vệ người tiêu dùng là rất quan trọng đối với sự thành công của bất kỳ thương mại nào, đặc biệt là giao dịch điện tử, nơi giao dịch giữa người mua và người bán không phải đối mặt. Ủy ban Thương mại Liên bang (FTC) thi hành luật bảo vệ người tiêu dùng tại Hoa Kỳ. FTC cung cấp một danh sách các trò lừa đảo trực tuyến phổ biến (xem [onguardonline.gov/articles/0002-common-online-scams](file:///C:\Users\QUANGTHAI\Desktop\onguardonline.gov\articles\0002-common-online-scams)). Ngoài ra, Liên minh châu Âu và Hoa Kỳ đang cố gắng phát triển các chính sách bảo vệ người tiêu dùng chung. Để biết chi tiết, xem trang web Đối thoại người tiêu dùng xuyên Đại Tây Dương tại [tacd.org](http://tacd.org/).

Năm 2016, FTC đã đưa ra các khuyến nghị của OECD về bảo vệ người tiêu dùng trong thương mại điện tử. Các khuyến nghị nhằm tăng cường bảo vệ thanh toán, giảm rủi ro bảo mật và quyền riêng tư, mở rộng an toàn sản phẩm và khuyến khích sử dụng ngôn ngữ đơn giản trong quảng cáo. Để biết chi tiết, xem Blog Luật ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR70)) và [oecd.org/sti/consumer/EC Commerce-Recommendation-2016.pdf](http://oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf).

**Lời khuyên đại diện và nguồn để bảo vệ bạn**

Một danh sách đại diện sau:

* Người dùng nên đảm bảo rằng họ vào trang web thực sự của các công ty nổi tiếng, chẳng hạn như Walmart, Disney và Amazon.com, bằng cách truy cập trực tiếp vào trang web chứ không phải thông qua liên kết.
* Kiểm tra bất kỳ trang web lạ nào để biết địa chỉ và số điện thoại và số fax. Gọi và đố một nhân viên bán hàng về công ty và các sản phẩm.
* Điều tra người bán với phòng thương mại địa phương, Văn phòng kinh doanh tốt hơn ( bbb.org ) hoặc TRUSTe ( truste.com ).
* Điều tra mức độ an toàn của trang web của người bán và cách thức tổ chức.
* Kiểm tra các bảo đảm hoàn lại tiền, bảo hành và thỏa thuận dịch vụ trước khi mua hàng.
* So sánh giá trực tuyến với giá trong các cửa hàng thông thường Giá quá thấp có thể là quá tốt là đúng.
* So sánh giá trực tuyến với giá trong các cửa hàng thông thường Giá quá thấp có thể là quá tốt là đúng.
* Hỏi bạn bè những gì họ biết về các trang web. Tìm lời chứng thực và chứng thực (hãy cẩn thận, một số có thể bị sai lệch).
* Tìm hiểu những biện pháp khắc phục có sẵn trong trường hợp tranh chấp.
* Tham khảo ý kiến Trung tâm gian lận liên minh người tiêu dùng quốc gia (fraud.org ).
* Kiểm tra các tài nguyên có sẵn tại Consumerworld.org .
* Amazon.com cung cấp bảo vệ toàn diện. Xem pay.amazon.com/us/merchant .

Ngoài những lời khuyên này, người tiêu dùng và người mua hàng cũng có quyền trên Internet,

* Ủy ban Thương mại Liên bang ([ftc.gov](file:///C:\Users\QUANGTHAI\Desktop\ftc.gov)): Bảo vệ người tiêu dùng Mỹ. Email lạm dụng nên được chuyển tiếp đến spam@uce.go. Để biết các mẹo và lời khuyên, hãy xem ftc.gov/tips-advice .
* Chính phủ an toàn trực tuyến liên bang (usa.gov/online-safe)
* Trung tâm gian lận liên minh người tiêu dùng quốc gia (fraud.org).
* Trung tâm thông tin công dân liên bang tại (gsa.gov/portal/).
* Bộ Tư như được mô tả trong danh sách các nguồn sau đây:pháp Hoa Kỳ (Justice.gov).
* Trung tâm Khiếu nại Tội phạm Internet (ic3.gov).
* Hiệp hội Luật sư Hoa Kỳ cung cấp các mẹo mua sắm trực tuyến tại Americanbar.org/groups/business\_law/migrated/safeshopping.html.
* Cục kinh doanh tốt hơn (bbb.org).
* Cục Quản lý Thực phẩm và Dược phẩm Hoa Kỳ cung cấp thông tin về việc mua thuốc và các sản phẩm y tế trực tuyến (www.fda.gov/forconsumers/protectyourself/default.html).
* Cục kinh doanh tốt hơn (bbb.org).
* Cục Quản lý Thực phẩm và Dược phẩm Hoa Kỳ cung cấp thông tin về việc mua thuốc và các sản phẩm y tế trực tuyến (www.fda.gov/forconsumers/protectyourself/default.html).
* Hiệp hội tiếp thị trực tiếp (thedma.org).

Để biết các mẹo cụ thể về cách phát hiện các trang web và sản phẩm giả mạo, hãy xem Horowitz và Horowitz ([2015](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR48)). Chống lại tin tức giả mạo có thể bao gồm gian lận, xem LaCapria ([2017](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR67)).

Tuyên bố miễn trừ trách nhiệm: Đây là thông tin chung về quyền của người tiêu dùng. Đây không phải là tư vấn pháp lý về cách bất kỳ cá nhân cụ thể nên tiến hành. Nếu bạn cần tư vấn pháp lý cụ thể, tham khảo ý kiến ​​một luật sư.

**Dịch vụ đảm bảo của bên thứ ba**

Một số tổ chức công cộng và các công ty tư nhân cũng cố gắng bảo vệ người tiêu dùng. Sau đây chỉ là một vài ví dụ.

***Bảo vệ bởi một bên trung gian của bên thứ ba***

Các trung gian quản lý thị trường điện tử cố gắng bảo vệ người mua và người bán. Một ví dụ điển hình là eBay, nơi cung cấp một chương trình bảo vệ rộng rãi (xem Bảo đảm hoàn lại tiền của eBay ([trang.ebay.com/ebay-money-back-guarantee/](http://pages.ebay.com/ebay-money-back-guarantee/)) và Trung tâm giải quyết tranh chấp).

***Tin tưởng của TRUSTe***

TRUSTe ([truste.com](http://truste.com/)) là một công ty vì lợi nhuận, có nhiệm vụ là đảm bảo rằng các doanh nghiệp của [**Tuân**](http://truste.com/) thủ các thông lệ tốt nhất về việc thu thập và sử dụng thông tin cá nhân trên trang web của họ (xem [Truste.com/about-TRUSTe/](http://truste.com/about-TRUSTe/)).

Chương trình TRUSTe là tự nguyện. Phí cấp phép sử dụng Trustmark được trả bởi người bán, tùy thuộc vào quy mô của doanh nghiệp trực tuyến.

***Cục kinh doanh tốt hơn***

Văn phòng kinh doanh tốt hơn (BBB; [bbb.org](http://bbb.org/)), một tổ chức phi lợi nhuận được hỗ trợ chủ yếu bởi tư cách thành viên, thu thập và cung cấp các báo cáo về các doanh nghiệp mà người tiêu dùng có thể xem xét trước khi mua hàng. BBB trả lời hàng triệu câu hỏi mỗi năm. BBB cũng xử lý các tranh chấp của khách hàng đối với các doanh nghiệp.

***Con dấu WebTrust***

Chương trình con dấu WebTrust tương tự TRUSTe. Viện Kế toán công chứng Hoa Kỳ ([aicpa.org](http://aicpa.org/)) tài trợ cho nó (xem [webtrust.org/item64428.aspx](http://webtrust.org/item64428.aspx)).

***Đánh giá của người tiêu dùng***

Một số lượng lớn các trang web bao gồm đánh giá sản phẩm và nhà cung cấp được cung cấp bởi người tiêu dùng. Ví dụ: trên Yelp!, Tỷ lệ thành viên cộng đồng và nhận xét về doanh nghiệp.

**Đạo luật lạm dụng và gian lận máy tính (CFAA)**

Các **gian lận máy tính và Lạm dụng Luật (CFAA)**, được thông qua năm 1984 và sửa đổi nhiều lần, là một mốc quan trọng trong pháp luật EC. Ban đầu, phạm vi và mục đích của CFAA là bảo vệ máy tính của chính phủ và máy tính của ngành tài chính khỏi hành vi trộm cắp hình sự của người ngoài. Năm 1986, CFAA đã được sửa đổi để bao gồm các hình phạt cứng hơn cho các vi phạm, nhưng nó vẫn chỉ bảo vệ các máy tính được sử dụng bởi chính phủ liên bang hoặc các tổ chức tài chính. Khi Internet mở rộng phạm vi, CFAA cũng vậy.

**Bảo vệ người bán (người bán)**

Internet cũng giúp người mua dễ dàng tham gia vào EC để thực hiện hành vi gian lận chống lại thương nhân.

Để biết ví dụ về cách người mua cố gắng lừa tiền hoặc hàng hóa từ người bán, hãy xem Shrubb ([2015](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR105)). Mellor ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR79)) thảo luận về vấn đề này và đưa ra một số gợi ý để sử dụng dữ liệu có sẵn bằng cách nghiên cứu hồ sơ và hành vi của khách hàng.

Người bán phải được bảo vệ chống lại:

* Những khách hàng từ chối rằng họ đã đặt hàng
* Khách hàng tải phần mềm có bản quyền và bán cho người khác
* Khách hàng cung cấp thông tin thanh toán gian lận (thẻ tín dụng giả hoặc séc xấu) cho các sản phẩm và dịch vụ mà họ mua
* Khách hàng có danh tính giả
* Những kẻ mạo danh người bán hàng sử dụng tên của người bán khác (xem Báo cáo thường niên của CyberSource)
* Những người bán khác sử dụng tên, nhãn hiệu của người bán ban đầu và các tính năng độc đáo khác và thậm chí cả địa chỉ Web của họ (hoặc tương tự với nó)

Gian lận thanh toán của người tiêu dùng và tội phạm (ví dụ: sử dụng thẻ tín dụng không hợp lệ).

Người bán cũng có thể bị tấn công bất hợp pháp hoặc phi đạo đức bởi các đối thủ cạnh tranh. Thương nhân cũng là đối tượng của vi phạm bản quyền.

**Thí dụ**

Một vụ kiện tập thể đã được đệ trình chống lại McAfee tại Tòa án Khu vực Hoa Kỳ cho Quận Bắc California (Vụ án số 10-1455-HRL) cáo buộc rằng sau khi các nguyên đơn mua phần mềm McAfee từ trang web của McAfee, một quảng cáo bật lên lừa đảo (từ một của các đối tác của McAfee) trông giống như một trang McAfee đã xuất hiện và cảm ơn các nguyên đơn đã mua phần mềm của họ. Quảng cáo bật lên yêu cầu họ nhấp vào nút Thử Thử ngay bây giờ, mà họ cho rằng sẽ tải xuống phần mềm họ mới mua, nhưng không biết họ đã nhận được đăng ký dùng thử 30 ngày cho Arpu, Inc. sản phẩm không phải của McAfee). Sau đó, họ phát hiện ra rằng McAfee truyền thẻ tín dụng / thẻ ghi nợ của khách hàng và thông tin thanh toán đến Arpu (khách hàng bị tính phí 4 đô la.

**Người bán có thể làm gì?**

Các công ty như ChargeBack stop ( [**ChargBackstopper.com**](http://webtrust.org/item64428.aspx) ) và ChargeBack Protection ( [**ChargBackprotection.org**](http://chargebackprotection.org/) ) cung cấp cho các thương nhân một cơ sở dữ liệu về các số thẻ tín dụng đã có các đơn đặt hàng bồi hoàn trực tuyến. Người bán có quyền truy cập vào cơ sở dữ liệu có thể sử dụng thông tin này để quyết định có nên tiến hành bán hàng hay không. Trong tương lai, ngành công nghiệp thẻ tín dụng đang có kế hoạch sử dụng sinh trắc học để quản lý hoạt động mua sắm điện tử. Ngoài ra, người bán có thể sử dụng PKI và chứng chỉ kỹ thuật số, đặc biệt là giao thức SET, để giúp ngăn chặn gian lận.

Các giải pháp khả thi khác bao gồm:

* Sử dụng phần mềm thông minh để xác định khách hàng nghi vấn (hoặc trong các công ty nhỏ, thực hiện nhận dạng này theo cách thủ công). Một kỹ thuật, ví dụ, liên quan đến việc so sánh thanh toán thẻ tín dụng và địa chỉ giao hàng được yêu cầu.
* Xác định các tín hiệu cảnh báo, tức là cờ đỏ cho các giao dịch gian lận có thể xảy ra.
* Hỏi khách hàng có địa chỉ thanh toán khác với địa chỉ giao hàng để gọi cho ngân hàng của họ và có địa chỉ thay thế được thêm vào tài khoản ngân hàng của họ. Các nhà bán lẻ sẽ đồng ý vận chuyển hàng hóa đến địa chỉ thay thế chỉ khi việc này được thực hiện.
* Yêu cầu khách hàng tiết lộ mã xác minh thẻ tín dụng.
* Trì hoãn giao hàng cho đến khi nhận được tiền.

Đối với thiết bị đầu cuối thương mại bảo mật và hệ thống EC, xem Báo cáo của Trung tâm chia sẻ thông tin mạng bán lẻ (R-CISC); xem chi tiết tại ISAC ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR50)).

Để thảo luận thêm về những gì thương nhân có thể làm để bảo vệ bản thân khỏi gian lận, hãy xem CyberSource (ví dụ: [**www.cybersource.com/products/fraud\_man quản lý**](http://www.cybersource.com/products/fraud_management) ). Để biết mười biện pháp để giảm gian lận thẻ tín dụng cho Thương gia Internet (Sách trắng FraudLabs.com), hãy xem [**gian lậnlabs.com/docs/fraudlabs\_white\_apers.pdf**](http://fraudlabs.com/docs/fraudlabs_white_paper.pdf) .

Ban cho ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR37)) cung cấp danh sách các trò gian lận sau đây đối với hoạt động kinh doanh: (1) tổng đài cũ, (2) trả lại giả, (3) kiểm toán giả mạo, (4) đã thay đổi và (5) thanh toán vượt mức quốc tế. Ban cho ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR37)) cũng gợi ý cách tránh những gian lận và lừa đảo này.

Bảo vệ thị trường và dịch vụ mạng xã hội

Các thị trường như eBay, Yahoo!, Amazon.com và Alibaba phải đối mặt với vấn đề người bán hàng cố gắng bán sản phẩm giả trực tuyến. Vấn đề đặc biệt nghiêm trọng đối với Alibaba và eBay, có mô hình kinh doanh là kết nối người bán và người mua, ngược lại với Amazon.com và các nhà bán lẻ điện tử khác chủ yếu mua sản phẩm và bán lẻ cho người tiêu dùng. Thị trường cố gắng trấn áp người làm giả, nhưng đó không phải là một công việc dễ dàng.

Facebook và các mạng xã hội khác đã chuyển sang thương mại hóa đang đối mặt với vấn đề tài khoản giả mạo. Đối với vấn đề và giải pháp, xem Jones ([2016a](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR53)).

**Phần mềm phát hiện gian lận**

Một số lượng lớn các sản phẩm phần mềm có sẵn để phát hiện gian lận của người tiêu dùng, các doanh nghiệp khác, tổn thất tuân thủ, v.v. Để đánh giá các sản phẩm phần mềm chính, hãy xem [capterra.com/fin finance-fraud-detection-software](http://capterra.com/financial-fraud-detection-software).

**Bảo vệ cả người mua và người bán: Sử dụng chữ ký điện tử và các tính năng bảo mật khác**

Có một số phương pháp bảo vệ các giao dịch EC và cả khách hàng và người bán. Để biết chi tiết, xem Hyatt ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR49)).

Một phương pháp giúp phân biệt giữa giao dịch hợp pháp và gian lận là chữ ký điện tử.

Một **chữ ký điện tử** là “điện tương đương của một chữ ký viết tay” (mỗi [pcmag.com/encyclopedia/term/42500/electronic-signature](http://pcmag.com/encyclopedia/term/42500/electronic-signature)). Chữ ký điện tử cung cấp mức độ bảo mật cao và được hầu hết các pháp nhân công nhận là tương đương với chữ ký viết tay. Tất cả các chữ ký điện tử được đại diện kỹ thuật số. Các tài liệu và hợp đồng điện tử đã ký có tính ràng buộc về mặt pháp lý như các tài liệu và hợp đồng trên giấy.

**Xác thực**

Trong môi trường trực tuyến nơi người tiêu dùng và thương nhân không có liên hệ vật lý với nhau, việc chứng minh tính xác thực của mỗi người là cần thiết vì người mua và người bán không nhìn thấy nhau. Tuy nhiên, nếu người ta có thể chắc chắn về danh tính của người ở đầu dây bên kia, có thể có nhiều ứng dụng thương mại điện tử hơn. Ví dụ, sinh viên sẽ có thể làm bài kiểm tra trực tuyến từ bất cứ đâu mà không cần proctors. Gian lận giữa những người nhận thanh toán của chính phủ sẽ được giảm thiểu. Người mua sẽ yên tâm ai là người bán và người bán sẽ biết, với mức độ tin cậy rất cao, người mua thực sự là ai. Phỏng vấn việc làm trực tuyến sẽ chính xác bởi vì người nộp đơn gần như không thể mạo danh người khác. Nhìn chung, niềm tin vào các giao dịch trực tuyến và trong EC nói chung sẽ tăng đáng kể.

**Hệ thống phát hiện gian lận**

Có một số lượng lớn các hệ thống phát hiện gian lận như sử dụng khai thác dữ liệu để gian lận thẻ tín dụng. CyberSource cũng đã phát triển một số công cụ để phát hiện gian lận. Để biết chi tiết, hãy xem các báo cáo định kỳ của CyberSource và [Authorize.net/resource/files/fdswhitepaper.pdf](http://pcmag.com/encyclopedia/term/42500/electronic-signature).

**Mục 11.7 Câu hỏi ôn tập**

1. Mô tả các biện pháp bảo vệ người tiêu dùng.
2. Mô tả dịch vụ đảm bảo.
3. Người bán phải làm gì để tự bảo vệ mình trước sự gian lận? Làm sao?
4. Mô tả các loại chữ ký điện tử. Ai được bảo vệ? Tại sao?
5. Mô tả xác thực.

**11.8 Triển khai bảo mật thương mại điện tử**

Güldenast ([2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR41)) khuyên bạn nên làm theo bốn bước sau: (1) xác định các yêu cầu rõ ràng, (2) đặt tiêu chuẩn của bạn, (3) tìm kiếm các luồng và (4) tiến hành giám sát liên tục.

Bây giờ bạn đã biết về cả các mối đe dọa và phòng thủ, chúng ta có thể thảo luận về một số vấn đề triển khai bắt đầu với lý do tại sao khó khăn, hoặc thậm chí là không thể, để ngăn chặn tội phạm máy tính và sự cố của hệ thống thông tin. Để quản lý an ninh nói chung, xem Sennewald và Baillie ([2015](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR102)).

### Các trình điều khiển của quản lý an ninh EC

Sự phát triển bùng nổ của EC và SC, cùng với sự gia tăng các chiến lược luôn thay đổi của tội phạm mạng, kết hợp với các yêu cầu và quy định pháp lý của các công ty bảo hiểm, thúc đẩy nhu cầu quản lý an ninh EC toàn diện. Trình điều khiển bổ sung là:

* Các luật và quy định mà các tổ chức phải tuân thủ.
* Hành vi của EC toàn cầu. Cần bảo vệ nhiều hơn khi làm kinh doanh với nước ngoài.
* Tài sản thông tin đã trở nên quan trọng đối với hoạt động của nhiều doanh nghiệp.
* Công nghệ thông tin mới và nhanh hơn được chia sẻ trên khắp các tổ chức. Hợp tác tổ chức là cần thiết.
* Sự phức tạp của cả các cuộc tấn công và phòng thủ đòi hỏi một cách tiếp cận hợp tác trên toàn tổ chức.

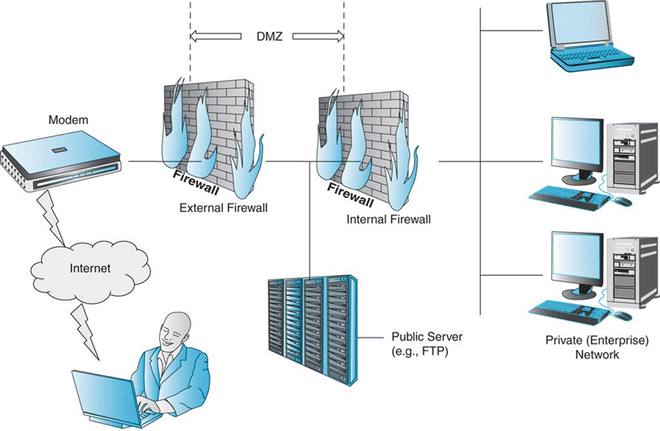
**Độ nghiêm trọng trong an ninh mạng**

Theo Editors ( [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR25) ), 1 nghìn tỷ đô la sẽ được chi tiêu trên toàn cầu cho an ninh mạng (riêng về quốc phòng) từ năm 2017 đến năm 2021. Báo cáo về tội phạm mạng năm 2016 rằng tội phạm mạng sẽ tiêu tốn 6 nghìn tỷ đô la trên thế giới. Rõ ràng, quản lý cấp cao phải được tham gia. Để biết phạm vi bảo hiểm toàn diện về quản lý bảo mật thông tin, xem Whitman và Matford ( [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR123) ).

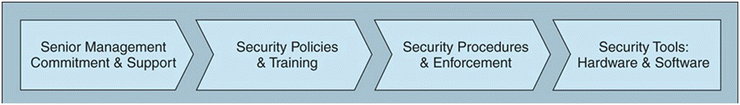
### Cam kết và hỗ trợ quản lý cấp cao

Thành công của một chiến lược và chương trình bảo mật EC phụ thuộc vào sự cam kết và sự tham gia của quản lý cấp cao. Nhiều hình thức bảo mật không phổ biến vì chúng bất tiện, hạn chế, tốn thời gian và tốn kém. Thực tiễn bảo mật có thể không phải là ưu tiên hàng đầu của tổ chức trừ khi chúng được ủy quyền.

Do đó, mô hình bảo mật và quyền riêng tư của EC để bảo mật doanh nghiệp hiệu quả nên bắt đầu bằng cam kết và hỗ trợ của quản lý cấp cao, như trong Hình 10.10. Mô hình này xem bảo mật EC (cũng như bảo mật CNTT rộng hơn) là sự kết hợp giữa cam kết và hỗ trợ, chính sách và đào tạo, quy trình và thực thi và các công cụ, tất cả được thực hiện như một quy trình liên tục (Hình [11.10](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#Fig10) và [11.11](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#Fig11)).



*Hình 11.10 Hai tường lửa: kiến trúc DMZ*



*Hình 11.11 Enterprisewide EC bảo mật và quy trình bảo mật*

Theo Sách trắng *rủi ro Delta* (xem Nhân viên [2016a](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR109) ), sự tham gia của Hội đồng quản trị vào an ninh mạng cần tuân theo bốn lĩnh vực chính sau đây:

* Đảm bảo rằng các thành viên hội đồng quản trị được đào tạo về an ninh mạng phù hợp với trình độ và vai trò của họ.
* Kết hợp bảo vệ an ninh mạng vào Tuyên bố về sự chấp nhận rủi ro của tổ chức.
* Thúc đẩy việc thực hiện chương trình quản lý rủi ro không gian mạng được tích hợp với quản lý doanh nghiệp rộng hơn của tổ chức về mọi rủi ro, như rủi ro tài chính (ví dụ: thị trường. Thanh khoản, tín dụng), rủi ro tuân thủ và các rủi ro hoạt động khác (ví dụ: gian lận, kiện tụng, báo cáo , an toàn, an ninh vật lý).
* Thúc đẩy an ninh mạng trong toàn bộ tổ chức.

### Chính sách bảo mật và đào tạo của EC

Một nhiệm vụ bảo mật quan trọng là phát triển chính sách bảo mật EC của tổ chức, cũng như các quy trình cho các hoạt động bảo mật và EC cụ thể như kiểm soát truy cập và bảo vệ dữ liệu của khách hàng. Khách hàng nên:

* Biết rằng dữ liệu đang được thu thập và khi điều này được thực hiện
* Cho phép họ thu thập dữ liệu
* Có kiến ​​thức và một số kiểm soát về cách dữ liệu được kiểm soát và sử dụng
* Được thông báo rằng thông tin thu thập sẽ không được chia sẻ với các tổ chức khác

Để bảo vệ chống lại tội phạm sử dụng phương tiện truyền thông xã hội, bạn có thể:

* Xây dựng chính sách và thủ tục để khai thác cơ hội nhưng bảo vệ khách hàng
* Giáo dục nhân viên và những người khác về những gì được chấp nhận và những gì không được chấp nhận

#### **Đào tạo để hack**

Trong khi một số người đào tạo mọi người để hack để kiếm tiền, những người khác tin rằng nếu bạn học cách hack, bạn sẽ bảo vệ hệ thống của mình tốt hơn. Để xem video cho thấy cách hack Facebook bằng cách lừa đảo, hãy xem video 10 phút tại [**youtube.com/watch?v=Z2z9zncsYW8**](http://youtube.com/watch?v=Z2z9zncsYW8) .

#### **Mạng thông minh**

Theo WiseGeek ([2017](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR125)), tình báo Cyber ​​Cyber ​​là công cụ theo dõi, phân tích và chống lại các mối đe dọa an ninh kỹ thuật số. Loại trí thông minh này là sự pha trộn giữa gián điệp vật lý và phòng thủ với công nghệ thông tin hiện đại. Nhiều nỗ lực tình báo mạng khác nhau giúp chống lại virus, tin tặc và khủng bố tồn tại trên Internet với mục đích đánh cắp thông tin nhạy cảm. Bảo vệ các bên, như chính phủ, khỏi các mối đe dọa này là một phần chính của lĩnh vực này, nhưng vì vậy, đang quyết liệt chống lại các mối đe dọa này.

Một trong những nhiệm vụ lớn nhất của cộng đồng tình báo mạng là cung cấp bảo mật chống lại các mối đe dọa kỹ thuật số này. Một chuyên gia tình báo có thể sẽ có một nền tảng kép về gián điệp và bảo mật Internet hoặc công nghệ thông tin. Thiết lập tường lửa, chương trình quét vi-rút và kiểm tra thường xuyên các vi phạm trong bảo mật là những vai trò quan trọng giúp bảo mật hệ thống máy tính khỏi các lực lượng bên ngoài.

Phân tích các mối đe dọa khủng bố là một khía cạnh quan trọng khác của tình báo mạng. Khía cạnh này của lĩnh vực này giống như các chiến thuật tình báo và gián điệp truyền thống về thu thập thông tin. Sử dụng các nguồn của bên thứ ba, hoặc là người cung cấp thông tin hoặc một trong nhiều công ty độc lập giúp xác định các mối đe dọa trên mạng, các chuyên gia phải thu thập dữ liệu này và xác định cách nó đe dọa những gì đang được bảo vệ. Thông thường, việc tạo báo cáo và đề xuất cho người khác là phổ biến trong lĩnh vực này hơn là công việc điện tử.

Theo [**sans.org**](http://youtube.com/watch?v=Z2z9zncsYW8) , tình báo mạng là một công cụ phòng thủ quan trọng.

### Phân tích rủi ro EC và các vấn đề đạo đức

Các quy trình bảo mật của EC yêu cầu đánh giá các tài sản kỹ thuật số và tài chính có rủi ro, bao gồm các cân nhắc về chi phí và hoạt động.

Một đánh giá liên quan là phân tích tác động kinh doanh. **Phân tích tác động kinh doanh (BIA)** đề cập đến một phân tích về tác động của việc mất chức năng của một hoạt động EC (ví dụ: mua sắm điện tử, đặt hàng điện tử) cho một tổ chức. Một khi rủi ro như vậy được tính toán, tổ chức nên tập trung chiến lược quốc phòng vào những rủi ro lớn nhất.

#### **Vấn đề đạo đức**

Thực hiện các chương trình bảo mật đặt ra một số vấn đề đạo đức. Đầu tiên, một số người chống lại việc giám sát mọi hoạt động của cá nhân. Áp dụng một số biện pháp kiểm soát nhất định được một số người coi là vi phạm quyền tự do ngôn luận hoặc các quyền dân sự khác. Một cuộc khảo sát của Tập đoàn Gartner cho thấy ngay cả sau vụ tấn công khủng bố ngày 11 tháng 9 năm 2001, chỉ có 26% người Mỹ chấp thuận cơ sở dữ liệu ID quốc gia. Nhiều người thậm chí coi việc sử dụng sinh trắc học là vi phạm quyền riêng tư.

Lưu ý: Năm 2015, Quốc hội Hoa Kỳ gây áp lực với Tổng thống Obama khi lập ID sinh trắc học quốc gia cho tất cả người Mỹ (Newman [2015](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR83) ). Đề nghị này vẫn đang được thảo luận.

Xử lý sự riêng tư so với tiến thoái lưỡng nan về bảo mật là khó khăn. Có những nghĩa vụ đạo đức và pháp lý khác có thể yêu cầu các công ty phải xâm phạm quyền riêng tư của nhân viên và theo dõi hành động của họ. Đặc biệt, các biện pháp bảo mật CNTT là cần thiết để bảo vệ chống lại mất mát, trách nhiệm pháp lý và kiện tụng.

### Tại sao khó ngăn chặn tội phạm Internet?

Sau đây là những lý do chính khiến tội phạm Internet rất khó ngăn chặn.

#### **Làm cho mua sắm không thuận tiện**

Bảo mật EC mạnh có thể làm cho việc mua sắm trực tuyến trở nên bất tiện và cũng có thể làm chậm thời gian mua sắm. Do đó, người mua hàng có thể không thích một số biện pháp bảo mật.

#### **Thiếu sự hợp tác của các đối tác kinh doanh**

Có sự thiếu hợp tác tiềm năng từ các tổ chức phát hành thẻ tín dụng, nhà cung cấp, các ISP trong nước và đặc biệt là nước ngoài và các đối tác kinh doanh khác. Nếu ISP nguồn sẽ hợp tác và đình chỉ quyền truy cập của hacker, sẽ rất khó để tin tặc truy cập vào hệ thống.

#### **Tiêu cực của người mua sắm**

Nhiều người mua hàng trực tuyến không thực hiện các biện pháp phòng ngừa cần thiết (nhưng bất tiện) để tránh trở thành nạn nhân của hành vi trộm cắp danh tính hoặc gian lận (ví dụ: thay đổi mật khẩu).

#### **Bỏ qua các thực tiễn tốt nhất về bảo mật của EC**

Nhiều công ty không có quản lý bảo mật CNTT thận trọng hoặc nhận thức về bảo mật nhân viên. Nhiều mối đe dọa phổ biến ở Hoa Kỳ xuất phát từ việc thiếu nhận thức của người dùng về phần mềm độc hại và các cuộc tấn công hack. Ngoài ra, nhiều doanh nghiệp không đáp ứng các tiêu chuẩn tuân thủ bảo mật (xem Blog [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR10) ).

#### **Vấn đề thiết kế và kiến ​​trúc**

Người ta biết rằng việc ngăn ngừa lỗ hổng trong giai đoạn thiết kế và thực hiện trước EC ít tốn kém hơn nhiều so với việc giảm thiểu các vấn đề sau này; Thật không may, phòng ngừa như vậy không phải lúc nào cũng được thực hiện. Ngay cả các lỗi thiết kế nhỏ cũng có thể làm tăng hack.

#### **Thiếu cẩn thận trong thực tiễn kinh doanh**

Một lý do khác cho khó khăn là thiếu sự quan tâm đúng mức trong việc thực hiện nhiều quy trình kinh doanh (ví dụ, trong dịch vụ đám đông). Các **tiêu chuẩn về chăm sóc do** là tối thiểu và tập quán rằng một công ty dự kiến sẽ hợp lý để áp dụng để bảo vệ các công ty và các nguồn lực của mình trước các rủi ro có thể. Đối với một cuộc khảo sát lớn, xem PwC ( [2013](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR91) ).

### Bảo vệ thiết bị di động và ứng dụng di động

Với sự phát triển bùng nổ của tính di động và thương mại di động, nhiệm vụ bảo vệ các hệ thống này khỏi các vấn đề bảo mật được mô tả trước đó trong chương này và từ một số vấn đề mới. Để biết tổng quan, xem Faulkner ( [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR27) ). Đối với một dự đoán được thực hiện bởi Gartner Consulting, xem Krishnan ( [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR66) ).

#### **Vấn đề bảo mật di động**

Các vấn đề bảo mật điển hình bao gồm từ việc truyền không dây không được mã hóa đến thiếu tường lửa hoặc mật khẩu trên thiết bị di động hoặc kết nối với mạng Wi-Fi không bảo mật.

Reisinger ( [2014](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR93) ) liệt kê các vấn đề bảo mật bổ sung như trộm dữ liệu và mở khóa các thiết bị bẻ khóa. Sự phổ biến của BYOD cũng mang đến các mối đe dọa cho doanh nghiệp (xem Faulkner [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR27) ) và Security News ( [2016](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR101) ).

#### **Hệ thống phòng thủ của hệ thống di động**

Để bảo vệ các hệ thống di động, cần thực hiện các công cụ và quy trình như được mô tả trong phần [Hệ thống thông tin bảo vệ và thương mại điện tử bao gồm các hệ thống di động](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#Sec113) và sửa đổi chúng cho môi trường di động. Một danh sách kiểm tra thực tế để giảm rủi ro bảo mật được cung cấp bởi Lenovo ( [2013](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR72) ). Cuối cùng, một vấn đề lớn là trộm cắp thiết bị di động. Hai giải pháp đang hoạt động: thứ nhất, bảo mật tự động chỉ cho phép chủ sở hữu sử dụng thiết bị của họ và thứ hai, biến công tắc tiêu diệt thành một tính năng bắt buộc trong tất cả các điện thoại thông minh. Năm 2016, tính năng này vẫn chỉ khả dụng ở California.

#### **Những thứ bảo mật trong Internet**

IoT rất dễ bị tấn công bởi tội phạm mạng. Trong IoT, người ta có thể tìm thấy một số lượng lớn thiết bị từ các nhà sản xuất và rượu vang khác nhau được kết nối với một hệ thống. Nếu kết nối thông qua Internet, tình hình có thể còn tồi tệ hơn. Theo DeNisco ( [2017](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR24) ), có rất nhiều rủi ro bảo mật trong IoT. Tác giả dựa trên kết luận về báo cáo của Gartner. Báo cáo ước tính rằng hơn 8.4 tỷ thiết bị đã được kết nối với Internet. Hầu hết người dùng là người tiêu dùng cá nhân (5,2 tỷ thiết bị) và doanh nghiệp 3,1 tỷ (thiết bị). Ô tô và xe tải đang được kết nối với Internet là tốt. Gartner cũng dự đoán rằng vào năm 2018, sẽ có 1 tỷ thiết bị công nghiệp chéo. Tất cả những điều này góp phần vào rủi ro bảo mật.

McLellan ( [2017](https://link.springer.com/chapter/10.1007%2F978-3-319-58715-8_11#CR76) ) cung cấp một báo cáo miễn phí, toàn diện, dài 47 trang về cách khai thác IoT trong doanh nghiệp (bạn cần đăng ký, nhưng không phải trả phí, để nhận báo cáo).

**Các vấn đề quản lý**

Một số vấn đề quản lý liên quan đến chương này được nêu dưới đây.

1. Những bước nào các doanh nghiệp nên làm theo trong việc thiết lập một kế hoạch bảo mật? Quản lý bảo mật là một quá trình liên tục bao gồm ba giai đoạn: xác định tài sản, đánh giá rủi ro và triển khai. Bằng cách chủ động giám sát các chính sách và quy trình bảo mật hiện có, các công ty có thể xác định xem chúng có thành công hay không thành công, cái nào nên được sửa đổi hoặc loại bỏ. Tuy nhiên, điều quan trọng là phải giám sát các thay đổi trong quy trình kinh doanh và môi trường kinh doanh từ đó điều chỉnh các kế hoạch cho phù hợp. Theo cách này, một tổ chức có thể giữ các chính sách và các biện pháp bảo mật được cập nhật.
2. Các tổ chức có nên quan tâm đến các mối đe dọa an ninh nội bộ? Ngoại trừ phần mềm độc hại, các vi phạm do người trong tổ chức có thể xảy ra thường xuyên hơn so với các hành vi do người ngoài thực hiện. Điều này đúng cho cả các trang web B2C và B2B. Các chính sách và biện pháp bảo mật cho các trang web thương mại điện tử cần phải giải quyết các mối đe dọa trong nội bộ. Ngoài ra, người trong cuộc có thể là nạn nhân của tội phạm an ninh. Do đó, các công ty nên giáo dục nhân viên, đặc biệt là nhân viên mới, về các mối đe dọa như vậy.
3. Chìa khóa để thiết lập bảo mật thương mại điện tử mạnh mẽ là gì? Hầu hết các cuộc thảo luận về bảo mật tập trung vào công nghệ, với các tuyên bố như, tất cả các tin nhắn nên được mã hóa. Mặc dù các công nghệ rất quan trọng, không có giải pháp bảo mật nào hữu ích trừ khi được nhân viên áp dụng. Xác định các yêu cầu kinh doanh là bước đầu tiên trong việc tạo ra một giải pháp bảo mật.
4. Chúng ta nên làm gì trong trường hợp chúng ta là nạn nhân của tấn công đòi tiền chuộc? Sẽ không tốt cho bạn nếu bạn không có hệ thống dự phòng. Tuy nhiên, bạn có thể phải trả tiền để lấy lại dữ liệu của mình. Nếu tiền chuộc được yêu cầu để tránh DoS, hãy nhanh chóng cố gắng thiết lập bảo vệ để tránh sự cố lan rộng. Trong cả hai trường hợp, nên báo cáo vụ việc với cảnh sát.

**Tổng kết**

1. **Tầm quan trọng và giá trị của bảo mật thông tin thương mại điện tử**. Để thương mại điện tử thành công, nó phải được bảo mật. Thật không may, đây không phải là một nhiệm vụ dễ dàng do nhiều có mối nguy hiểm vô ý và cố ý. Sự cố bảo mật và vi phạm làm gián đoạn các giao dịch thương mại điện tử và tăng chi phí kinh doanh trực tuyến. Thiết kế Internet là dễ bị tổn thương, và sự cám dỗ để phạm tội máy tính đang gia tăng với các ứng dụng và khối lượng thương mại điện tử tăng lên. Tội phạm đang mở rộng hoạt động, tạo ra một nền kinh tế ngầm chứa thông tin đánh cắp có giá trị. An ninh thương mại điện tử sẽ vẫn còn phát triển vì các mối đe dọa đang thay đổi liên tục. Do đó, kinh doanh điện tử cần phải thích nghi. Một chiến lược bảo mật thương mại điện tử là cần thiết để tối ưu hóa năng suất cũng như sự phát triển của doanh nghiệp.
2. **Các vấn đề bảo mật thương mại điện tử cơ bản**. Vấn đề bảo mật có thể được xem là một trận chiến không hồi kết giữa những kẻ tấn công và những người phòng vệ. Có nhiều biến thể ở cả hai phía và nhiều tình huống va chạm có thể xảy ra. Chủ sở hữu các trang web thương mại điện tử cần quan tâm đến nhiều vấn đề bảo mật: xác thực, xác minh danh tính của những người tham gia giao dịch; ủy quyền, đảm bảo rằng một người hoặc tiến trình có quyền truy cập vào các hệ thống hoặc dữ liệu cụ thể; và kiểm toán, có thể xác định liệu các hành động cụ thể đã được thực hiện và bởi ai.
3. **Mối nguy hiểm, lỗ hổng bảo mật và các cuộc tấn công kỹ thuật**. Các trang web thương mại điện tử phải đối mặt với một loạt các cuộc tấn công. Tấn công có thể là phi kỹ thuật (kỹ thuật xã hội), trong đó một tên tội phạm dụ dỗ mọi người tiết lộ thông tin cá nhân nhạy cảm. Ngoài ra, các cuộc tấn công có thể là kỹ thuật, theo đó chuyên môn về phần mềm và hệ thống được áp dụng để tấn công vào các mạng, cơ sở dữ liệu hoặc chương trình. Các cuộc tấn công DoS khiến hoạt động bị đình trệ bằng cách gửi một lượng lớn dữ liệu đến các máy tính và trang web cụ thể. Các cuộc tấn công mã độc bao gồm virus, worm, Trojan hay sự kết hợp giữa chúng. Trong vài năm qua, các xu hướng phần mềm độc hại mới đã xuất hiện, chẳng hạn như Blackhole và ZeroAccess (nguồn: https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophos\_from\_blackhole\_to\_zeroaccess\_wpna.pdf). Các xu hướng mới bao gồm sự gia tăng về tốc độ cũng như số lượng của các phương thức tấn công mới, thời gian ngắn hơn giữa việc phát hiện ra lỗ hổng và bắt đầu một cuộc tấn công (để khai thác lỗ hổng). Cuối cùng, các xu hướng mới bao gồm việc sử dụng bot để khởi động các cuộc tấn công; sự gia tăng các cuộc tấn công vào các hệ thống di động, mạng xã hội và các ứng dụng Web; và chuyển sang các cuộc tấn công có lợi nhuận.
4. **Gian lận internet, lừa đảo và thư rác**. Một loạt lớn các tội phạm Internet tồn tại. Đáng chú ý là đánh cắp danh tính rồi lạm dụng, lừa đảo trên thị trường chứng khoán, gian lận... Lừa đảo cố gắng để có được thông tin có giá trị từ mọi người bằng cách giả mạo như một thực thể đáng tin cậy. Thông tin cá nhân được trích xuất từ mọi người (hoặc bị đánh cắp) và bán cho tội phạm, những người sử dụng nó để thực hiện các tội phạm tài chính như chuyển tiền vào tài khoản của chính họ. Một lĩnh vực liên quan là việc sử dụng quảng cáo hoặc bán hàng không được yêu cầu thông qua thư rác.
5. **Đảm bảo thông tin**. Mô hình đảm bảo thông tin đại diện cho một quy trình quản lý bảo vệ dữ liệu và hệ thống máy tính bằng cách đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của chúng. Bảo mật là sự đảm bảo quyền riêng tư dữ liệu. Tính toàn vẹn là sự đảm bảo rằng dữ liệu là chính xác hoặc thông báo không bị thay đổi. Tính khả dụng là sự đảm bảo rằng quyền truy cập vào dữ liệu, trang web hoặc các hệ thống và ứng dụng thương mại điện tử có sẵn, đáng tin cậy và bị hạn chế cho người dùng được ủy quyền bất cứ khi nào họ cần.
6. **Đảm bảo kiểm soát truy cập thương mại điện tử và truyền thông.** Trong thương mại điện tử, các vấn đề giao tiếp giữa các đối tác thương mại là tối quan trọng. Trong nhiều trường hợp, các đối tác thương mại điện tử không biết các đối tác của họ, vì vậy họ cần giao tiếp bảo mật và xây dựng lòng tin. Niềm tin bắt đầu bằng việc xác thực các bên liên quan đến giao dịch, nghĩa là xác định các bên trong giao dịch cùng với các hành động mà họ được ủy quyền thực hiện. Xác thực có thể được thiết lập bằng một cái gì đó mà người ta biết (ví dụ: mật khẩu), thứ mà người ta có (ví dụ: thẻ căn cước) hoặc một số đặc điểm vật lý (ví dụ: dấu vân tay). Hệ thống sinh trắc học có thể xác nhận danh tính của một người. Máy quét vân tay, máy quét mống mắt, nhận dạng khuôn mặt và nhận dạng giọng nói là những ví dụ về hệ thống sinh trắc học.
7. **Gian lận trên Internet và làm thế nào để bảo vệ người tiêu dùng và người bán chống lại nó.** Bảo vệ là cần thiết vì không có sự tiếp xúc trực tiếp giữa người mua và người bán; dẫn đến khả năng lớn xảy ra gian lận; không có đủ các ràng buộc pháp lý; các vấn đề mới và lừa đảo xuất hiện liên tục.
8. **Tại sao rất khó để ngăn chặn tội phạm máy tính?** Người mua hàng trực tuyến không thực hiện các biện pháp phòng ngừa cần thiết để tránh trở thành nạn nhân. Thiết kế và kiến trúc hệ thống an ninh vẫn rất dễ bị tấn công. Mọi doanh nghiệp thương mại điện tử đều biết rằng có các mối đe dọa về thẻ tín dụng bị đánh cắp, vi phạm dữ liệu, lừa đảo, phần mềm độc hại và vi rút không bao giờ kết thúc và các mối đe dọa này phải được giải quyết một cách toàn diện và chiến lược.
9. **Tương lai của thương mại điện tử.** Thương mại điện tử đang phát triển ổn định và nhanh chóng, mở rộng để bao gồm các sản phẩm, dịch vụ, mô hình kinh doanh mới. Các lĩnh vực tăng trưởng đáng chú ý nhất là sự tích hợp của thương mại trực tuyến và ngoại tuyến, thương mại di động (chủ yếu là ứng dụng điện thoại thông minh), tiếp thị dựa trên video và phương tiện truyền thông mạng xã hội. Một số công nghệ mới nổi, từ các ứng dụng thông minh đến các thiết bị đeo được, đang tạo điều kiện cho thương mại điện tử phát triển. Mặt khác, một số yếu tố đang làm chậm sự phát triển của thương mại điện tử như lo ngại về bảo mật và quyền riêng tư, băng thông hạn chế và thiếu tiêu chuẩn trong một số lĩnh vực thương mại điện tử.

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

Dyn là một công ty quản lý hiệu suất Internet (IPM) dựa trên đám mây, cung cấp khả năng hiển thị và kiểm soát các tài nguyên Internet công cộng và đám mây (một công ty của Oracle). Công ty kiểm soát và tối ưu hóa cơ sở hạ tầng giúp nhanh hơn, an toàn hơn và cung cấp dịch vụ đáng tin cậy hơn. Dyn cung cấp dịch vụ hệ thống tên miền (DNS), về cơ bản hoạt động như một sổ địa chỉ cho Internet. Công ty phục vụ các mạng lưới với hàng ngàn khách hàng. Để biết thêm về ngành công nghiệp IPM và Dyn, tham khảo <dyn.com/blog/what-is-iNET-performance-manloyment-industry-tech-talk-with-dyn-exceed>.

**Sự cố**

Nói ngắn gọn là vào ngày 21 tháng 10 năm 2016, bạn không thể truy cập Internet từ mạng Dyn. Kẻ tấn công Dyn, sử dụng DDoS, nhắm vào trụ sở chính của Dyn ở New Hampshire. Cuộc tấn công đầu tiên được phát động lúc 7h sáng và được Dyn giải quyết trong khoảng 2h. Một cuộc tấn công thứ hai bắt đầu vào khoảng giữa trưa và lần thứ ba vào khoảng 4 giờ chiều. Những kẻ tấn công đã bắn phá Dyn bằng một loạt các yêu cầu độc hại, được gửi từ hàng chục triệu địa chỉ IP. Kết quả là dịch vụ Internet của Dyn bị tạm dừng, chủ yếu ở Bờ Đông Hoa Kỳ và sau đó ở các vùng khác của đất nước. Cuộc tấn công diễn ra rất phức tạp và tinh vi.

**Kết quả**

Theo Newman (2016), “Dyn cung cấp dịch vụ hệ thống tên miền (DNS), về cơ bản hoạt động như một sổ địa chỉ cho Internet. DNS là một hệ thống phân giải các địa chỉ web mà chúng ta thấy hàng ngày, như Wired.com, thành các địa chỉ IP tương ứng để tìm kiếm và kết nối. Một cuộc tấn công DDoS làm quá tải máy chủ DNS với các yêu cầu tra cứu, khiến nó không có khả năng hoàn thành bất kỳ tra cứu nào nữa. Trước đó, Dyn đã trải qua các cuộc tấn công DDoS và chiến đấu với chúng thành công, nhưng đó là những cuộc tấn công với quy mô nhỏ. Quy mô và độ tinh vi của cuộc tấn công này là quá lớn đối với Dyn để bảo vệ, vì vậy việc truy cập vào hàng trăm trang web và dịch vụ đã bị phá vỡ bởi cuộc tấn công. Cuộc tấn công này nêu bật mức độ quan trọng của DNS trong việc duy trì dịch vụ Internet ổn định và an toàn.