**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.