CHƯƠNG 5

Bảo mật dữ liệu và An ninh mạng

|  |  |
| --- | --- |
| TỔNG KẾT CHƯƠNG | MỤC TIÊU HỌC TẬP |
| Trường hợp 5.1 Vụ việc mở đầu : Yahoo bị phạt 117,5 triệu đô la vì vụ hack dữ liệu tồi tệ nhất trong lịch sử y |  |
| 5.1 Quyền riêng tư về dữ liệu y Mối quan tâm và Quy định | 5.1 Mô tả bốn mối quan tâm chính về quyền riêng tư về dữ liệu xác định aradox y\_p riêng tư và mô tả các quy định về bảo mật dữ liệu đang bảo vệ người tiêu dùng như thế nào . |
| 5.2 Mức độ và chi phí của các cuộc tấn công C y và các mối đe dọa C | 5.2 Xác định mức độ và chi phí của các cuộc tấn công mạng và 12 loại tấn công mạng có chủ ý và không chủ ý khác nhau . |
| 5.3 Mục tiêu tấn công và hậu quả | 5.3 Thảo luận về sáu mục tiêu nguy hiểm nhất của các cuộc tấn công mạng và cung cấp một ví dụ về cách mỗi tác nhân tác động đến người tiêu dùng và các hoạt động Qlg . |
| 5.4 Bảo vệ chống lại các cuộc tấn công C y và quản lý rủi ro | 5.4 Xác định sáu chiến lược phòng thủ mạng và bốn phương pháp tiếp cận quản lý rủi ro và các công cụ phòng thủ CNTT có thể được sử dụng để bảo vệ hoặc tổ chức khỏi các cuộc tấn công mạng . |
| 5.5 Bộ điều khiển và Bộ điều khiển Khung và Mô hình | 5.5 Xác định năm biện pháp kiểm soát phòng thủ chung chính , tám biện pháp kiểm soát phòng thủ ứng dụng chính cũng như các quy định và khuôn khổ giúp Lp bảo vệ người tiêu dùng và hướng dẫn quản trị CNTT . |
| Tình huống 5.2 Tình huống kinh doanh: Tập đoàn Marriott đa quốc gia  Các khách sạn có thể đối mặt với phản ứng dữ dội của người tiêu dùng và tăng lên Sl  hàng tỷ cho  Vi phạm dữ liệu lớn |  |
|

Trường hợp 5.1 Mở trường hợp

# 8 PHÓNG SỰ

Yahoo bị phạt 117,5 triệu đô la vì vụ hack dữ liệu tồi tệ nhất trong lịch sử

Nhờ giải quyết vụ kiện tập thể gần đây, bạn có thể được hưởng hai năm dịch vụ giám sát tín dụng miễn phí bằng AllClear ID hoặc tối đa $358,80 tiền mặt. Nếu bạn có tài khoản Yahoo từ ngày 1 tháng 1 năm 2012 đến

vào ngày 31 tháng 12 năm 2016 và là cư dân của Hoa Kỳ hoặc Israel, bạn có thể gửi yêu cầu tại www.yahoodatabreachsettlement.com trước tháng 7 năm 2020 để bồi thường cho những tổn thất của bạn. Vụ kiện tập thể đã được đưa ra chống lại Yahoo vì không chỉ một mà là hai vụ vi phạm dữ liệu lớn nhất được biết đến trong lịch sử. Phán quyết dàn xếp đã được thực hiện trong ba năm,

Mãi cho đến mùa thu năm 2016, Yahoo mới cảnh báo người dùng và công chúng về một vụ vi phạm dữ liệu lớn đối với thông tin cá nhân của người dùng đã xảy ra 2-3 năm trước đó. Vào ngày 22 tháng 9 năm 2016, Yahoo đã tiết lộ công khai rằng hơn 1

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

|  |
| --- |
| tỷ hồ sơ tài khoản Yahoo đã bị đánh cắp một thời gian trong năm 2014. Vào tháng 12 năm 2016, Yahoo đã công bố một vụ hack khác kể từ năm 2013, mà họ cho biết đã ảnh hưởng đến 1 tỷ hồ sơ người dùng. Tác động của vụ hack thứ hai sau đó đã được cập nhật trong một bản tin tháng 10 năm 2017 khi Yahoo tiết lộ rằng 3 tỷ tài khoản Yahoo đã thực sự bị xâm phạm, khiến đây là vụ vi phạm dữ liệu lớn nhất trong lịch sử. Sự chậm trễ trong việc báo cáo một phần là do chính Yahoo đã không biết về vi phạm cho đến khi công bố những tuyên bố này ra công chúng một thời gian ngắn. Thông tin bị rò rỉ trong các cuộc tấn công bao gồm tài khoản e-mail, số điện thoại, địa chỉ đường phố, câu hỏi và câu trả lời bảo mật không được mã hóa, nhưng không có thông tin tài chính.      Để làm trầm trọng thêm vấn đề đối với Yahoo, công ty đang đàm phán với tập đoàn lớn Verizon để mua lại Yahoo với giá 4,83 tỷ USD, Verizon nói rằng thông báo ban đầu có thể có tác động tiêu cực đến quyết định mua hàng của họ. Bản phát hành tháng 12 năm 2016 đã khiến Verizon xem xét thêm các tác động tài chính của hai vi phạm và giảm đề nghị mua lại Yahoo xuống 350 triệu đô la.    Vụ vi phạm năm 2013 được thực hiện bởi một bên thứ ba trái phép không xác định. Thông tin bị đánh cắp trong vụ tấn công năm 2014 đã được bán bởi một "diễn viên được nhà nước bảo trợ" trên Dark Web với giá 3 Bitcoin (khoảng 1.900 USD). Diễn viên mà    đã sử dụng tên "Peace", có nguồn gốc từ Nga và đã cố gắng bán dữ liệu của 200 triệu người dùng Yahoo trực tuyến. Yahoo kêu gọi tất cả người dùng thay đổi mật khẩu và câu hỏi bảo mật, đồng thời xem xét tài khoản của họ để phát hiện hoạt động đáng ngờ. Cho đến nay, có rất ít thông tin về vụ vi phạm năm 2013 được tiết lộ, nhưng người ta biết nhiều hơn về vụ việc xảy ra vào năm 2014.  Cuộc tấn công thứ hai được thực hiện như thế nào  Việc đánh cắp dữ liệu tương tự như cách thức thực hiện một cuộc tấn công trực tuyến điển hình vào cơ sở dữ liệu. Các biện pháp bảo vệ được sử dụng cho cơ sở dữ liệu chứa thông tin đăng nhập và thông tin cá nhân không đủ để bảo vệ chống lại các phương pháp tiên tiến mà tin tặc sử dụng. Trong trường hợp này, phương pháp mã hóa được sử dụng trong cơ sở dữ liệu đã bị tin tặc phá vỡ. Ngoài ra; nhà phân tích tội phạm mạng Vitali Kremez khẳng định rằng: tin tặc đã đánh cắp thông tin từ Yahoo một cách chậm rãi và có phương pháp để không thu hút sự chú ý đến vụ vi phạm đang diễn ra.    Vì vi phạm không được phát hiện ngay lập tức nên tin tặc có nhiều thời gian để tận dụng thông tin đó theo cách có lợi về mặt tài chính, cá nhân hoặc chính trị. Không rõ liệu người bán có phải là hacker ban đầu hay không.  Tác động của vi phạm dữ liệu    Vì các vụ vi phạm quá tàn khốc và ảnh hưởng sâu rộng đến hầu hết cơ sở khách hàng của Yahoo, nên Verizon đang phải suy nghĩ lại về việc mua lại. Craig Silliman, cố vấn chung của Verizon, cho biết Verizon có "cơ sở hợp lý" để tin rằng việc vi phạm dữ liệu sẽ có tác động đáng kể đến thủ tục thỏa thuận và khả năng nó sẽ xảy ra (Fiegerman, 2016 ) . Anh ấy vui vẻ giải thích rằng Yahoo sẽ phải thuyết phục Verizon rằng vi phạm sẽ không ảnh hưởng đến các quy trình trong tương lai của công ty và rằng nhiều tính năng bảo mật hơn sẽ có.    đã và sẽ thực hiện. Ngoài ra, các sự cố có thể làm cho thỏa thuận Yahoo trị giá khoảng 200 triệu đô la ít hơn 4,3 tỷ đô la được giải quyết ban đầu. Ngoài việc giảm giá trị tài sản cốt lõi của Yahoo,  cổ phiếu của công ty đã giảm khoảng 2 0 /o sau những bình luận của Craig Sillimall'          Công lý được phục vụ  Vào ngày 17 tháng 3 năm 2017, Bộ Tư pháp Hoa Kỳ đã truy tố hai nhân viên Tình báo Nga và hai tin tặc được nhà nước bảo trợ, Alexsey Belan và Karim Baratov, vì hành vi trộm cắp dữ liệu người dùng Yahoo vào năm 2014. Belan, một trong những tin tặc hình sự khét tiếng nhất của FBI, đã •đã từng bị truy tố trong hai trường hợp khác. Trong bản cáo trạng, người ta tiết lộ rằng các mục tiêu của vụ trộm bao gồm các nhà báo Nga, quan chức chính phủ Hoa Kỳ và Nga, quân nhân và nhân viên lĩnh vực pr của các công ty tài chính, vận tải và các công ty khác. Vụ kiện chống lại Yahoo cuối cùng đã được giải quyết vào tháng 10 năm 2019 khi Yahoo được lệnh phải trả 117,5 triệu đô la tiền bồi thường cho người dùng của mình. Thỏa thuận dàn xếp đang chờ phê duyệt cuối cùng của tòa án được ấn định vào ngày 2 tháng 4 năm 2020.  câu hỏi |

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Bạn nghĩ tại sao Yahoo lại là mục tiêu cho những vi phạm dữ liệu này?

Tại sao Yahoo không công khai các vi phạm? Việc họ không tiết lộ thông tin ảnh hưởng như thế nào đến mối quan hệ của Yahoo với khách hàng và đối tác của mình?

• Ngoài việc dữ liệu bị đánh cắp, sự cố này còn gây thiệt hại gì nữa?

Những sự cố an ninh mạng này có thể thấy trước được không? Chúng có thể tránh được không?

Giả sử rằng CEO và CIO bị buộc phải từ chức, điều đó gửi thông điệp gì đến ban lãnh đạo cấp cao của Yahoo?

Nguồn; Tổng hợp từ Fiegerman ( 2016 ), Hackett ( 2016a ), Kan ( 2016 ), Lee ( 2016 ), Matwyshyn và Bhargava ( 2016 ), Murgia Sterling ( 2015 ), Balakrishnan ( 2017 ), Clement ( 2019 ), Colby ( 2019 ), và Tyko (2019 ),

|  |
| --- |
| BẠN CÓ BIẾT KHÔNG?  Hầu hết mọi người đều đã từng bị hack tài khoản e-mail thông qua mật khẩu của họ. Để kiểm tra xem liệu bạn có phải là một trong số ít người có tài khoản chưa bị xâm phạm hay không, bạn có thể nhập địa chỉ email của mình tại https:ffhaveibeenpwned.com/, Nếu bạn là một trong số nhiều người đã bị xâm phạm tài khoản, bạn' sẽ có thể xem lại danh sách các vi phạm. |

## Giới thiệu

Trong thế giới kết nối ngày nay, điều cần thiết là dữ liệu và mạng"được thảo luận trong Chương 3 và 4 phải được bảo vệ khỏi truy cập trái phép, giả mạo và phá hoại. Casð mở của chúng tôi chỉ là một ví dụ về sự coi thường trắng trợn mà một số công ty có thể có đối với dữ liệu của một cá nhân quyền riêng tư và hành vi không thể tha thứ của tin tặc đã đánh cắp dữ liệu để nổi tiếng hoặc Một số thách thức bảo mật và quyền riêng tư dữ liệu khó khăn nhất hiện nay thậm chí không tồn tại vào đầu thập kỷ này. Các công nghệ mới nhất như mạng xã hội, di động và đám mây là những lực lượng mạnh có thể làm tổn hại đến quyền riêng tư của thông tin cá nhân và phá vỡ các biện pháp bảo mật cần được thực hiện để bảo vệ thông tin đó. . 

Do đó, các tổ chức cần hiểu sâu hơn về cách thức và thời điểm các cuộc tấn công mạng có thể xảy ra, đồng thời kết hợp hiểu biết đó với bối cảnh kinh doanh, kỹ thuật định giá và định lượng tài chính để xác định chi phí thiệt hại thực sự của họ. Áp dụng kiến thức chính xác hơn về các tác động kinh doanh tiềm ẩn này, các nhà lãnh đạo có thể quản lý và kiểm soát rủi ro mạng hiệu quả hơn nhiều, đồng thời cải thiện khả năng phục hồi sau một cuộc tấn công mạng.

Bạn và công ty của bạn đã sẵn sàng để giải quyết hiệu quả các vấn đề về quyền riêng tư và trách nhiệm của công ty mà công nghệ xã hội, di động, dữ liệu lớn và phân tích tạo ra trong kinh doanh chưa? Nghiên cứu giai thoại cho thấy câu trả lời là "Không"! Nhiều người thậm chí không nhận ra khi các vấn đề về quyền riêng tư xuất hiện. Nếu mọi người và các công ty không thể nhận ra các vấn đề, thì thật khó để tưởng tượng họ có thể hành động có trách nhiệm như thế nào để chống lại chúng.

Trong chương này, bạn sẽ tìm hiểu về một số mối quan ngại về quyền riêng tư CNTT và cách các công ty và chính phủ giải quyết vấn đề Những vấn đề này sẽ được xem xét trong bối cảnh quy định, kết quả nghiên cứu và ví dụ điển hình. Tất nhiên, không có câu trả lời dễ dàng nào cho sự sụp đổ của quyền riêng tư, vi phạm bản quyền và trộm cắp tài sản trí tuệ. Không có sửa chữa dễ dàng, phán đoán hoặc giải pháp rõ ràng. Là người dùng có hiểu biết, bạn cần có khả năng nhận ra các vấn đề về quyền riêng tư khi chúng phát sinh và biết các loại biện pháp bảo mật và sáng kiến quản lý rủi ro cần được áp dụng để bảo vệ nhân viên, khách hàng và các bên liên quan

Bạn cũng sẽ tìm hiểu về thuật ngữ an ninh mạng, số vụ vi phạm dữ liệu ngày càng tăng, nguồn đe dọa mạng, các loại' thiệt hại do chiến thuật hung hãn của tội phạm mạng gây ra và tác động của chúng đối với các tổ chức. Cuối cùng, bạn sẽ tìm hiểu cách các tổ chức có thể bảo vệ chống lại các cuộc tấn công mạng, đánh giá chính xác thiệt hại mà chúng gây ra và đảm bảo rằng các sáng kiến quản lý rủi ro cần thiết cho hoạt động kinh doanh liên tục được triển khai và đáp ứng các yêu cầu của quy định .

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

## 5.1 Mối quan tâm và Quy định về Quyền riêng tư Dữ liệu

L05.1 Mô tả bốn mối quan tâm chính về quyền riêng tư dữ liệu, xác định nghịch lý về quyền riêng tư và mô tả cách các quy định về quyền riêng tư dữ liệu đang bảo vệ người tiêu dùng.

Dữ liệu riêng tư đang trở thành ưu tiên hàng đầu của các cá nhân, tổ chức và chính phủ trên toàn cầu. Các vấn đề về quyền riêng tư dữ liệu có thể phát triển xung quanh dữ liệu được thu thập từ nhiều nguồn, bao gồm hồ sơ chăm sóc sức khỏe, bằng lái xe, trích dẫn phương tiện , điều tra tội phạm, giao dịch với các tổ chức tài chính, thông tin sinh học (chẳng hạn như DNA) và



nơi cư trú và hồ sơ địa lý. Một tổ chức lớn duy nhất có thể sở hữu thông tin cá nhân của hàng triệu khách hàng. Để đảm bảo duy trì danh tiếng tốt, công ty phải đảm bảo rằng thông tin khách hàng của họ luôn an toàn và tốt nhất có thể.

Quyền riêng tư về dữ liệu là quyền tự quyết định thông tin nào về bạn được truy cập, cho ai, khi nào và cho việc sử dụng hay mục đích gì.

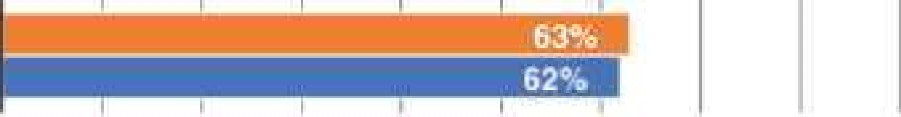
Quyền riêng tư dữ liệu đảm bảo rằng các cá nhân, nhóm và công ty có quyền tự do lựa chọn và kiểm soát thông tin cá nhân mà các công ty thu thập về họ, bao gồm cả những gì họ làm hoặc không muốn được chia sẻ hoặc sử dụng bởi những người khác và xoay quanh bốn mối quan tâm chính sau :

1. Cách dữ liệu được chia sẻ với bên thứ ba
2. Cách dữ liệu được thu thập và lưu trữ
3. Dữ liệu được sử dụng như thế nào
4. Dữ liệu được quy định như thế nào

Lượng thông tin cá nhân được chia sẻ là quyết định mà các cá nhân liên tục đưa ra. Đây là khái niệm quan trọng iS@Å vì nội dung trực tuyến có thể tồn tại suốt đời. Không thể làm cho nội dung riêng tư mà thanh thiếu niên có đánh giá xấu đã đăng hoặc gửi không bị cấm để biến mất khi họ nộp đơn xin việc yêu cầu kiểm tra an ninh hoặc kiểm tra lý lịch nghiêm ngặt hoặc tranh cử vào chức vụ công. Một quyết định sai lầm về loại thông tin mà một người chia sẻ có thể quay trở lại ám ảnh họ sau này trong cuộc đời.

### Bối rối, lo lắng và mất kiểm soát

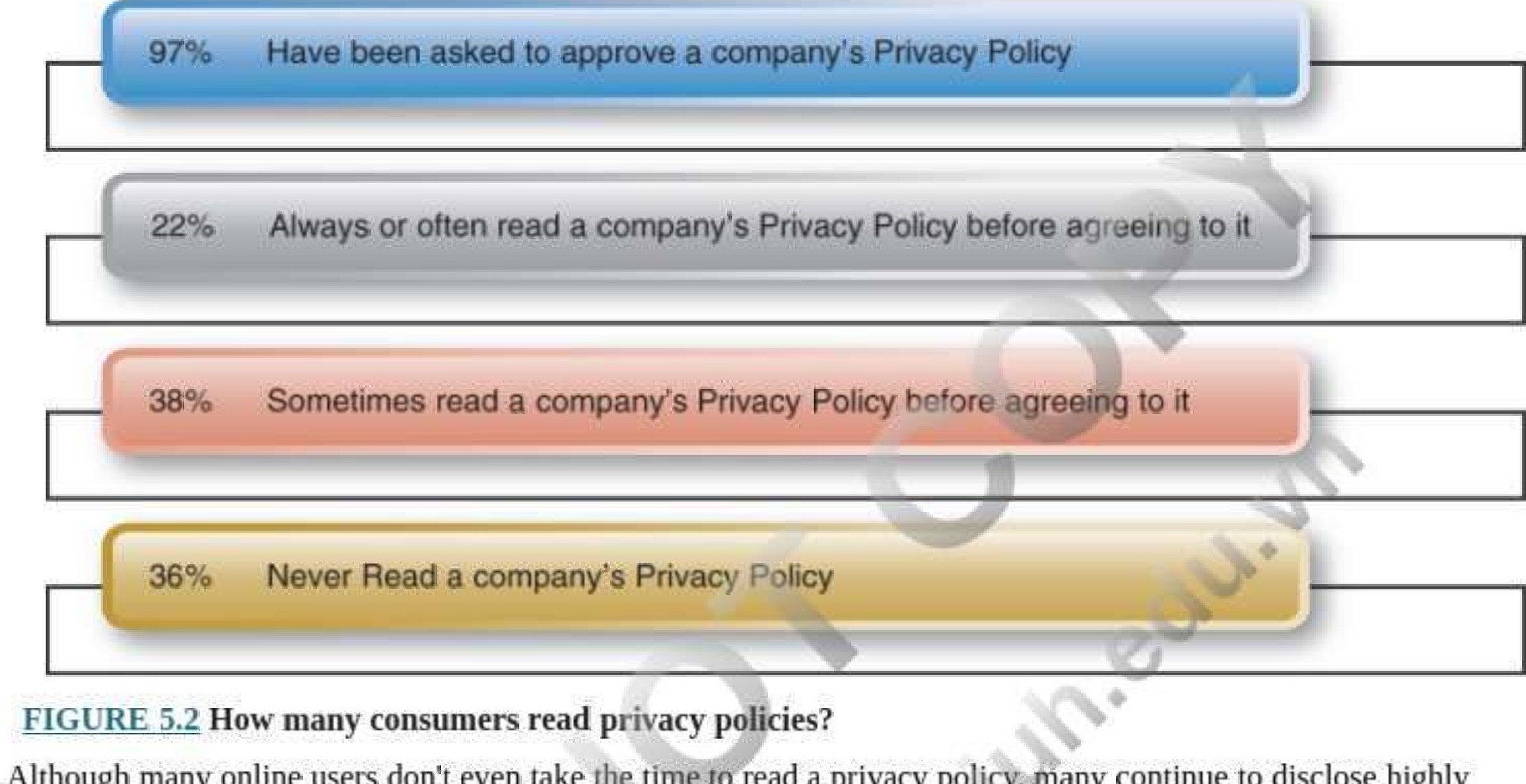
Trong một cuộc khảo sát quốc gia về quyền riêng tư năm 2019 (Auxier và cộng sự, 4.272 người trưởng thành ở Hoa Kỳ, Pew Research (www.pewresearch.org) đã báo cáo rằng phần lớn người Mỹ quan niệm sâu sắc về quyền riêng tư dữ liệu. Ví dụ: phần lớn không nghĩ rằng điều đó là có thể trải qua cuộc sống hàng ngày mà không bị các công ty và cơ quan chính phủ theo dõi, việc thu thập dữ liệu trực tuyến gây ra nhiều rủi ro hơn là lợi ích và họ cảm thấy mình có ít hoặc không kiểm soát được cách các công ty và chính phủ sử dụng dữ liệu cá nhân của họ, từ vị trí thực tế cho đến các bài đăng trên mạng xã hội . Ngoài ra, đại đa số có rất ít hoặc không tin tưởng rằng các công ty sẽ thừa nhận sai lầm và chịu trách nhiệm nếu họ sử dụng sai hoặc xâm phạm thông tin cá nhân của họ. ioyin cách họ cảm thấy thoải mái với

Không thể trải qua cuộc sống hàng ngày mà không có dữ liệu về tôi được thu thập

|  |  |
| --- | --- |
| Chính phủ | Các công ty |

HÌNH 5.1 Người Mỹ lo ngại, bối rối và cảm thấy mất kiểm soát về việc thu thập thông tin cá nhân của họ.

Bất chấp sự đồng thuận rộng rãi này đối với quyền riêng tư dữ liệu, rất ít người tiêu dùng thực sự thực hiện các bước để chia sẻ ít thông tin hơn hoặc xóa dữ liệu được thu thập về họ trực tuyến. Ví dụ: nhiều người thừa nhận họ ít quan tâm hoặc không quan tâm đến chính sách bảo mật và điều khoản dịch vụ. Mặc dù hầu hết tất cả đều nói rằng họ đã được yêu cầu phê duyệt chính sách quyền riêng tư nhưng chỉ 1/5 cho biết họ luôn hoặc thường xuyên đọc chính sách quyền riêng tư của công ty trước khi đồng ý. Hơn một phần ba nói rằng họ thỉnh thoảng đọc và khoảng tỷ lệ tương tự nói rằng họ chưa bao giờ đọc chính sách quyền riêng tư của công ty (Ví dụ 5.2). Trong số những người đọc chính sách riêng tư của công ty, chỉ một phần năm đọc hết nó trước khi đồng ý với các điều khoản của nó.

HÌNH 5.2 Có bao nhiêu người tiêu dùng đọc chính sách quyền riêng tư?

Mặc dù nhiều người dùng trực tuyến thậm chí không dành thời gian để đọc chính sách quyền riêng tư; nhưng mọi người vẫn tiếp tục tiết lộ các chi tiết mang tính cá nhân cao về cuộc sống hàng ngày của họ, bao gồm cả hành vi buộc tội hoặc hành vi phạm pháp, trong hồ sơ hoặc bài đăng của họ. Ví dụ: mặc dù là tâm điểm của các vụ bê bối về quyền riêng tư, nhưng trong một ngày, Facebook có hơn một tỷ người dùng chia sẻ ảnh và thông tin chi tiết về cuộc sống cá nhân của họ và người dùng gửi gần 2 triệu tin nhắn và tải gần 300 giờ video lên YouTube mỗi phút . Mua sắm trực tuyến cũng đang gia tăng, như được phản ánh bởi trang web siêu mua sắm trực tuyến Amazon đã báo cáo tổng tài sản là 199,1 tỷ đô la cho quý kết thúc vào ngày 30 tháng 9 năm 2019—tăng 38,56% so với năm 2018 ,

### Nghịch lý về quyền riêng tư

Sự không nhất quán giữa các nhu cầu cạnh tranh để sử dụng CNTT và có sự hiện diện trực tuyến, trong khi bảo vệ chống lại các mối đe dọa tiềm tàng đối với an toàn và quyền riêng tư cá nhân do sử dụng sai thông tin cá nhân được gọi là giải pháp riêng tư . Nghịch lý về quyền riêng tư xảy ra khi người dùng mạng xã hội và người tiêu dùng trực tuyến lo ngại về quyền riêng tư, nhưng hành vi của họ lại mâu thuẫn với những mối quan tâm này ở mức độ cực đoan.

Nghịch lý về quyền riêng tư là sự mất kết nối giữa mức độ quan trọng của mọi người đối với quyền riêng tư trực tuyến của họ so với cách họ thực sự cư xử trong cuộc sống thực.

Có thể lý giải rằng nghịch lý về quyền riêng tư có thể là do 78% người dân vẫn chưa thực sự hiểu thông tin cá nhân của họ đang được các công ty thu thập và sử dụng như thế nào và tỷ lệ thông tin được chính phủ thu thập và sử dụng thấp hơn một chút. (xem Hình 5.1 ). Cũng có thể lập luận rằng nghịch lý về quyền riêng tư có thể được giải thích bởi thực tế là các trang web xã hội đã trở nên gắn bó với đời sống xã hội của người dùng đến mức họ tiết lộ thông tin về bản thân mặc dù người ta thường biết rằng các trang web này không

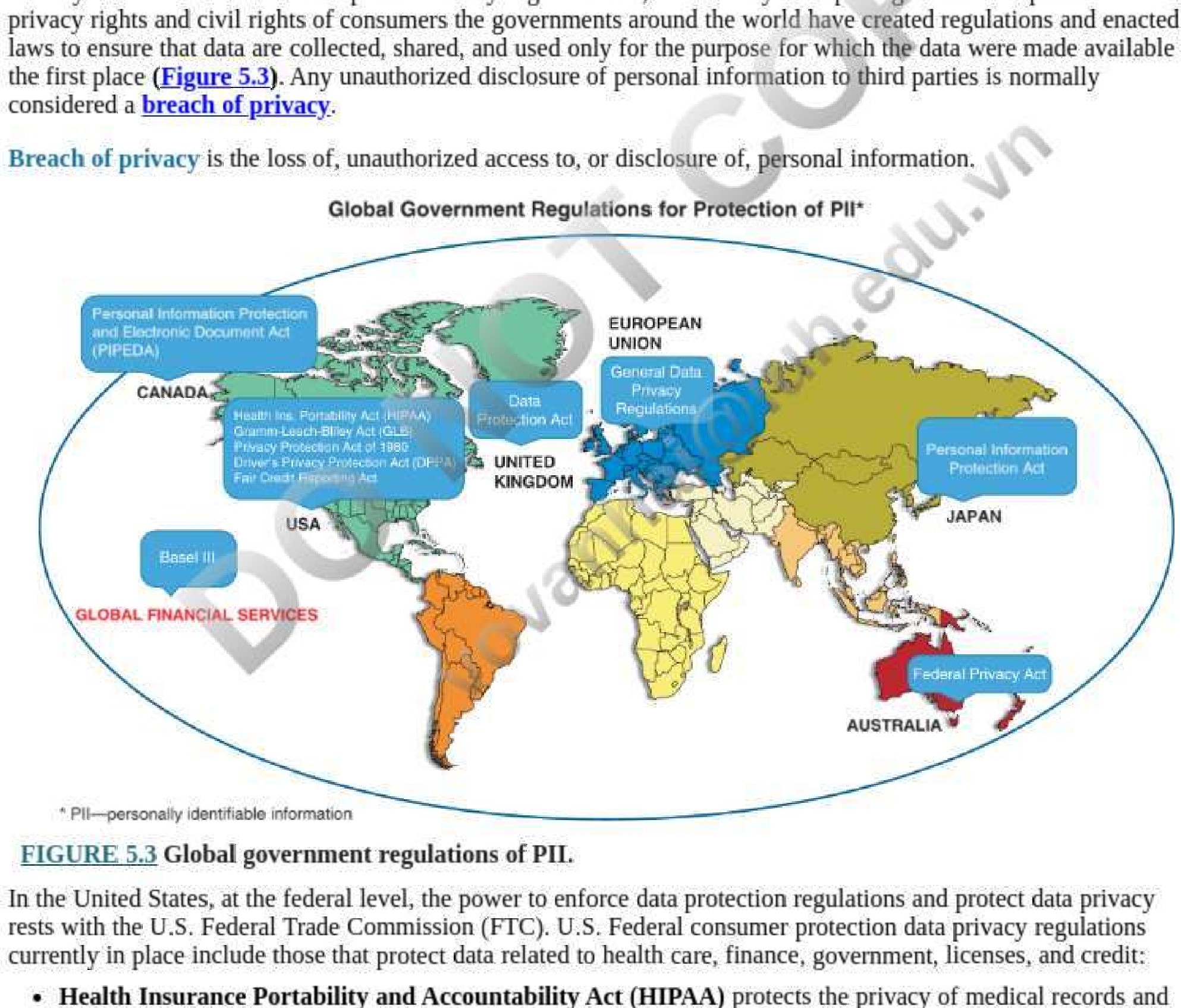
cung cấp đầy đủ các biện pháp kiểm soát quyền riêng tư và sẵn sàng chấp nhận hậu quả.

### Quyền riêng tư là quyền dân sự

Việc thu thập và phân tích dữ liệu ngày càng trở nên quan trọng đối với việc điều hành một doanh nghiệp và đang trở thành một phần không thể thiếu trong cách các doanh nghiệp cung cấp sản phẩm và dịch vụ cho khách hàng của họ. Kết quả là, mọi thứ được thực hiện trực tuyến đều tạo ra dữ liệu, phần lớn trong số đó được theo dõi. Dữ liệu được theo dõi được đưa vào các thuật toán mạnh mẽ để phân phối quảng cáo được cá nhân hóa và các dịch vụ khác xuất hiện trên các trang web mà chúng tôi truy cập. Mặc dù những điều này đôi khi có lợi, nhưng những thuật toán tương tự này có thể được sử dụng để tạo điều kiện cho sự phân biệt đối xử trong việc làm, cho vay mua nhà ở, thương mại điện tử và bỏ phiếu.

Ví dụ, hãy xem xét„các thuật toán tuyển dụng dự đoán tiết lộ các kiểu bất bình đẳng dựa trên các quyết định tuyển dụng và đánh giá việc làm trong quá khứ hoặc các quảng cáo phân biệt đối xử nhắm mục tiêu dựa trên các bài đăng trên Facebook dẫn đến việc loại trừ các ứng viên dựa trên các đặc điểm được bảo vệ như chủng tộc, giới tính và tình dục, Trong và cho vay một nghiên cứu của UC Berkeley đã phát hiện ra rằng những người cho vay thế chấp trực tuyến tính phí vay của người da đen và người Latinh nhiều hơn một cách có hệ thống đối với các khoản vay và các công ty như Home Depot và Staples đang tính giá cao hơn cho cùng một sản phẩm ở các địa điểm khác nhau dựa trên việc định giá trực tuyến của họ dựa trên nơi người mua đã sống. Và, tất cả chúng ta đều quen thuộc với các can thiệp trực tuyến của nước ngoài xảy ra trong cuộc bầu cử năm 2016 được thiết kế để tác động đến dư luận ủng hộ ứng cử viên này hơn ứng cử viên kia.

Tất cả những hành vi này đều coi thường các biện pháp bảo vệ quyền công dân được trao cho những loại phân biệt đối xử này, bao gồm Đạo luật Quyền Công dân năm 1964, Đạo luật Quyền Bầu cử năm 1965 và Đạo luật Nhà ở Công bằng năm 1968.



U.S.

Consumer

Protection

Data

Privacy

Regulations

Privacy

is

a

business-critical

discipline

for

many

organizations,

enforced

by

multiple

regulations.

To

protect

the

in

Health

Insurance

Portability

and

Accountability

Act

(HIPAA)

protects

the

privacy

of

medical

records

and

thông tin chăm sóc sức khỏe có thể nhận dạng cá nhân khác trừ khi đó là thông tin dành cho người cần thông tin vì họ tham gia vào quá trình xử lý thanh toán cho dịch vụ chăm sóc của người chăm sóc hoặc thông tin đó là cần thiết để hỗ trợ các hoạt động chăm sóc sức khỏe .

* Đạo luật GrammA-each-Bliley yêu cầu các tổ chức tài chính cung cấp các sản phẩm tài chính tiêu dùng 1S như khoản vay, tư vấn tài chính hoặc đầu tư hoặc bảo hiểm phải giải thích các hoạt động chia sẻ thông tin của họ cho khách hàng và để bảo vệ dữ liệu nhạy cảm,
* Đạo luật Bảo vệ Quyền riêng tư năm 1980 quy định việc một quan chức hoặc nhân viên chính phủ, liên quan đến việc điều tra hoặc truy tố một tội hình sự, tìm kiếm hoặc thu giữ bất kỳ tài liệu sản phẩm công việc nào được sở hữu bởi một người được cho là có mục đích phổ biến cho người khác là bất hợp pháp. công khai một tờ báo, cuốn sách, chương trình phát sóng hoặc hình thức xuất bản tương tự khác, trong hoặc ảnh hưởng đến thương mại giữa các tiểu bang hoặc nước ngoài,



* Đạo luật Bảo vệ Quyền riêng tư của Người lái xe (DPPA) bảo vệ thông tin nhận dạng cá nhân của những người lái xe được cấp phép khỏi việc sử dụng hoặc tiết lộ không đúng cách.
* Đạo luật Báo cáo Tín dụng Công bằng chi phối cách cơ quan báo cáo tín dụng có thể thu thập, truy cập, sử dụng và chia sẻ thông tin tín dụng để đảm bảo tính chính xác, công bằng và quyền riêng tư của thông tin trong hồ sơ của văn phòng tín dụng tiêu dùng. Luật về quyền riêng tư cấp tiểu bang của Hoa Kỳ

Mặc dù FTC có nhiều thẩm quyền đối với việc thực thi các quy định bảo vệ dữ liệu, nhưng không có luật liên bang về quyền riêng tư dữ liệu hoặc cơ quan bảo vệ dữ liệu trung tâm chịu trách nhiệm tuân thủ các quy định đó. Thay vào đó, hầu hết các quy định đều ở cấp tiểu bang và tổng chưởng lý tiểu bang đóng vai trò chính trong việc thực thi. Số lượng luật bảo mật dữ liệu cấp tiểu bang được ban hành trên khắp Hoa Kỳ đang tăng lên. Alf 50 tiểu bang của Hoa Kỳ đã thông qua luật thông báo vi phạm dữ liệu. Ít nhất 35 tiểu bang và Pueno Rico có luật xử lý dữ liệu và 25 tiểu bang đã ban hành luật bảo mật dữ liệu (Brooks, 2019) . 

Gần đây nhất và đáng chú ý nhất trong số này là Đạo luật về quyền riêng tư của người tiêu dùng California (CCPA) có hiệu lực vào ngày

Ngày 1 tháng 1 năm 2020 (Germain, 2020 ). Đây là phiên bản cập nhật của một đạo luật kém hiệu quả hơn đã được Cơ quan lập pháp bang California thông qua vào ngày 28 tháng 6 năm 2018 và cấp cho cư dân California các biện pháp bảo vệ quyền riêng tư mới mạnh mẽ hơn nhiều, một số biện pháp này có thể được mở rộng cho người tiêu dùng trên khắp Hoa Kỳ. CCPA cung cấp một số quyền riêng tư cơ bản của người tiêu dùng bao gồm quyền được biết thông tin cá nhân nào đang được thu thập; quyền truy cập dữ liệu đó; quyền biết nó được bán cho ai; và quyền từ chối bán dữ liệu đó. Quan trọng nhất, CCPA cũng đảm bảo cho cư dân California quyền xóa dữ liệu mà các Công ty đã thu thập về họ. Giờ đây, thay vì các công ty như Google và Facebook có thể nói không với những người tiêu dùng yêu cầu xóa hoặc tính phí dữ liệu của họ, CCPA cung cấp cho các cá nhân quyền hợp pháp để yêu cầu các công ty xóa dữ liệu của họ hoặc đối mặt với hậu quả của chính sách bảo mật mới . hành động, Nếu bạn sống ở California, hãy nhớ tìm kiếm liên kết từ chối "Không bán thông tin cá nhân của tôi" mới mà CCPA hiện yêu cầu các công ty đăng trên trang Web của họ nếu họ có chính sách bán dữ liệu khách hàng.

#### Quy tắc bảo vệ dữ liệu chung của Liên minh châu Âu ÇGDPR)

Gần đây, Quy tắc bảo vệ dữ liệu chung (GDPR) của Liên minh châu Âu đã dẫn đầu một phong trào toàn cầu về phát triển luật bảo vệ dữ liệu và quyền riêng tư với các yêu cầu rất nghiêm ngặt. GDPR (https://gdpr-info.eu]) là Đạo luật về Quyền của người tiêu dùng trên toàn EU được ban hành vào tháng 5 năm 2016 trao quyền cho người tiêu dùng EU bằng cách buộc các nhà bán lẻ, nhà tiếp thị và những người khác nói rõ với người tiêu dùng cách họ thu thập, sử dụng và lưu trữ dữ liệu cá nhân của người tiêu dùng. Khi làm như vậy, nó đảm bảo các biện pháp bảo vệ dữ liệu được tích hợp vào các sản phẩm và dịch vụ từ giai đoạn phát triển sớm nhất, cung cấp "thiết kế bảo vệ dữ liệu" trong các sản phẩm và công nghệ mới. GDPR thống nhất luật bảo vệ dữ liệu trên tất cả 28 quốc gia thành viên của EU cộng với Ireland, Lichtenstein, Na Uy và Thụy Sĩ để cung cấp cho người dùng nhiều quyền hơn và kiểm soát thông tin có thể được ghép lại với nhau để nhận dạng một cá nhân, bao gồm dữ liệu vị trí và sinh trắc học, địa chỉ IP và bất kỳ thông tin nào khác được chia sẻ trực tuyến.

Bằng cách trao cho các cá nhân nhiều quyền kiểm soát hơn đối với thông tin cá nhân của họ và cơ hội tương tác an toàn với các trang web trực tuyến, luật mới sẽ kiềm chế những gã khổng lồ công nghệ và cung cấp một khuôn khổ an toàn nhưng nghiêm ngặt để tiến hành kinh doanh trực tuyến (Foggy 2019 ) . GDPR không chỉ áp dụng cho các doanh nghiệp hoạt động trong EU mà còn áp dụng cho các doanh nghiệp trên toàn thế giới nhắm mục tiêu dữ liệu người tiêu dùng EU và bảo vệ dữ liệu của tất cả công dân EU, bất kể họ hiện đang sống ở EU hay không.

Các công ty vi phạm GDPR phải đối mặt với mức phạt tối đa là 23 triệu đô la (20 triệu euro) hoặc 4% tổng doanh thu toàn cầu hàng năm của họ„ tùy theo mức nào lớn hơn, IT at Work 5.1 mô tả cách Google bị phạt 56,8 triệu đô la (50 triệu euro) vì không thông báo đầy đủ người dùng về cách dữ liệu của họ sẽ được sử dụng. Nhiều quốc gia bên ngoài EU đang lấy cảm hứng từ các nguyên tắc GDPR để thực hiện các quy định tương tự của riêng họ.

|  |
| --- |
| CNTT tại nơi làm việc 5.1    Google bị phạt 56,8 triệu USD vì vi phạm GDPR  Chỉ một tuần sau khi GDPR có hiệu lực, cơ quan quản lý quyền riêng tư của Pháp , Cơ quan Bảo vệ Dữ liệu Quốc gia  Ủy ban (CNIL) đã áp đặt khoản tiền phạt chưa từng có là 56,8 triệu đô la (50 triệu euro) đối với Google vì đã coi thường các nguyên tắc cơ bản của GDPR về tính minh bạch, thông tin và sự đồng ý. Tiền phạt là một trong những hồ sơ cao nhất    với các chính sách quyền riêng tư mới và không có cơ sở pháp lý để xử lý dữ liệu người dùng cho các tiện ích được cá nhân hóa. CNIL cho biết việc vi phạm thiếu minh bạch bắt nguồn từ việc người dùng Google không thể dễ dàng nói ra tất cả thông tin mà Google thu thập về họ khi đăng ký dịch vụ của họ  Phán quyết của Pháp tập trung vào mức độ dễ tìm và mức độ đầy đủ của thông tin về sự đồng ý của người tiêu dùng do Google cung cấp. Nó phát hiện ra rằng thông tin đầy đủ về mục đích xử lý dữ liệu và thời gian lưu trữ dữ liệu không được trình bày ở cùng một nơi, mà thay vào đó, cần tới năm hoặc sáu lần nhấp chuột. Nó cũng nói rằng một số hộp cho phép đã được kiểm tra trước vi phạm pháp luật.    Theo các quy tắc bảo mật cũ của châu Âu, mức phạt tối đa có thể áp dụng đối với một công ty vi phạm là 170.500 đô la (150.000 euro). Khi GDPR có hiệu lực vào ngày 25 tháng 5 năm 2018, các cơ quan quản lý quyền riêng tư quốc gia đã được trao quyền phạt các công ty tới 4% doanh thu hàng năm trên toàn cầu của họ đối với những vi phạm nghiêm trọng nhất. Lần đầu tiên sử dụng quyền hạn của mình để đưa ra mức phạt nặng, các nhà chức trách Pháp cho biết họ cảm thấy mức phạt "được biện minh bởi mức độ nghiêm trọng của các hành vi vi phạm được quan sát thấy liên quan đến các nguyên tắc cơ bản." Google đã nhiều lần bị kiểm tra theo các quy tắc cũ trước khi các quy tắc GDPR mới có hiệu lực nhưng chưa bao giờ bị phạt ở bất kỳ đâu cao như mức hiện tại.  Theo quy tắc GDPR, Google không thể kháng cáo khoản tiền phạt cho đến khi họ đã bàn giao 56,8 triệu đô la (50 triệu euro). Tuy nhiên, Google nên tự coi mình là người may mắn vì công ty đã kiếm được 33,74 tỷ đô la trong quý cuối cùng của năm 2018. Nếu họ bị phạt ở mức tối đa cho phép là 4% doanh thu toàn cầu hàng năm, thì số tiền phạt có thể lên tới hơn SI tỷ!  Nguồn: Tổng hợp từ Enright ( 2018 ), Bloomberg News 2019 , Bondini ( 2019 ), Grothaus ( 2012 ) và Schechner ( 2019 ). |

#### Lá chắn bảo mật EU-Hoa Kỳ

Theo các quy tắc GDPR, EU không cho phép chuyển dữ liệu về công dân của mình ra bên ngoài quốc gia trừ khi quốc gia đó được coi là có luật bảo mật dữ liệu đầy đủ. EU không coi luật về quyền riêng tư dữ liệu hiện có tại Hoa Kỳ là đầy đủ, theo như Hoa Kỳ: các doanh nghiệp phải giải quyết yêu cầu này bằng cách tuân thủ Lá chắn bảo mật của EC T -US. Một cơ chế tương tự cũng có sẵn giữa Switieriand và Hoa Kỳ. 

EC T -US và Swiss-US. PrivacyShields được thiết kế để cung cấp cho các công ty ở cả hai bờ Đại Tây Dương một cơ chế tuân thủ các yêu cầu bảo vệ dữ liệu GDPR khi chuyển dữ liệu cá nhân từ Liên minh Châu Âu (EU ) và Thụy Sĩ sang Hoa Kỳ để hỗ trợ thương mại xuyên Đại Tây Dương. Bằng cách trở thành thành viên tuân thủ của lá chắn bảo mật, các công ty Hoa Kỳ tham gia được coi là có bảo vệ dữ liệu đầy đủ để tạo điều kiện thuận lợi cho việc chuyển dữ liệu của EU (Fugairon, 2012 ). Tại một cuộc họp gần đây của Diễn đàn Kinh tế Thế giới

(https://www.weforum.org/), Giám đốc điều hành của Microsoft, Satya Nadella, đã lên tiếng ủng hộ GDPR và bày tỏ hy vọng rằng Hoa Kỳ sẽ thực hiện một cách tiếp cận nghiêm ngặt tương tự để bảo vệ quyền riêng tư đối với dữ liệu của người dùng (Đọc tối, 2019 ).

##### Công chúng thiếu hiểu biết

Khi các chính phủ trên toàn cầu tiếp tục nỗ lực bảo vệ việc xử lý và bảo mật dữ liệu của công dân bằng cách áp dụng các luật mạnh mẽ hơn, các tổ chức được yêu cầu xem xét lại cách họ thu thập, lưu trữ và xử lý thông tin cá nhân. Thật không may, những quy định và luật về quyền riêng tư dữ liệu này đã được đưa ra để bảo vệ người tiêu dùng nói chung không được công chúng hiểu rõ. Chẳng hạn, hai phần ba người dùng được khảo sát trong Báo cáo nghiên cứu Pew năm 2019 (Auxier et al., 2019 ) cho biết họ hiểu rất ít hoặc không hiểu gì về luật và quy định hiện hành để bảo vệ quyền riêng tư dữ liệu của họ: Hy vọng rằng thông tin được cung cấp trong báo cáo này phần đã nâng cao nhận thức và hiểu biết của bạn về chúng.



##### r tatinnn

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

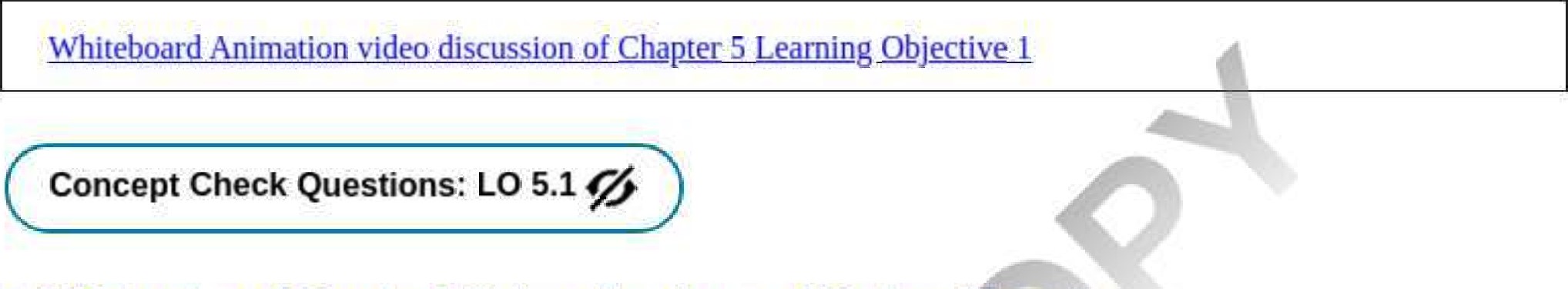
##### câu hỏi

1. Bốn mối quan tâm chính của quyền riêng tư dữ liệu là gì?
2. Tại sao điều quan trọng là bạn phải biết dữ liệu trực tuyến của mình được xử lý như thế nào?
3. Tên của hiện tượng mà người dùng lo ngại về quyền riêng tư của dữ liệu, nhưng hành vi của họ mâu thuẫn với những quan niệm này là gì?

4. Ai chịu trách nhiệm về luật bảo mật dữ liệu ở cấp liên bang Hoa Kỳ?

1. Kể tên ba quy định về quyền riêng tư dữ liệu bảo vệ người tiêu dùng của Hoa Kỳ.
2. Tên của luật bảo vệ dữ liệu mới của California là gì?
3. Công dân EU không sống ở EU có được bảo vệ theo GDPR không?
4. Tại sao Hoa Kỳ không được coi là một phần của GDPR?

9, Tên của cơ chế đặt Hoa Kỳ dưới quyền tài phán của GDPR là gì?

Câu hỏi kiểm tra khái niệm: LO 5.16/3

### 5.2 Mức độ và chi phí của các cuộc tấn công mạng và đe dọa mạng

1-05.2 Xác định mức độ và chi phí của các cuộc tấn công mạng và 12 loại đe dọa mạng có chủ ý và không chủ ý khác nhau.

Tội phạm mạng sử dụng Intemet và mạng riêng để chiếm đoạt số lượng lớn hồ sơ và hệ thống bao gồm PC, thiết bị di động, máy chủ và thiết bị Internet of Thing (IOT) để theo dõi người dùng, gửi thư rác cho họ, phá hoại hoạt động kinh doanh và đánh cắp danh tính . Điều quan trọng là phải bảo vệ chống lại các cuộc tấn công này vì khối lượng dữ liệu nhạy cảm chưa từng có mà chính phủ, quân đội, tập đoàn, tổ chức tài chính và tổ chức y tế đang thu thập, xử lý và lưu trữ trên máy tính và các thiết bị khác. Phần lớn dữ liệu này bao gồm thông tin nhận dạng cá nhân, dữ liệu tài chính sở hữu trí tuệ, hồ sơ y tế và các thông tin nhạy cảm khác và Q sẽ dẫn đến hậu quả tiêu cực cho chủ sở hữu nếu bị truy cập trái phép bởi những người không được ủy quyền.

Trong Báo cáo nghiên cứu Pew năm 2019 (Aukieret al., 2019 ) 70% trong số 4.272 người trưởng thành cảm thấy dữ liệu cá nhân của họ kém an toàn hơn so với 5 năm trước, chỉ 6% tin rằng dữ liệu của họ an toàn hơn so với trước đây . Trong nền kinh tế kỹ thuật số, dữ liệu tổ chức thường có sẵn theo yêu cầu 24/7 để cho phép các công ty hưởng lợi từ các cơ hội cải thiện năng suất và chia sẻ dữ liệu với khách hàng, nhà cung cấp và đối tác kinh doanh. Khái niệm dữ liệu theo yêu cầu này là một nhu cầu cần thiết trong hoạt động và cạnh tranh đối với các công ty toàn cầu, nhưng thật không may, nó cũng mở ra cơ hội cho các cuộc tấn công mạng sử dụng một số loại mối đe dọa mạng khác nhau để thực hiện chúng.



Tấn công mạng là một nỗ lực thực tế nhằm phơi bày, thay đổi, vô hiệu hóa, phá hủy, đánh cắp hoặc giành quyền truy cập trái phép vào hệ thống máy tính, cơ sở hạ tầng©, mạng hoặc bất kỳ thiết bị thông minh nào khác.

An ninh mạng là kỷ luật dành riêng để bảo vệ thông tin và hệ thống được sử dụng để xử lý và lưu trữ thông tin khỏi bị tấn công, phá hoại hoặc truy cập trái phép.

Các cuộc tấn công mạng thường bao gồm các vi phạm về quyền riêng tư dữ liệu giống như những vi phạm mà Yahoo đã trải qua trong trường hợp đầu tiên và không may là đang trở thành một sự cố phổ biến. Bảng 5.1 liệt kê năm vụ vi phạm dữ liệu lớn nhất được ghi nhận kể từ tháng 7 năm 2019.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | BẢNG 5.1 | | | | | | |  |
| Top 5 vụ vi phạm dữ liệu lớn nhất Nguồn: CNBC (2019). | | | | | | |
| xếp hạng công ty | | | | Năm Nguyên nhân | | |
| Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố. | | | | | | | | | |
|  | |  | Để lộ ra |  | |  |
| 1. | | Yahoo | 3 tỷ | 2013 | | hack |
|  | | Tập đoàn tài chính đầu tiên của Mỹ | 885 triệu 2019 | | | Bảo mật kém |
| 3. | | Facebook | 540 triệu 2019 | | | Bảo mật kém |
| 4. | | Yahoo | 500 triệu | 2014 | | hack |
| 5. | | Marriott | 500 triệu | hack 2018 | | |

Vấn đề rõ ràng xung quanh các vi phạm dữ liệu của Yahoo được thảo luận trong trường hợp mở đầu là thiếu các biện pháp an ninh mạng tinh vi . Các câu hỏi sử dụng, mật khẩu và bảo mật đơn giản không đủ để ngăn chặn tin tặc. Giáo sư Hemant Bhargava của UC Davis lưu ý rằng xác thực hai yếu tố (TFA) đã thành công ở nhiều công ty khác và Yahoo lẽ ra nên làm theo (Matwyshyn & Bhargava, 2016). Một ví dụ về TFA là khi người dùng được yêu cầu nhập thông tin như tên người dùng và mật khẩu, sau đó ứng dụng dành cho thiết bị di động sẽ tạo và gửi mã số ngẫu nhiên để người dùng nhập trước khi được cấp quyền truy cập vào tài khoản của họ. Cả tài khoản Yahoo và ứng dụng di động đều được liên kết với một tài khoản chung, an toàn. Phương pháp này đặc biệt phổ biến và hữu ích vì hơn 50% người dùng Web truy cập Web thông qua điện thoại di động của họ. Thật không may, nhiều công ty không thực hiện các biện pháp thích hợp để bảo mật thông tin nhận dạng cá nhân (PII). Việc không làm như vậy thường dẫn đến các cuộc tấn công mạng , chẳng hạn như các cuộc tấn công được mô tả trong các ví dụ sau:



Sau khi phát hiện một vụ hack mạng, công ty xử lý thẻ tín dụng Global Payments, Inc. đã dành 14 tháng để điều tra vụ rò rỉ dữ liệu làm lộ 1,5 triệu lượt quảng cáo trên thẻ ghi nợ và thẻ tín dụng của Hoa Kỳ. Toàn cầu thiệt hại tổng cộng 93 triệu đô la. Tổn thất này bao gồm 36 triệu đô la tiền phạt và tổn thất do gian lận và 77 triệu đô la cho việc điều tra, khắc phục, giám sát và bảo hiểm Trộm danh tính cho người tiêu dùng bị ảnh hưởng.

* Capitol One đã công bố một vụ vi phạm dữ liệu khiến 100 triệu người tiêu dùng Hoa Kỳ và 6 triệu người tiêu dùng Canada gặp rủi ro. Công ty thẻ tín dụng đã đưa ra một tuyên bố viện dẫn "sự truy cập trái phép của một cá nhân bên ngoài",
* Equifax, một trong ba cơ quan báo cáo tín dụng lớn nhất thế giới, thông báo họ đã bị vi phạm dữ liệu đối với hơn 148 triệu hồ sơ tín dụng cá nhân của người tiêu dùng.
* Ủy ban Thương mại Liên bang đã cảnh báo công chúng về một trò lừa đảo an sinh xã hội trong đó một người gọi tự xưng là từ Cơ quan An sinh Xã hội (SSA) thông báo cho bạn rằng đã có hoạt động đánh cắp danh tính đáng ngờ liên quan đến SSN của bạn. Sau đó, bạn được khuyến khích mua thẻ ghi nợ trả trước hoặc thẻ quỹ có thể nạp lại khác và chuyển tất cả tiền từ tài khoản ngân hàng của bạn vào thẻ đó để ngăn tin tặc lấy được tiền của bạn. Sau đó , người gọi gọi lại và yêu cầu số tài khoản và mã PIN của thẻ để ghi lại để lưu giữ an toàn trong hồ sơ SSA của bạn. Khi họ có thông tin đó, họ rút tiền ra khỏi thẻ và tất cả tiền tiết kiệm cả đời của bạn là của họ!
* Chỉ ba tuần sau khi kế hoạch vi phạm dữ liệu đáng chú ý (NDB) của Úc có hiệu lực, Văn phòng



Ủy viên Thông tin Úc (OAIC) đã nhận được 31 thông báo về vi phạm dữ liệu (Barbascgow, 2018).

Đe dọa mạng là phương pháp được sử dụng để thực hiện một cuộc tấn công mạng nhằm làm hỏng dữ liệu, đánh cắp dữ liệu nhạy cảm hoặc làm gián đoạn cuộc sống kỹ thuật số nói chung.

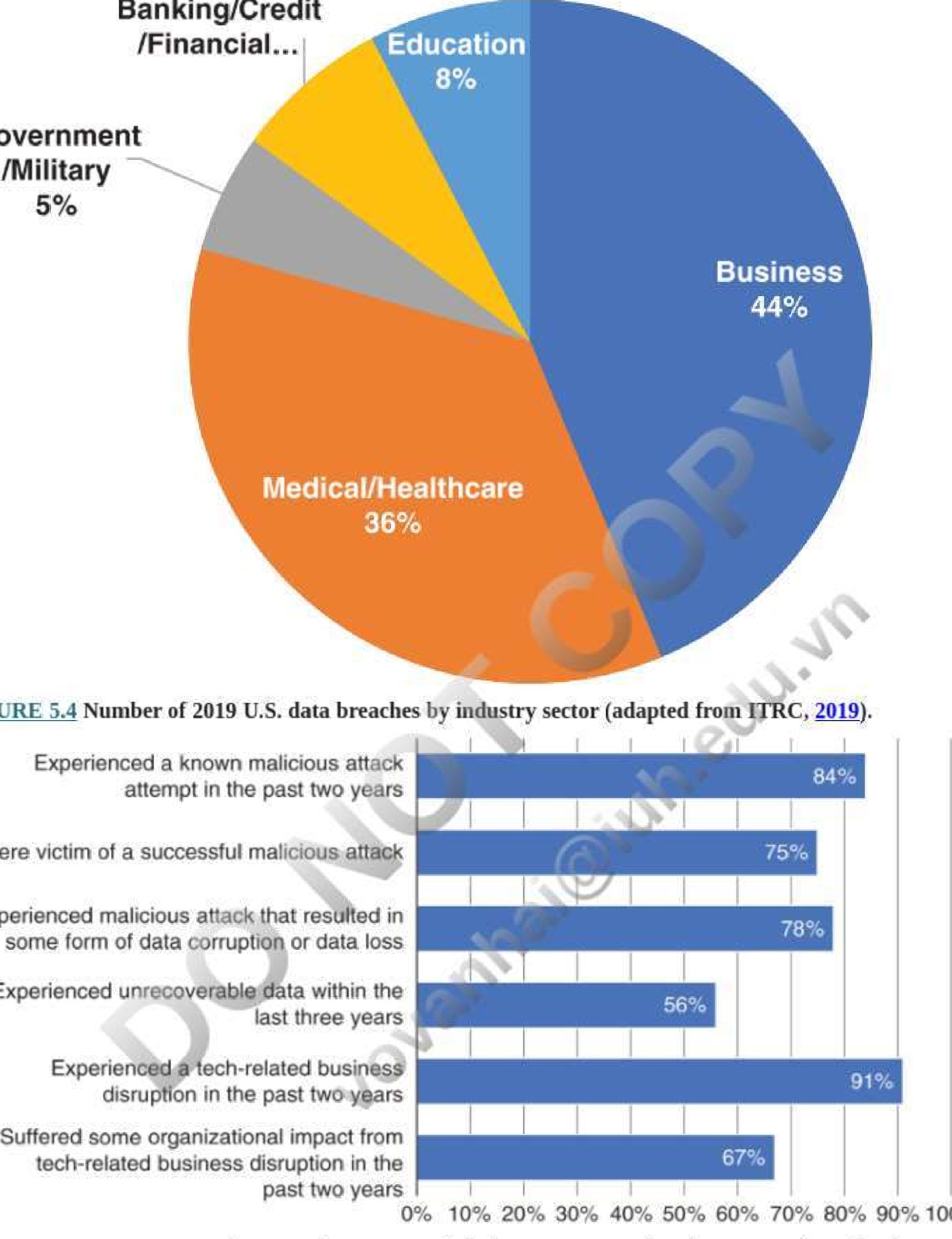
Các cuộc tấn công mạng như thế này tập trung chủ yếu vào những gì các công ty được yêu cầu báo cáo công khai, đó là hành vi trộm cắp thông tin nhận dạng cá nhân (PII), dữ liệu thanh toán và thông tin sức khỏe cá nhân (PHI). Do đó, chi phí thường liên quan đến một cuộc tấn công mạng chỉ tính đến những tác động dễ hiểu hơn này. Nhưng đây không phải lúc nào cũng là mục tiêu của kẻ tấn công. Hiếm khi người ta nhìn thấy đầy đủ hành vi trộm cắp tài sản trí tuệ (IP), hoạt động gián điệp, phá hủy dữ liệu, tấn công các hoạt động cốt lõi của 011 hoặc cố gắng vô hiệu hóa cơ sở hạ tầng quan trọng. Những cuộc tấn công này có thể có tác động đáng kể hơn nhiều đối với các tổ chức. Nhưng thiệt hại mà chúng gây ra không được hiểu rộng rãi và khó định lượng hơn nhiều.

Trong Báo cáo vi phạm dữ liệu hàng năm, Trung tâm tài nguyên nhận dạng hành vi trộm cắp (ITRC) đã báo cáo rằng các vụ vi phạm dữ liệu đã tăng 17% vào năm 2019. Tổng cộng có 1.473 vụ vi phạm đã được báo cáo và 164.683.455 hồ sơ nhạy cảm đã bị lộ (ITRC, 2020 ). Các lĩnh vực công nghiệp bị nhắm mục tiêu nhiều nhất bởi các cuộc tấn công mạng được thể hiện trong Biểu đồ 5.4 . Các loại và mức độ của trải nghiệm tấn công mạng mà các công ty phải chịu khác nhau, từ các nỗ lực thực hiện thành công các cuộc tấn công độc hại có tác động đến tổ chức như hỏng dữ liệu, dữ liệu không thể khôi phục và gián đoạn kinh doanh liên quan đến công nghệ có tác động đến tổ chức như được trình bày trong Ví dụ 5.5 (CIO , 2019 ) .

Tổng số sự cố = 1,473

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Chính phủ



Banking/Credit

FIGURE

Were

Experienced

Experienced

100%

[Quân đội

50/0

HÌNH 5.5 Tỷ lệ phần trăm các công ty trong tất cả các lĩnh vực công nghiệp đã từng bị tấn công mạng (điều chỉnh từ CIO, 2019) .

Những vi phạm dữ liệu này có thể làm lộ mọi thứ từ tên người dùng đến mật khẩu đến số An sinh xã hội và gây ra bởi việc khai thác thành công các lỗ hổng trong hệ thống thông tin bởi một mối đe dọa mạng (rủi ro = lỗ hổng đe dọa mạng).

Vi phạm dữ liệu là thành công tôi truy xuất thông tin nhạy cảm bởi một cá nhân, nhóm hoặc phần mềm trái phép

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.



hệ thống

Lỗ hổng bảo mật là lỗ hổng trong hệ thống phòng thủ bảo mật CNTT của mạng, hệ thống hoặc ứng dụng có thể bị mối đe dọa mạng khai thác để giành quyền truy cập trái phép.

Các lỗ hổng tồn tại trong mạng, ứng dụng hệ điều hành, cơ sở dữ liệu, thiết bị di động và môi trường đám mây. Các lỗ hổng này được coi là vectơ tấn công hoặc điểm vào cho 'phần mềm độc hại, tin tặc, kẻ tấn công và tội phạm có tổ chức. Các thiết bị và ứng dụng di động, phương tiện truyền thông xã hội và dịch vụ đám mây thậm chí còn giới thiệu nhiều vectơ tấn công hơn cho phần mềm độc hại, lừa đảo và tin tặc. Do đó, các cách thức mới để thực hiện các cuộc tấn công mạng đang xuất hiện.

vectơ tấn công là một đường dẫn hoặc phương tiện mà tội phạm máy tính có thể truy cập vào máy tính hoặc máy chủ mạng để thực hiện một kết quả độc hại.

Ví dụ về các lỗ hổng bao gồm thiếu kiểm soát xung quanh con người (đào tạo người dùng, chính sách không phù hợp), quy trình (phân chia nhiệm vụ không phù hợp, kiểm soát quy trình kém) hoặc công cụ (thiếu thực thi hoặc giám sát kiểm soát kỹ thuật). Các lỗ hổng đe dọa tính bảo mật, tính toàn vẹn hoặc tính khả dụng (CIA) của dữ liệu và hệ thống thông tin, đồng thời khiến các tổ chức dễ bị tấn công bởi một số loại mối đe dọa mạng không chủ ý và cố ý.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

#### Các mối đe dọa mạng không chủ ý

Không phải tất cả các mối đe dọa mạng là cố ý. Các vi phạm an ninh có nguồn gốc từ nội bộ • không cố ý có thể là kết quả của sự sơ suất đơn giản, thiếu chú ý hoặc thiếu kiến thức của quản trị viên, nhân viên, người vận hành máy tính và lập trình viên máy tính. Chúng cũng có thể liên quan đến công nghệ, chẳng hạn như lỗi phần mềm ngoài ý muốn hoặc lỗi cấu hình hệ thống. Nguyên nhân của những mối đe dọa mạng không chủ ý này thuộc ba loại chính: lỗi của con người, các mối nguy môi trường và lỗi hệ thống máy tính.

* Lỗi của con người có thể xảy ra trong quá trình thiết kế phần cứng hoặc hệ thống thông tin. Nó cũng có thể xảy ra trong quá trình lập trình, thử nghiệm hoặc nhập dữ liệu. Việc bỏ qua việc thay đổi mật khẩu mặc định trong các ứng dụng hoặc trên hệ thống hoặc không quản lý các bản vá sẽ tạo ra các lỗ hổng bảo mật. Lỗi của con người cũng bao gồm những người dùng không được đào tạo hoặc không biết trở thành nạn nhân của các công cụ xã hội như lừa đảo trực tuyến hoặc bỏ qua các thủ tục bảo mật. Lỗi của con người góp phần vào hầu hết các vấn đề về kiểm soát nội bộ (IC) và bảo mật thông tin.
* Các nguy cơ môi trường bao gồm núi lửa, động đất, bão tuyết, lũ lụt, mất điện hoặc biến động mạnh, hỏa hoạn (nguy cơ phổ biến nhất), hệ thống sưởi, thông gió và điều hòa không khí (HVAC) bị lỗi, các vụ nổ, bụi phóng xạ và sự cố hệ thống làm mát bằng nước . Ngoài thiệt hại chính, tài nguyên máy tính có thể bị hư hỏng do tác dụng phụ của mối nguy hiểm, chẳng hạn như khói và nước. Những mối nguy hiểm như vậy có thể làm gián đoạn hoạt động bình thường của máy tính, dẫn đến không thể truy cập dữ liệu trong thời gian dài và chi phí phục hồi và khôi phục quá cao.
* Lỗi hệ thống máy tính có thể xảy ra do sản xuất kém, vật liệu bị lỗi hoặc bảo trì kém. Trục trặc ngoài ý muốn cũng có thể xảy ra vì những lý do khác, từ quản trị viên thiếu kinh nghiệm đến kiểm tra không đầy đủ.

#### Các mối đe dọa mạng có chủ ý

Mặt khác, các vi phạm bảo mật có chủ ý hữu ích là các hành động trực tiếp và công khai được thiết kế để phá vỡ hệ thống và bao gồm hành vi trộm cắp dữ liệu, chẳng hạn như sử dụng dữ liệu không phù hợp (ví dụ: thao tác đầu vào); đánh cắp thời gian máy tính; trộm cắp thiết bị và/hoặc phần mềm; thao tác có chủ ý trong việc xử lý, nhập, lập trình, xử lý hoặc truyền dữ liệu; sự phá hoại; thiệt hại độc hại cho tài nguyên máy tính; phá hủy phần mềm độc hại và các cuộc tấn công tương tự; và lạm dụng máy tính linh tinh và gian lận Internet . Mười hai mối đe dọa mạng phổ biến sẽ được mô tả tiếp theo.

##### hack

Một dấu hiệu phổ biến được sử dụng khi một cuộc tấn công mạng xảy ra là hệ thống đã bị "tấn công". Hackin g là một ngành rất có lợi nhuận, là một phần lớn của tội phạm mạng trong thế giới ngầm và là cách để những người theo chủ nghĩa hack phản đối. Cả tính ẩn danh của Internet và việc thiếu tính quốc tế đều mang lại cho tin tặc cảm giác gần như bất khả chiến bại vì chúng phải đối mặt với nguy cơ bị bắt và trừng phạt rất thấp.

Hacktivist là viết tắt của hackeractivist hoặc ai đó thực hiện hack để nâng cao nhận thức hoặc hỗ trợ xã hội, chính trị, kinh tế hoặc nguyên nhân khác. Việc hack một ứng dụng, hệ thống hoặc mạng mà không được phép, bất kể động cơ là một tội ác

Hacking được định nghĩa rộng rãi là cố ý truy cập máy tính mà không được phép hoặc vượt quá quyền truy cập được phép. Nhiều luật tiểu bang và liên bang chi phối việc hack máy tính.

Trong văn hóa Hacker có ba loại Hacker, được trình bày trong Bảng 5.2 .

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | BẢNG 5.2 | | | | | |  |
| Ba loại tin tặc | | | | | |
| Loại Đặc điểm Kết quả | | | | | |
| mũ trắng | | Chuyên gia bảo mật máy tính đột nhập vào các hệ thống và mạng được bảo vệ để kiểm tra và đánh giá tính bảo mật của chúng. | | Sử dụng các kỹ năng của họ để cải thiện bảo mật bằng cách phơi bày các lỗ hổng trước khi tin tặc độc hại (mũ đen) có thể phát hiện và khai thác chúng. | |
| Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố. | | | | | | | | |
|  | | | |  | |
| Mũ đen | | Người cố gắng tìm lỗ hổng bảo mật máy tính và khai thác chúng vì lợi ích tài chính cá nhân hoặc các lý do độc hại khác. | | Có thể gây ra thiệt hại lớn cho cả người dùng máy tính cá nhân và các tổ chức lớn bằng cách đánh cắp thông tin tài chính cá nhân, làm tổn hại đến tính bảo mật của các hệ thống chính hoặc tắt hoặc cảnh báo chức năng của các trang web và mạng. | |
| mũ xám | | Người có thể vi phạm các tiêu chuẩn hoặc nguyên tắc đạo đức, nhưng không có ý đồ xấu như hacker mũ đen. | | Có thể tham gia vào các hoạt động kém đạo đức, nhưng thường hoạt động vì lợi ích chung, ví dụ: khai thác chứng khoán lỗ hổng để phổ biến nhận thức cộng đồng rằng lỗ hổng tồn tại. | |

Mũ trắng Chuyên gia bảo mật máy tính đột nhập vào các hệ thống và mạng được bảo vệ để kiểm tra và đánh giá tính bảo mật của chúng,

Mũ xám Người có thể vi phạm các tiêu chuẩn hoặc nguyên tắc đạo đức, nhưng không có ý đồ xấu như hacker mũ đen.

##### Cái nhìn sâu sắc về cách thức hoạt động của ngành công nghiệp hack

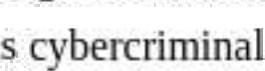
Hacking là một ngành có cách thức hoạt động, lực lượng lao động và các dịch vụ hỗ trợ riêng, Hacker theo hợp đồng có sẵn để thuê hoặc có thể mua toàn bộ các cuộc tấn công hack, Bộ phận trợ giúp hack cung cấp hỗ trợ 24/7—làm cho các cuộc tấn công phức tạp trở nên dễ quản lý và thực hiện hơn. Tin tặc sử dụng các mạng xã hội, diễn đàn ngầm và Deep Web để xếp hạng và quảng bá dịch vụ, chia sẻ các khai thác và tuyển dụng những người khác. Trong một số diễn đàn nhất định và trong Deep Web, tin tặc có thể mua quyền sử dụng bất kỳ số lượng dịch vụ nào, chẳng hạn như:

* Dịch vụ giáo dục
* Nền tảng phần mềm để xây dựng và phân phối các công cụ hack và phần mềm độc hại/ransomware
* Mua hoặc bán dữ liệu bị đánh cắp từ các mục đơn giản như tài khoản e-mail đến thẻ tín dụng, thuế TNCN và dữ liệu công ty.

Con người dễ dàng bị tấn công, khiến họ và phương tiện truyền thông xã hội của họ đăng các phương tiện tấn công có nguy cơ cao. Chẳng hạn, thường rất dễ khiến người dùng lây nhiễm mạng công ty hoặc thiết bị di động của họ bằng cách lừa họ.!pto tải xuống và cài đặt cửa hậu

##### Kỹ thuật xã hội

Expense tin rằng một trong những nguy cơ an ninh mạng lớn nhất trong vài năm tới sẽ liên quan đến việc tin tặc sử dụng thông minh để đánh lừa hoặc thao túng xu hướng tin tưởng, giúp đỡ của mọi ngườiHoặc đơn giản là theo dõi sự tò mò của họ trên mạng xã hội. Hiện tượng này được gọi là kỹ thuật xã hội và ngay cả những hệ thống bảo mật CNTT mạnh nhất cũng khó có thể chống lại những gì có thể được tạo ra để có vẻ như được ủy quyền.

khét tiếng  đã sử dụng kỹ thuật xã hội làm phương pháp chính để truy cập vào mạng máy tính và thảo luận về một loạt các cuộc tấn công kỹ thuật xã hội trong cuốn sách của mình, "Nghệ thuật lừa dối". Trong hầu hết các vụ khai thác kỹ thuật xã hội, tội phạm không bao giờ gặp trực tiếp nạn nhân mà giao tiếp qua điện thoại hoặc e- mail. Phishin g là công cụ lâu đời nhất trong kho vũ khí của tin tặc và vẫn là kỹ thuật tấn công xã hội hiệu quả nhất. Trong một cuộc tấn công lừa đảo, kẻ tấn công gửi e-mail để lấy lòng tin của nạn nhân bằng cách gợi lên cảm giác tò mò, khẩn cấp hoặc sợ hãi, nhằm đánh cắp thông tin bí mật. Điều này được thực hiện bởi kẻ tấn công giả làm một người hoặc tổ chức hợp pháp đã biết, chẳng hạn như PayPal, ngân hàng, công ty thẻ tín dụng hoặc nguồn đáng tin cậy khác và yêu cầu người dùng thực hiện một hành động khiến máy tính của họ bị đe dọa hoặc tiết lộ thông tin xác thực, thông tin cá nhân, tài chính hoặc liên quan đến kinh doanh „ Tin nhắn lừa đảo được gửi trong các chiến dịch hàng loạt hoặc chúng được nhắm mục tiêu cụ thể vào một nhóm người cụ thể hoặc một cá nhân. Cái trước không yêu cầu công việc trước để đạt được ngữ cảnh cho mục tiêu mà dựa vào khối lượng tin nhắn tuyệt đối (hàng triệu đến hàng chục triệu) để đạt được lợi nhuận. 

Loại thứ hai đòi hỏi nhiều nỗ lực hơn để thu thập ngữ cảnh có liên quan về mục tiêu thư và do đó được gửi theo lô nhỏ hơn nhiều nhưng có tỷ lệ hoàn vốn cao hơn trên cả số lượng thư đã mở và khoản hoàn vốn trên mỗi thư cho nỗ lực đó. Cách tiếp cận thứ hai được thảo luận sau trong phần này.

Tin nhắn lừa đảo bao gồm yêu cầu phản hồi với một số loại thông tin hoặc liên kết đến một trang web lừa đảo thường trông giống như một trang xác thực mà người dùng làm việc cùng. Khi người dùng nhấp vào liên kết đến trang web, họ sẽ trở thành nạn nhân của phần mềm độc hại tải xuống , tấn công bằng lái xe hoặc đọc lướt thông tin chẳng hạn như bị yêu cầu cung cấp số thẻ tín dụng, số An sinh xã hội, số tài khoản hoặc mật khẩu.

Spear p hishin g là một kiểu lừa đảo nhắm mục tiêu vào một số nhóm người có điểm chung . Họ có thể

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

làm việc tại cùng một ngân hàng công ty tại cùng một tổ chức tài chính, sử dụng một nhà cung cấp Internet cụ thể hoặc tham dự cùng một nhà thờ hoặc trường đại học. Các e-mail lừa đảo dường như được gửi từ các tổ chức hoặc những người mà các nạn nhân tiềm năng thường nhận được e-mail từ đó, khiến chúng trở nên lừa đảo hơn.

Đây là cách hoạt động của lừa đảo giáo:

1. Spear phishe1S thu thập thông tin về hoạt động của mọi người, các nhóm xã hội, công ty và/hoặc công việc từ các thông báo trên phương tiện truyền thông chung, mạng xã hội hoặc tài khoản bị xâm nhập, ứng dụng được thiết kế kém và làm rò rỉ thông tin hoặc họ có thể đánh cắp thông tin đó từ các trang web, máy tính hoặc thiết bị di động mà họ đã xâm phạm, sau đó sử dụng thông tin đó để tùy chỉnh tin nhắn.

2, Sau đó, họ gửi email tùy chỉnh cho các nạn nhân được nhắm mục tiêu, tạo ra một số loại lý do yêu cầu người dùng hành động hoặc phản hồi. Đây có thể là các mối đe dọa đóng tài khoản, mất quyền truy cập hoặc đặc quyền, mất tiền hoặc các khoản phí bổ sung, hành động pháp lý ảnh hưởng đến bạn bè hoặc các thành viên gia đình, v.v., Với thông tin cơ bản thu được, thông báo sẽ tạo ra một lời giải thích rất hợp lý và thuyết phục về lý do tại sao họ cần dữ liệu cá nhân của bạn,

3. Cuối cùng, 'các nạn nhân được yêu cầu nhấp vào một liên kết bên trong e-mail đưa họ đến một trang web giả mạo nhưng trông giống như thật, nơi họ được yêu cầu cung cấp mật khẩu, số tài khoản, ID người dùng, mã truy cập, mã PIN và sớm. Khi các mục tiêu lừa đảo trực tuyến là giám đốc điều hành hoặc những người giàu có, quyền lực, ảnh hưởng hoặc kiểm soát, hoạt động này được gọi là "đánh bắt cá voi".

Phần mềm độc hại đề cập đến các cấp độ khác nhau của phần mềm độc hại hoặc xâm nhập có thể chạy ngầm mà không bị phát hiện trên IS hoặc máy tính cá nhân. Ít xâm nhập hơn có nhiều giá trị phiền toái hơn mục đích xấu. Phần mềm độc hại thù địch hơn được thiết kế đặc biệt để làm gián đoạn hoạt động của máy tính hoặc thiết bị di động, thu thập thông tin nhạy cảm và giành quyền truy cập vào hệ thống máy tính cá nhân.

Phần mềm thù địch ngày nay thường được thiết kế để kiểm soát lâu dài các máy bị nhiễm. Phần mềm độc hại có thể tự đính kèm vào các chương trình phần mềm khác và tự sao chép trên các hệ thống hoặc ẩn trong các ứng dụng hữu ích. Advanced npalware thiết lập các kênh giao tiếp bên ngoài để tải dữ liệu bị đánh cắp lên, tải trọng xuống hoặc do thám. Tải trọng của phần mềm độc hại là mã được thả vào hệ thống để thực hiện bất kỳ hoặc tất cả các chức năng sau: tạo điều kiện lây nhiễm hoặc giao tiếp với máy chủ chỉ huy và kiểm soát hoặc tải xuống nhiều mã hơn. Khi làm như vậy, tải trọng thực hiện mục đích của phần mềm độc hại. Tải trọng có thể gây ra thiệt hại có thể nhìn thấy hoặc hoạt động ở chế độ tàng hình để không bị phát hiện. 

Các loại phần mềm xâm nhập, nhưng không nhất thiết là phần mềm độc hại bao gồm:

* Cookie —một mẩu dữ liệu nhỏ được gửi từ một trang web và được lưu trữ trong trình duyệt Web của người dùng trong khi người dùng đang duyệt một trang web. Mỗi cookie có thể được lưu trữ dưới dạng tệp nhỏ riêng lẻ oólfcookie từ một nguồn, chẳng hạn như những cookie được Firefoxy sử dụng được lưu trữ trong một tệp duy nhất. Mục đích của cookie là cung cấp dịch vụ được cá nhân hóa như lưu trữ mật khẩu và ID người dùng để sử dụng nhiều lần. Mặc dù cookie độc hại về mặt kỹ thuật, nhưng chính những gì trang web làm với chúng mới quyết định liệu chúng có vô hại hay không. • Có lo ngại rằng cookie có thể gây rủi ro về quyền riêng tư nếu chúng được sử dụng để theo dõi người dùng và các tài nguyên máy tính có giá trị có thể làm chậm hiệu quả của máy tính,

Spamware—phần mềm cho phép kẻ tấn công niêm phong, sắp xếp và biên dịch danh sách địa chỉ email, tạo địa chỉ ngẫu nhiên, chèn tiêu đề giả vào thư và sử dụng đồng thời nhiều máy chủ thư để phát các thư không mong muốn đến những người nhận không nghi ngờ.

mềm quảng cáo —phần mềm nhúng quảng cáo trong ứng dụng. Nó được coi là một giải pháp thay thế hợp pháp được cung cấp cho những người tiêu dùng không muốn trả tiền cho phần mềm,

* dụ : phần mềm theo dõi không được thiết kế để cố ý làm hỏng hoặc vô hiệu hóa hệ thống. Ví dụ: chủ lao động có thể cài đặt phần mềm gián điệp trên máy tính xách tay của công ty để theo dõi các hoạt động duyệt web của nhân viên hoặc nhà quảng cáo có thể sử dụng cookie để theo dõi những trang Web mà người dùng truy cập theo thứ tự để nhắm mục tiêu quảng cáo trong một chiến dịch tiếp thị.

Các loại phần mềm độc hại thù địch bao gồm:

* Zero-Day—loại phần mềm độc hại nguy hiểm nhất và là mối đe dọa mạng phát triển nhanh nhất. Theo Báo cáo bảo mật Internet quý 3 năm 2019 do WatchGuard đưa ra, công ty hàng đầu thế giới về bảo mật mạng và phần mềm độc hại zero-day chiếm gần 50% tổng số cuộc tấn công bằng phần mềm độc hại (Warfield, 2019 ). Khai thác zero-day nhắm vào các lỗ hổng hệ thống mà kẻ tấn công tìm thấy, nhưng tổ chức đó vẫn chưa phát hiện ra. Trong khai thác zero-day, các tổ chức không có thời gian để phản ứng làm tăng khả năng thành công của nó. Phần mềm độc hại nguy hiểm lợi dụng lỗ hổng để gây ra thiệt hại lớn cho mạng, ứng dụng, máy tính cá nhân hoặc cho phép vi phạm dữ liệu. Nhiều cuộc tấn công trong số này xảy ra thông qua e-mail hoặc Internet trong các e-mail hoặc tệp đính kèm đáng ngờ. Trong hầu hết các trường hợp, một khi lỗ hổng bị phát hiện bởi khai thác zero-day, một bản vá có thể khắc phục sự cố, nhưng thiệt hại

qi7P

|  |
| --- |
| dnnA A zprn-rlav pynlnitsan rpqllltin tn nroani7atinnq nf,qlJ tvnpq và  Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố. |

hoan thanh. Việc khai thác zero-day có thể dẫn đến hậu quả nghiêm trọng đối với các tổ chức ở mọi loại hình và quy mô.

* Cửa sau —cũng là một chương trình máy tính độc hại khó phát hiện được sử dụng để cung cấp cho kẻ tấn công quyền truy cập từ xa trái phép vào PC bị xâm nhập bằng cách khai thác các lỗ hổng bảo mật và hoạt động trong nền ẩn đối với người dùng:
* Rootkit —một bộ công cụ phần mềm cho phép kẻ tấn công giành quyền kiểm soát hệ thống máy tính mà không bị phát hiện.
* Boot Record Infector—tự gắn vào bản ghi khởi động chính trên đĩa cứng nơi nó được tải vào bộ nhớ khi hệ thống khởi động và có thể tự sao chép sang các ổ đĩa hoặc máy tính khác.
* File Infector—tự gắn vào mã thực thi (tệp .exe) và được cài đặt sau khi mã được mở.
* Keylogger—một phần mềm hoặc phần cứng ghi lại mọi phím được nhấn trên bàn phím máy tính. Nó có thể ghi lại các tin nhắn cá nhân, mật khẩu, số thẻ tín dụng và bất kỳ thứ gì được nhập.
* Vi -rút —lây nhiễm các ứng dụng như Microsoft Word trong đó vi-rút thực thi các hướng dẫn sau khi được mở trước khi chuyển quyền kiểm soát trở lại ứng dụng.
* Sâu —không tự gắn vào máy chủ, giống như vi-rút, nhưng các chương trình độc lập này có thể tự nhân bản trên các máy tính và mạng.
* Trojan—ẩn mình trong một chương trình hữu ích để lây nhiễm vào hệ thống của nạn nhân. Trojan không tự sao chép nhưng có thể được sử dụng để thiết lập các cửa hậu mà kẻ tấn công khám phá.
* mềm truy cập từ xa ( RATS ) —một dạng ngựa thành Troia tạo ra một cửa hậu không được bảo vệ vào một hệ thống mà qua đó tin tặc có thể điều khiển hệ thống đó từ xa. Đúng như tên gọi, một cửa hậu cung cấp quyền truy cập dễ dàng vào hệ thống, máy tính hoặc tài khoản bằng cách tạo quyền truy cập có thể yêu cầu hoặc không yêu cầu xác thực. Sâu Storm , lây lan qua s pam, là một trojan cửa hậu nhúng bên trong hơn 25 triệu máy tính. Sức mạnh tổng hợp của Storm được so sánh với sức mạnh xử lý của một siêu máy tính + Các cuộc tấn công do Stom tổ chức có thể làm tê liệt bất kỳ trang web nào,

Hầu hết các loại vi-rút, sâu máy tính và trojan đều được kích hoạt khi tệp đính kèm được mở hoặc liên kết orüi được nhấp vào. Nhưng khi các tính năng được tự động hóa, chúng có thể tự động kích hoạt phần mềm độc hại. Ví dụ:

* Nếu một ứng dụng e-mail, chẳng hạn như Microsoft Outlook hoặc Gmail, được đặt thành cho phép • sao chép, thì việc lây nhiễm vi-rút sẽ xảy ra khi chỉ cần mở một thư hoặc tệp đính kèm. —
* Xem thư điện tử ở định dạng HTML, thay vì ở dạng văn bản thuần túy, có thể gây nhiễm vi-rút.

##### Các cuộc tấn công bằng phần mềm độc hại là một phần của hoạt động hàng ngày

Các nhà nghiên cứu bảo mật CNTT phát hiện ra gần một triệu chương trình độc hại mỗi ngày và các cuộc tấn công bằng phần mềm độc hại đang trở nên phổ biến hơn. Trong một báo cáo gần đây, WatchGuard đã báo cáo rằng các cuộc tấn công bằng phần mềm độc hại đã tăng 30% từ quý 2 đến ngày 23 tháng 2 năm 2019 (Warfield, 2019 ).



Những người tạo phần mềm độc hại thường sử dụng kỹ thuật xã hội để tối đa hóa việc phân phối hiệu quả các sáng tạo của họ. Ví dụ: ILoveYou worrnž đã sử dụng Kỹ thuật xã hội để lôi kéo mọi người mở các e-mail bị nhiễm phần mềm độc hại. Nó đã tấn công thành công hàng chục triệu máy tính chạy Windows khi nó được gửi dưới dạng tệp đính kèm e-mail với dòng chủ đề: ILOVEYOU. Trong vòng 9 ngày, con sâu này đã lan rộng khắp thế giới, làm tê liệt các mạng, phá hủy các tệp và gây thiệt hại ước tính 5,5 tỷ USD.

###### botnet

Khi bạn xâu chuỗi một số máy tính bị nhiễm phần mềm độc hại lại với nhau, bạn sẽ có một botnet „ Thuật ngữ botnet bắt nguồn từ các từ robot và mạng. Tội phạm mạng sử dụng vi-rút trojan để vi phạm bảo mật của một số máy tính người dùng, chiếm quyền kiểm soát từng máy tính và tổ chức tất cả các máy bị nhiễm thành một mạng "bot" mà chúng có thể điều khiển từ xa cho các mục đích xấu. Botnet thường được sử dụng để gửi thư rác và e-mail lừa đảo và khởi chạy các cuộc tấn công DDoS. Botnet cực kỳ nguy hiểm vì chúng quét và xâm nhập các máy tính khác, sau đó có thể được sử dụng cho mọi loại tội phạm và tấn công máy tính, serve1S và mạng.

Ransomware được thiết kế để chặn quyền truy cập vào hệ thống máy tính cho đến khi một khoản tiền được thanh toán. Việc sử dụng ransomware bắt đầu ở quy mô khá nhỏ, nhắm mục tiêu đến người dùng cá nhân, nhưng mối đe dọa trên mạng của ransomware đang gia tăng và



các cuộc tấn công đã trở thành quy mô lớn. Giờ đây, một số giám đốc điều hành lo sợ toàn bộ công ty sẽ bị đóng cửa bởi ransomware cho đến khi họ thanh toán hoặc có nguy cơ mất tất cả dữ liệu.

Ransomware hoạt động bằng cách trước tiên xâm nhập vào máy tính bằng phần mềm độc hại, sau đó mã hóa tất cả các tệp trên đĩa. Phần mềm độc hại được sử dụng để mã hóa tệp có thể khó chống lại. và encrvotion trong hầu hết các trường hợp không thể bị phá vỡ

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

phần mềm độc hại sử dụng để mã hóa các đường có thể De auncult to aerena chống lại, và mã hóa 111 hầu hết các trường hợp không thể oe oroKen. Sau đó, người dùng được cung cấp một ưu đãi trong thời gian giới hạn: Mất tất cả dữ liệu của bạn hoặc gửi tiền với lời hứa rằng dữ liệu sẽ được mở khóa. Lệ phí thường thay đổi từ vài đô la đến đô la và thường phải được chuyển bằng Bitcoin. Một bệnh viện ở Los Angeles, có hệ thống hồ sơ y tế điện tử đã bị khóa trong 10 ngày, buộc phải trả cho những kẻ tấn công mạng 40 Bitcoin để mở khóa hệ thống khi cơ quan thực thi pháp luật và các chuyên gia máy tính không thể giúp khôi phục các tệp dữ liệu của bệnh viện.

Các chuyên gia bảo mật máy tính đã đưa ra giả thuyết rằng kiểu tấn công này có tỷ lệ thành công cao hơn so với hoạt động tội phạm mạng khác vốn đã trở nên khó khăn hơn: Biện pháp bảo hiểm tốt nhất chống lại mã độc tống tiền là có các bản sao lưu dữ liệu ngoại tuyến hoặc tách biệt.

Cryptoj ackin g là một cách mà tội phạm mạng có thể kiếm tiền với nỗ lực tối thiểu. Đây là một kế hoạch giống như phần mềm tống tiền nhằm sử dụng thiết bị của người khác mà không có sự đồng ý hoặc không biết của họ để bí mật bòn rút tiền điện tử với chi phí của nạn nhân. Bằng cách khiến nạn nhân nhấp vào một liên kết độc hại trong e-mail tải một vài dòng mã trên máy tính của họ hoặc bằng cách lây nhiễm một trang web hoặc quảng cáo trực tuyến bằng mã JavaScript tự động thực thi sau khi được tải trong trình duyệt của nạn nhân, kẻ tấn công cryptojacker máy tính của nạn nhân và lấy đi các mã thông báo tiền điện tử. Sau đó, nạn nhân phải chịu chi phí tính toán và điện đã sử dụng để lấy mã thông báo.

SQ L In j ection là một trong những lỗ hổng nguy hiểm nhất của ứng dụng mạng vì kẻ tấn công có thể sử dụng SQL injection để vượt qua các biện pháp bảo mật của ứng dụng. Mục đích là thực thi mã SQL bên trong một ứng dụng hoặc trang Web vì lợi ích cá nhân hoặc đơn giản là phá hoại. Bằng cách chèn mã độc hại vào câu lệnh SQL, kẻ tấn công có thể thao túng truy vấn SQL và buộc truy vấn trả về dữ liệu khác với dự định của người dùng được ủy quyền. Ví dụ: khi một trang web yêu cầu người dùng đăng nhập bằng tên người dùng và mật khẩu trên biểu mẫu Web, kẻ tấn công sẽ chặn yêu cầu và chèn một câu lệnh SQL chạy trên cơ sở dữ liệu mà không bị phát hiện làm thay đổi bất kỳ kết quả quelY nào sau đó.

trung gian ( MitM ) đang gia tăng. Chúng xảy ra khi bọn tội phạm mạng xen vào giữa hai bên trong một giao dịch với ý định đánh cắp dữ liệu. Một điểm truy cập MitM phổ biến là Wi-Fi công cộng không bảo mật„ Sau khi phần mềm độc hại đã xâm phạm hệ thống, kẻ tấn công có thể cài đặt phần mềm để xử lý thông tin của nạn nhân. Hình 5.6 cho thấy ba kiểu tấn công MitM phổ biến:



|  |  |
| --- | --- |
|  | Cướp phiên |
| • Kẻ tấn công chiếm quyền điều khiển phiên làm việc giữa nạn nhân và máy chủ mạng đáng tin cậy. | |



|  |  |
| --- | --- |
|  | Giả mạo IP |
| • Kẻ tấn công thuyết phục hệ thống máy tính của nạn nhân rằng nó đang liên lạc với một thực thể đã biết, đáng tin cậy để cung cấp cho kẻ tấn công quyền truy cập hệ thống. | |



FIGURE

One

example

of

a

MitM

attack

is

active

eavesdropping

where

the

attacker

makes

an

independent

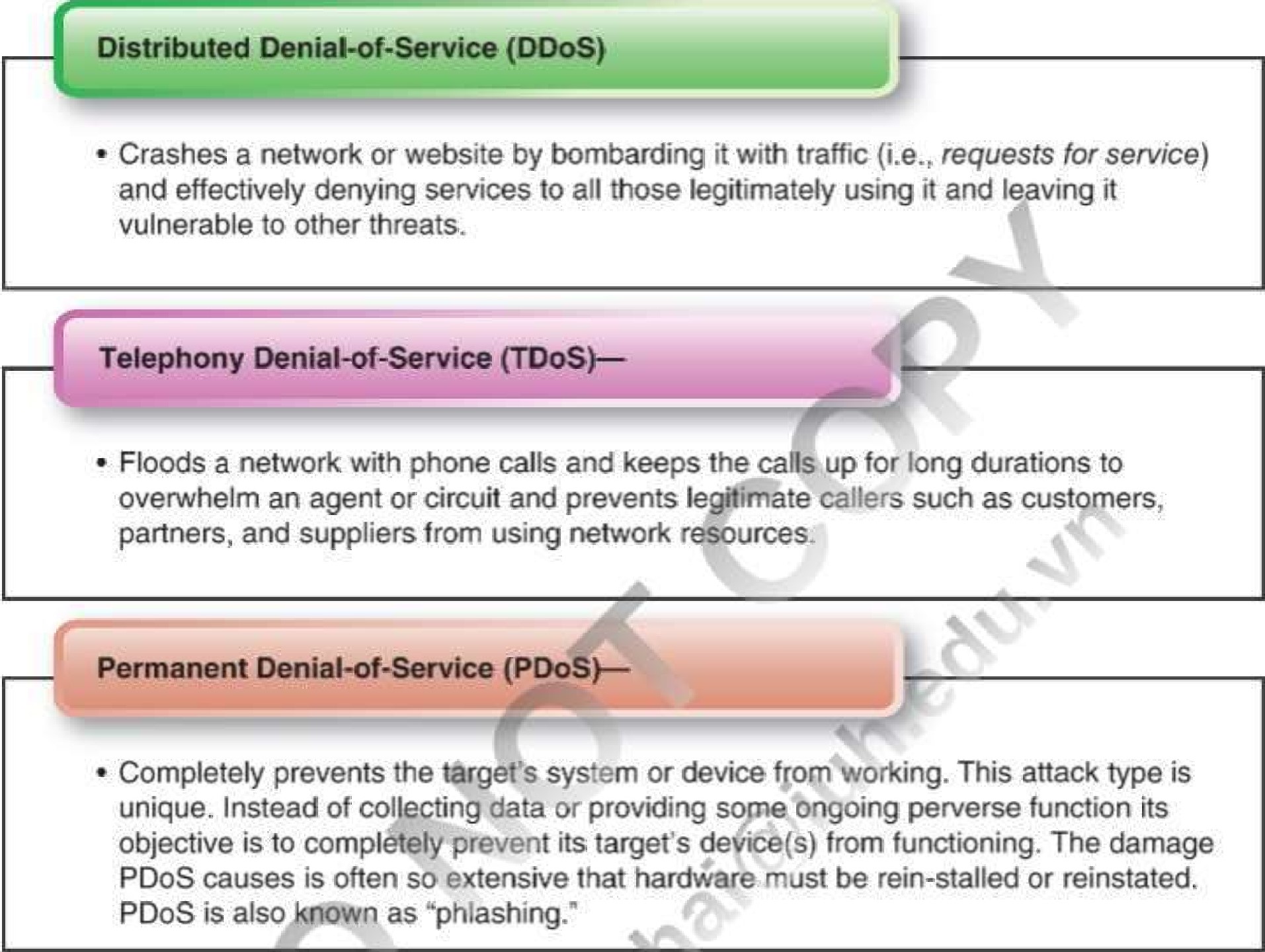
connection

with

two

nạn nhân và chuyển tiếp tin nhắn giữa họ để tạo cảm giác rằng họ đang nói chuyện trực tiếp với nhau trong một cuộc trò chuyện riêng tư trong khi thực tế toàn bộ cuộc trò chuyện đều do kẻ tấn công kiểm soát. Kẻ tấn công chặn tất cả các tin nhắn có liên quan giữa hai nạn nhân và xen vào những tin nhắn mới để có lợi cho anh ta. Thông thường, những kẻ tấn công trong cuộc tấn công MitM đang tìm kiếm các yêu cầu thanh toán mà chúng có thể chặn và thu lợi từ đó.

Theo các chuyên gia an ninh mạng, các mối đe dọa từ chối dịch vụ (DOS) cũng đang gia tăng và cần phải là ưu tiên hàng đầu của các tổ chức . Các mối đe dọa DOS có nhiều "hương vị", tùy thuộc vào mục tiêu của chúng. Ba dạng nổi bật nhất được mô tả trong Eig ure-52Z .



đ. HÌNH 5.7 Ba hình thức Dos.

Một ví dụ "lạnh sống lưng" về sự tàn phá mà PDoS có thể gây ra đã được chứng minh khi một cuộc tấn công PDoS khiến hệ thống quản lý tòa nhà ngoại tuyến trong một khu chung cư dân cư ở Phần Lan. Kết nối Internet của hệ thống đã bị chặn khiến hệ thống liên tục cố gắng [kết nối lại bằng cách tự khởi động lại. Trong thời gian ngừng hoạt động này, hệ thống không thể cung cấp nhiệt tại thời điểm nhiệt độ dưới mức đóng băng! May mắn thay, công ty năng lượng đã có thể tìm chỗ ở thay thế cho cư dân cho đến khi hệ thống được đưa trở lại trực tuyến.

##### Mối đe dọa nội bộ

Không phải tất cả những kẻ tấn công mạng đều do những người bên ngoài tổ chức thực hiện. Các mối đe dọa nội bộ và lạm dụng các mối đe dọa đặc quyền là một thách thức lớn phần lớn do có nhiều cách mà một nhân viên hoặc nhà thầu có thể thực hiện các hoạt động độc hại. Những người này có thể bỏ qua các biện pháp bảo mật vật lý (ví dụ: cửa bị khóa) và bảo mật kỹ thuật (ví dụ: mật khẩu) mà các tổ chức đã đưa ra để ngăn chặn truy cập trái phép. Tại sao? Bởi vì các biện pháp phòng thủ như tường lửa và hệ thống phát hiện xâm nhập (IDS) được thiết kế chủ yếu để bảo vệ chống lại các mối đe dọa từ bên ngoài. Một phương pháp thường được những người trong cuộc sử dụng là giả mạo dữ liệu , một phương thức tấn công mạng phổ biến bị các loại tấn công khác làm lu mờ. Giả mạo dữ liệu là cực kỳ nghiêm trọng vì nó có thể không bị phát hiện.

Giả mạo dữ liệu là một cuộc tấn công mạng trong đó ai đó nhập dữ liệu giả mạo hoặc gian lận vào máy tính hoặc thay đổi hoặc xóa dữ liệu hiện có.

Hai mối đe dọa mạng có thể được phân loại là cố ý và không cố ý là hành vi trộm cắp hoặc mất mát vật lý và các lỗi linh tinh.

Trộm cắp hoặc mất mát vật chất là mối đe dọa tài sản thông tin bị thất lạc, cho dù do sơ suất hay cố ý,

có thể khiến các công ty rơi vào tình trạng hoảng loạn. Việc "thu nhỏ" máy tính đã dẫn đến sự gia tăng trộm cắp hoặc mất mát vật lý. Máy tính xách tay, máy tính bảng, modem, bộ định tuyến và USB dễ vận chuyển hơn nhiều so với máy tính lớn hoặc máy chủ! Khi một máy tính xách tay hoặc máy tính bảng chứa các tài liệu nhạy cảm chưa được mã hóa bị thất lạc, rất khó để xác định xem liệu vi phạm dữ liệu có thực sự xảy ra hay không, nhưng phải luôn thực hiện các biện pháp phòng ngừa. Trộm cắp máy tính xách tay chủ yếu xảy ra trong khu vực làm việc của nạn nhân hoặc từ phương tiện của họ. Trộm cắp có nhiều khả năng liên quan đến việc mua ổ đĩa USB và giấy in. Về mặt tích cực, đồ bị mất phổ biến hơn nhiều so với hành vi trộm cắp.

Các lỗi khác cũng có thể là nguyên nhân dẫn đến vi phạm dữ liệu. Mối quan tâm chính liên quan đến nguồn đe dọa mạng này là tình trạng thiếu năng lực khiến thông tin không thể có sẵn ở bất cứ đâu và khi cần thiết. Các hành động đe dọa khác được trình bày trong Bảng 5.3 thuộc loại lỗi linh tinh này ít phổ biến hơn.

|  |  |
| --- | --- |
| BẢNG LÊ 5.3 | |
|  | |
| hành động đe dọa | Sự miêu tả |
| Thiếu công suất | Không đủ dung lượng máy tính để cung cấp thông tin ở đâu và khi cần |
| giao hàng sai | Thông tin được gửi đến nhầm người, khi e-mail hoặc tài liệu được gửi đến nhầm người |
| Lỗi xuất bản | Thông tin được xuất bản cho khán giả ngoài ý muốn, chẳng hạn như toàn bộ Internet, cho phép họ xem nó |
| cấu hình sai | Quy tắc tường lửa bị nhập sai cho phép truy cập vào máy chủ tệp nhạy cảm từ tất cả các mạng nội bộ thay vì một nhóm máy chủ cụ thể |
| lỗi xử lý | Ổ cứng không bị "xóa sạch" trên các thiết bị đã ngừng hoạt động |
| lỗi lập trình | Mã bị nhập sai hoặc logic bị thiếu sót |
| Lỗi nhập ngày | Dữ liệu được nhập không chính xác hoặc vào tệp không chính xác hoặc trùng lặp |
| Bỏ sót | Dữ liệu không được nhập vào; tài liệu không được gửi |

IT at Work 5.2 minh họa cách các mối đe dọa nội bộ có thể vô tình dẫn đến hậu quả thảm khốc.

|  |
| --- |
| CNTT tại nơi làm việc 5.2  Nhân viên của Bộ Dịch vụ Nhân sinh Oregon Thất bại vì Lừa đảo  Vào tháng 1 năm 2019, chín Bộ phận Dịch vụ Nhân sinh Oregon (OD ) đã bị lừa bởi các e-mail là sản phẩm của một chiến dịch lừa đảo có mục tiêu lớn. Ban đầu, vi phạm được báo cáo là đã ảnh hưởng đến 350.000 bệnh nhân, nhưng sau đó được tiết lộ rằng có tổng cộng 645.000 người đã đăng ký nhận trợ cấp với ODHS    đã có thông tin cá nhân của họ vô tình tiếp xúc với tin tặc.  Một ngày sau vụ tấn công, chín nhân viên của ODHS đã gặp sự cố khi truy cập tài khoản e-mail của họ và một cuộc điều tra sau đó đã phát hiện ra vi phạm. ODHS đã thuê @ nhóm bảo mật bên thứ ba để điều tra sự cố, họ đã xác định rằng không có phần mềm độc hại nào được cài đặt trên hệ thống của ODHS nhưng những kẻ tấn công đã có thể truy cập hơn hai triệu e-mail: Các e-mail chứa tệp đính kèm dữ liệu cá nhân và y tế của nhiều hơn    645.000 bệnh nhân đã đăng ký nhận các lợi ích khác nhau. Nhân viên của ODHS đã mất 20 ngày để bảo mật các tài khoản sau khi tin tặc tấn công hệ thống lần đầu tiên. Trong thời gian đó, tin tặc có quyền truy cập vào tên bệnh nhân, địa chỉ, ngày sinh, số an sinh xã hội, số hồ sơ và thông tin sức khỏe được bảo vệ khác. Để bảo đảm    hệ thống, các quan chức của ODHS đã bắt đầu thiết lập lại mật khẩu để ngăn chặn mọi truy cập trái phép khác và quyền truy cập từ xa vào các tài khoản bị xâm nhập đã bị chấm dứt. May mắn thay, cuộc điều tra đã không tìm thấy bằng chứng cho thấy những kẻ tấn công đã sao chép dữ liệu từ hệ thống ODHS. ODHS nhanh hơn hầu hết các mục tiêu bị ảnh hưởng khiến vi phạm được công khai chỉ ba tuần sau khi xảy ra. Đổi lại việc vi phạm an ninh, các bệnh nhân ODHS có cơ hội đăng ký tham gia một chương trình miễn phí mang đến cho họ một năm dịch vụ theo dõi và khôi phục hành vi trộm cắp danh tính.  Sau vụ tấn công, ODHS nhấn mạnh rằng họ có các biện pháp an ninh mạng để bảo vệ dữ liệu bệnh nhân, |
|

|  |
| --- |
| bao gồm các bản cập nhật bảo mật, bản vá cập nhật, đánh giá bảo mật độc lập, phần mềm bảo mật đặc biệt và định tuyến đào tạo nhân viên về lừa đảo. Một cuộc chữa lành trạng thái được tổ chức do cuộc tấn công đã làm sáng tỏ tần suất mà tin tặc đã nhắm mục tiêu vào các loại cơ quan chính phủ này trong vài năm qua và việc thiếu nhân sự và nguồn lực mà nhiều tổ chức chính phủ và chăm sóc sức khỏe phải đối mặt các loại tấn công mạng khó ngăn chặn và phát hiện.  Nguồn: Tổng hợp từ Anonymous ( 2019b ), Chaffin ( 2019 ), Cimpanu ( 2019 ), Davis ( 2019a ), Davis ( 2019b ) và Rajagopal ( 2019 ). |

Bảng 5.4 liệt kê một số cách mà các tổ chức có thể bảo vệ chống lại các mối đe dọa mạng có chủ ý và không chủ ý khác nhau mà chúng tôi đã thảo luận.

|  |  |
| --- | --- |
|  | |
| Cách bảo vệ chống lại các mối đe dọa mạng có chủ ý và không chủ ý | |
| Nguồn/Loại | Giải pháp |
| hack | Đào tạo nhân viên của bạn  Thay đổi mật khẩu thường xuyên Có mật khẩu "mạnh" |
| Kỹ thuật xã hội | Đừng tin tưởng. Xác thực nguồn. |
| Lừa đảo | Đào tạo nhân viên của bạn  Giám sát hoạt động |
| Lừa đảo giáo | Sử dụng mật khẩu bằng lời nói; triển khai bộ lọc thư rác chất lượng Chỉ cho phép e-mail từ máy chủ được ủy quyền |
| Phần mềm độc hại | Sử dụng phần mềm antimalwareJAV Patch kịp thời |
| phần mềm tống tiền | Theo dõi sự thay đổi và xem các chỉ số chính; sao lưu hệ thống thường xuyên Capture dữ liệu về các cuộc tấn công  Thực hành nguyên tắc đặc quyền tối thiểu |
| Đánh cắp tiền điện tử | Thêm tiện ích mở rộng cho trình duyệt Web như ke NoCoin, minerlLoc k 0BNoScript |
| tiêm SQL | Sử dụng cơ chế mã hóa tham số an toàn loại Xác thực chuỗi đầu vào ở phía máy chủ |
| Người trung gian | Sử dụng mã hóa mạnh giữa máy khách và máy chủ |
| Từ chối dịch vụ | Tách riêng các máy chủ chính  Chọn nhà cung cấp của bạn một cách cẩn thận  Kiểm tra dịch vụ chống DDoS của bạn |
| Nội gián và lạm dụng đặc quyền | Giám sát hành vi người dùng  Theo dõi việc sử dụng phương tiện di động  Biết dữ liệu của bạn |
| Trộm cắp vật chất | Mã hóa dữ liệu của bạn  Đào tạo nhân viên của bạn  Giảm sử dụng giấy |
| Tổn thất vật chất | Kích hoạt dữ liệu của bạn Đào tạo nhân viên của bạn |
| lỗi khác | Học hỏi từ những sai lầm của bạn Tăng cường kiểm soát  Đảm bảo tất cả các tài sản đều trải qua quá trình kiểm tra nghiêm ngặt của bộ phận CNTT trước khi ngừng hoạt động hoặc xử lý |

Điều gì thúc đẩy tội phạm mạng?

Những tên tội phạm Cvber có những lý do khác nhau và có những khó khăn khác nhau khi tiến hành một cuộc tấn công cvber. Một số Qrouv hoặc

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

các cá nhân thích tiến hành các cuộc tấn công "cao cấp" trong khi những người khác thích làm việc "dưới tầm ngắm". Sự khác biệt giữa hai điều này được giải thích tiếp theo.

##### Các cuộc tấn công mạng "Cấu hình cao"

Tin tặc và những người theo chủ nghĩa hack với mục đích cá nhân thực hiện các cuộc tấn công nổi tiếng để được công nhận và nổi tiếng. Các nhóm hoạt động tin tặc, chẳng hạn như Anonymous, một mạng lưới quốc tế liên kết lỏng lẻo gồm các thực thể hoạt động và hoạt động tin tặc và nhóm tin tặc phụ của nó, LulzSec, đã thực hiện các vụ vi phạm dữ liệu táo bạo, thỏa hiệp dữ liệu, rò rỉ dữ liệu, trộm cắp, đe dọa và xâm phạm quyền riêng tư. Hãy xem xét ba ví dụ sau:

• Ủy ban bầu cử Philippines Vài tháng trước cuộc bầu cử ở Philippines, nhóm tin tặc Anonymous đã xâm nhập vào trang web\*của ủy ban và tiết lộ thông tin cá nhân của 55 triệu cử tri đã đăng ký. Cuộc biểu tình nhằm đáp trả các biện pháp an ninh lỏng lẻo của Philippines xung quanh các máy bỏ phiếu của họ; 1,3 triệu thông tin của cử tri ở nước ngoài, bao gồm số hộ chiếu, đã được đưa vào vi phạm.

• Tổ hợp Hệ thống, Inc. Tự hào hiển thị lá cờ hacktivist của mình, Anonymous đã ghi công vì đã đánh sập Hệ thống kết hợp, Inc. ngoại tuyến và đánh cắp dữ liệu cá nhân từ các khách hàng của mình. Anonymous đã theo đuổi Hệ thống kết hợp, nơi bán hơi cay và các thiết bị kiểm soát đám đông cho các tổ chức thực thi pháp luật và quân sự, để phản đối những kẻ trục lợi chiến tranh.

• CIA Hai lần trong một năm, Anonymous tiến hành một cuộc tấn công DOS buộc trang web của CIA phải ngừng hoạt động. Cuộc triệt phá của CIA diễn ra sau một tuần bận rộn đối với những kẻ tấn công. Trong vòng 10 ngày, nhóm này cũng đã truy lùng nhà sản xuất điện tử Trung Quốc Foxconn, các nhóm phát xít Mỹ, AV finn Symantec và (anh ấy là văn phòng của tổng thống Syria.

###### Các cuộc tấn công mạng "dưới tầm radar"

Không phải tất cả bọn tội phạm mạng đều tìm kiếm sự nổi tiếng. Một số có động cơ vì lợi nhuận như những kẻ tấn công đe dọa liên tục nâng cao ( BET ) thường hoạt động ở chế độ tàng hình. APT hoạt động dưới sự giám sát của radar để chúng có thể giám sát hoạt động của mạng và đánh cắp dữ liệu thay vì gây thiệt hại cho mạng hoặc tổ chức, như được mô tả trong IT at Work 5.1

Mối đe dọa liên tục nâng cao (APT) là một cuộc tấn công mạng kéo dài và có mục tiêu, trong đó kẻ tấn công giành được quyền truy cập vào mạng và không bị phát hiện trong một khoảng thời gian. 

APTS thường nhắm vào các bí mật của công ty và chính phủ. Hầu hết các cuộc tấn công APT được thực hiện thông qua lừa đảo. Thông thường, kiểu tấn công này bắt đầu với một số do thám từ phía những kẻ tấn công. Điều này có thể bao gồm việc nghiên cứu thông tin công khai về công ty và nhân viên của công ty, thường là từ các trang mạng xã hội. Thông tin này sau đó được sử dụng để tạo các thư điện tử lừa đảo được nhắm mục tiêu'. Một cuộc tấn công thành công có thể cấp cho kẻ tấn công quyền truy cập vào mạng của doanh nghiệp .

Mục đích của APT là hoạt động gián điệp dài hạn. Sau khi được cài đặt trên mạng, APT sẽ truyền các bản sao của tài liệu, chẳng hạn như tệp Microsoft Office và PDF, ở chế độ ẩn. APT thu thập và'Lưu trữ các tệp trên mạng của công ty; mã hóa chúng; sau đó gửi chúng liên tục đến các máy chủ thường ở Trung Quốc hoặc Nga. Kiểu tấn công này đã được quan sát thấy trong các vụ vi phạm dữ liệu quy mô lớn khác làm lộ số lượng danh tính đáng kể.



Một cuộc tấn công mạng thực sự gây thiệt hại bao nhiêu cho một tổ chức?

Vào năm 2019, tổng chi phí trung bình toàn cầu của một vụ vi phạm dữ liệu là 3,92 triệu đô la, Quy mô trung bình của một vụ vi phạm dữ liệu là 25.575 bản ghi, chi phí cho mỗi bản ghi bị mất là 150 đô la và Mất trung bình 279 ngày để các công ty xác định và ngăn chặn vi phạm . Các công ty ở Hoa Kỳ đã báo cáo chi phí vi phạm trung bình cao nhất là 8,19 triệu đô la (tăng từ 7,91 triệu đô la vào năm 2018) và chăm sóc sức khỏe có chi phí trung bình cao nhất trong ngành là 6,45 triệu đô la (IBM Security, 2019). Một số chi phí rất dễ nhìn thấy và định lượng, chẳng hạn như giá cổ phiếu giảm, hình phạt tài chính và tiền phạt của chính phủ liên bang và tiểu bang được đánh giá do an ninh mạng không đầy đủ. Tuy nhiên, yếu tố đóng góp lớn nhất, mất việc kinh doanh, có thể gây ra những tác động tiêu cực nghiêm trọng kéo dài trong nhiều năm, dẫn đến một loạt chi phí vô hình liên quan đến phản ứng dữ dội của người tiêu dùng, danh tiếng bị tổn hại, gián đoạn hoạt động và mất IP hoặc các tài sản chiến lược khác. Một số trong số này rất khó đo lường vì chúng không dễ định lượng.

Khi đánh giá thiệt hại do một cuộc tấn công mạng gây ra, cùng với tổn thất kinh doanh cực kỳ quan trọng, có ba loại chi phí chính khác được tính vào tổng chi phí do vi phạm dữ liệu. Đó là:

Phát hiện và leo thang—chi phí để tiến hành các hoạt động cho phép công ty phát hiện vi phạm và báo cáo cho nhân viên thích hợp

1. Thông báo—chi phí để thực hiện các hoạt động cho phép công ty thông báo cho các cơ quan quản lý và cá nhân có dữ liệu người thừa kế được cnmnrom hóa trong hreac

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

tnel r data compromsea Trong tne Dreacn

1. Đăng phản hồi về vi phạm dữ liệu—chi phí để tạo, vận hành và duy trì các quy trình được thiết lập để giúp khách hàng giao tiếp với công ty, chẳng hạn như trung tâm cuộc gọi, cũng như chi phí liên quan đến khắc phục và sửa chữa.

#### câu hỏi

1. Xác định và đưa ra một ví dụ về một mối đe dọa cố ý và một mối đe dọa vô ý.
2. Tại sao ban quản lý không coi các mối đe dọa trực tuyến là ưu tiên hàng đầu?

3, Mô tả sự khác nhau giữa từ chối dịch vụ phân tán (DDoS), từ chối dịch vụ điện thoại (TDoS) và từ chối dịch vụ vĩnh viễn (PDoS).

1. Liệt kê và định nghĩa ba loại phần mềm độc hại.
2. Những rủi ro gây ra bởi giả mạo dữ liệu là gì?
3. Định nghĩa trojan là gì và giải thích tại sao nó nguy hiểm.
4. Tại sao các cuộc tấn công MitM đang gia tăng? Làm thế nào các công ty có thể bảo vệ chống lại các cuộc tấn công MitM?

8. Cryptojacking là gì? Làm thế nào bạn có thể tự bảo vệ mình khỏi trở thành nạn nhân của cryptojacking?

### 5.3 Mục tiêu và hậu quả của cuộc tấn công mạng

L05.3 Thảo luận về sáu mục tiêu nguy hiểm nhất của các cuộc tấn công mạng •và đưa ra ví dụ về tác động của từng mục tiêu đối với người tiêu dùng và tổ chức.

Mọi doanh nghiệp đều có dữ liệu mà tội phạm có động cơ lợi nhuận nhắm đến. Dữ liệu khách hàng, mạng, trang web, hệ thống thông tin độc quyền và bằng sáng chế là những ví dụ về tài sản kỹ thuật số có giá trị cần được bảo vệ. Tuy nhiên, ngay cả các công ty công nghệ cao và những người dẫn đầu thị trường dường như cũng phần nào tách rời khỏi giá trị của dữ liệu bí mật mà họ lưu trữ và cách thức mà bọn tội phạm mạng có động lực cao sẽ cố gắng/hoặc đánh cắp chúng.

Một trong những sai lầm lớn nhất mà các nhà quản lý mắc phải là đánh giá thấp các lỗ hổng và mối đe dọa CNTT. Ví dụ: người lao động sử dụng CNTT bóng như máy tính xách tay cá nhân và thiết bị di động để vừa làm việc vừa giải trí, và trong thời đại đa nhiệm, họ thường làm cả hai việc cùng một lúc. Tuy nhiên, việc sử dụng thiết bị ngoài thời gian hoặc ngoài địa điểm vẫn có rủi ro vì , bất chấp các chính sách, nhân viên vẫn tiếp tục tham gia vào các thói quen giao tiếp và trực tuyến nguy hiểm. Những thói quen đó khiến họ trở thành một mắt xích yếu trong nỗ lực bảo mật vững chắc của một tổ chức.

#### Mục tiêu tấn công mạng phổ biến và nguy hiểm nhất

Các mục tiêu nguy hiểm và phổ biến nhất mà tội phạm mạng tấn công vào các công ty và cơ quan chính phủ bao gồm: mật khẩu yếu, cơ sở hạ tầng quan trọng; trộm IP bf; hành vi trộm cắp danh tính; bóng IT; mang theo thiết bị của riêng bạn (BYOD) và phương tiện truyền thông xã hội.

##### mật khẩu yếu

Một trong những điểm yếu lớn nhất của an ninh mạng mà bọn tội phạm mạng muốn nhắm đến là những người dùng bỏ qua sự nguy hiểm của mật khẩu yếu và việc sử dụng lại mật khẩu. Việc nắm bắt và sử dụng sai thông tin đăng nhập, chẳng hạn như ID và mật khẩu của người dùng, là một trong những kỹ năng cơ bản mà tin tặc sử dụng để thực hiện nhiều các loại mối đe dọa mạng, chẳng hạn như lừa đảo, khiến các tổ chức dễ bị vi phạm dữ liệu. Ví dụ: kẻ tấn công có thể đưa một số mã SQL vào hộp nhập liệu Web fom chẳng hạn như hộp gửi hoặc hộp văn bản thanh toán có thể chỉnh sửa để có quyền truy cập vào tài khoản của người dùng nhằm thu thập tài nguyên hoặc thay đổi dữ liệu, với số lượng lớn các vụ vi phạm dữ liệu toàn cầu đang xảy ra, rất có thể mỗi người dùng đều có ít nhất một trang web hoặc ứng dụng đã bị xâm phạm. Quản lý thích hợp là điều cần thiết để bảo mật vì vi phạm mật khẩu người dùng có thể nguy hiểm. Ngay cả mật khẩu an toàn nhất cũng có thể trở nên vô hiệu nếu nó được sử dụng trên mọi trang web và trong mọi ứng dụng. Để chống lại điều này, một chính sách mật khẩu mạnh cần được áp dụng như một hình thức "thẩm định" để bảo vệ người tiêu dùng và tránh các vụ kiện. Chính sách mật khẩu nên bao gồm việc thực thi các mật khẩu mạnh cho tất cả các ứng dụng Web và thực hiện kiểm tra thường xuyên các mật khẩu yếu.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

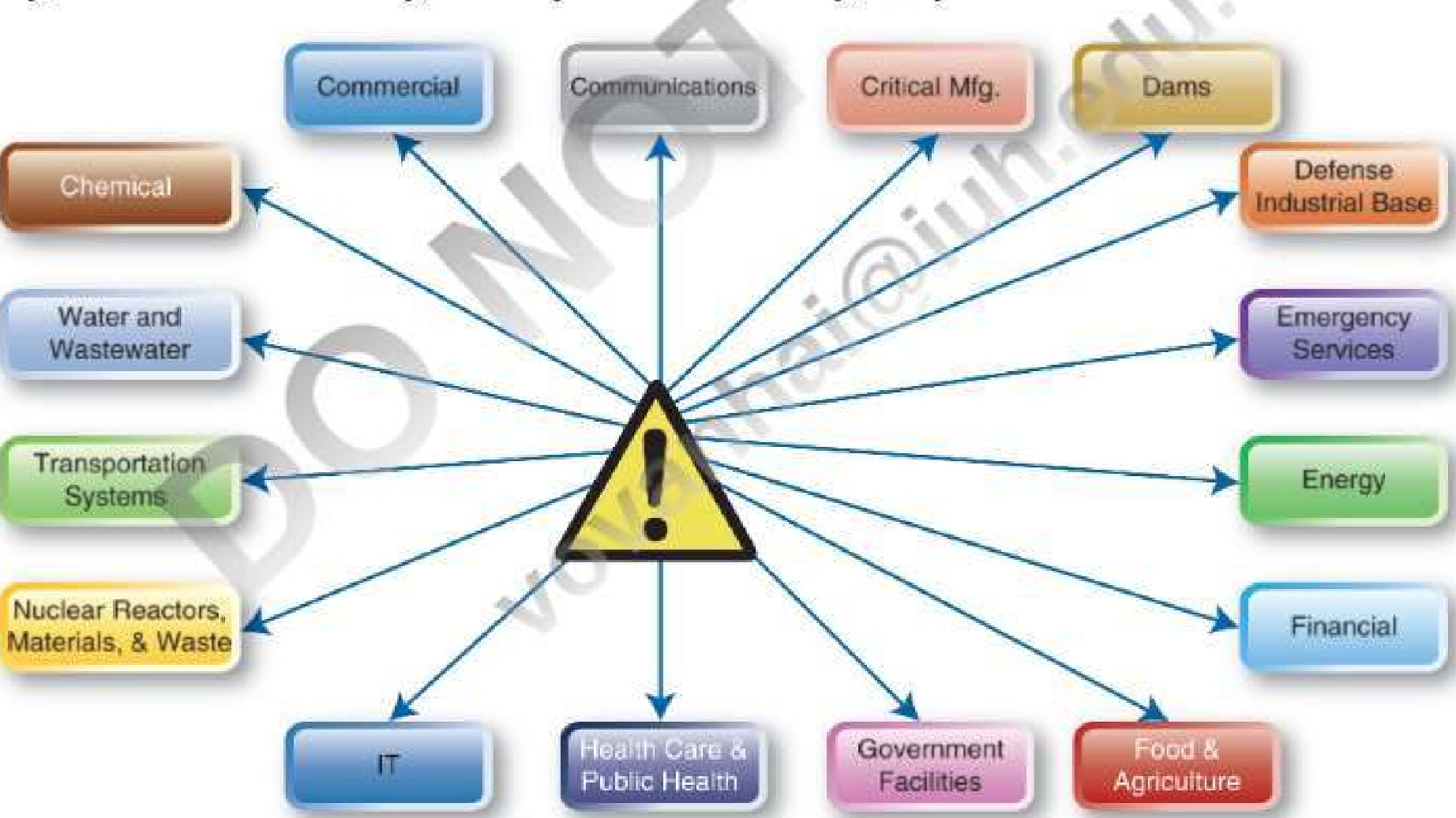
###### Cơ sở hạ tầng quan trọng

Cơ sở hạ tầng quan trọng được định nghĩa là "các hệ thống và tài sản dù là vật chất hay ảo, rất quan trọng đối với một quốc gia đến mức việc các hệ thống và tài sản đó không hoạt động hoặc bị phá hủy sẽ có tác động xấu đến an ninh, an ninh kinh tế quốc gia, sức khỏe hoặc an toàn công cộng quốc gia, hoặc bất kỳ sự kết hợp của những vấn đề đó” (Bộ Tư pháp, 2001).

Tin tặc, kẻ tấn công, tổ chức tội phạm, gián điệp công nghiệp của nhóm chiến binh, kẻ lừa đảo và chính phủ thù địch tiếp tục tấn công mạng vì lợi nhuận, danh tiếng, sự trả thù hoặc một hệ tư tưởng; tiến hành chiến tranh và khủng bố, chiến đấu chống lại chiến dịch khủng bố hoặc vô hiệu hóa mục tiêu của chúng. Ví dụ: Nhóm Ứng phó Khẩn cấp Mạng Hệ thống Kiểm soát Công nghiệp (ICS-CERT) của Bộ An ninh Nội địa (DHS) đã cảnh báo rằng các cuộc tấn công chống lại các cuộc tấn công quan trọng đang gia tăng. Ngành bị ảnh hưởng nhiều nhất là ngành năng lượng.

Một dạng phần mềm độc hại mới, được gọi là Industroyer đã được phát triển để nhắm mục tiêu vào cơ sở hạ tầng quan trọng trong lĩnh vực năng lượng. Industroyer kiểm soát trực tiếp các bộ ngắt mạch của trạm biến áp điện bằng cách sử dụng các giao thức truyền thông công nghiệp. Điều này có nghĩa là các nhà máy điện, hệ thống điều khiển giao thông, nhà máy nước và khí đốt đều là mục tiêu tiềm năng của công cụ mạnh mẽ này, 

Ví dụ 5.8: chỉ ra tài sản của 16 lĩnh vực cơ sở hạ tầng quan trọng; các hệ thống và mạng, dù là vật lý hay ảo, được coi là quan trọng đến mức việc mất khả năng hoặc sự phá hủy của chúng sẽ có tác động làm suy yếu an ninh của một quốc gia , an ninh kinh tế quốc gia, an toàn y tế công cộng quốc gia hoặc bất kỳ sự kết hợp nào của chúng.



FIGURE

5.8

Critical

infrastructure

sectors.

Các cuộc tấn công vào các lĩnh vực cơ sở hạ tầng quan trọng có thể làm gián đoạn đáng kể hoạt động của chính phủ và doanh nghiệp—đồng thời gây ra các tác động theo tầng vượt ra ngoài lĩnh vực được nhắm mục tiêu và vị trí thực tế xảy ra sự cố. Những cuộc tấn công mạng này có thể làm tổn hại đến cơ sở hạ tầng quan trọng của một quốc gia và khả năng cung cấp các dịch vụ thiết yếu cho công dân của quốc gia đó.

Ví dụ: cuộc tấn công mạng đầu tiên nhằm vào lưới điện của một quốc gia xảy ra vào tháng 12 năm 2015, khi một kẻ tấn công mạng chiếm quyền kiểm soát thành công Trung tâm điều khiển Prykarpattyaoblenergo (PCC) ở miền Tây Ukraine khiến 230.000 công dân không có điện trong vòng 6 giờ. Những kẻ tấn công đã lên kế hoạch cẩn thận cho cuộc tấn công của chúng trong nhiều tháng. Họ đã nghiên cứu các mạng và thông tin đăng nhập của người điều hành siphon và cuối cùng tung ra cuộc tấn công đồng bộ tàn khốc vào giữa mùa đông. PCC vận hành hệ thống điều khiển giám sát và thu thập dữ liệu (SCADA), là một dạng phổ biến của hệ thống điều khiển công nghiệp, phân phối điện năng. Các thiết bị quan trọng tại 16 trạm biến áp không phản hồi với bất kỳ lệnh từ xa nào của người vận hành sau khi kẻ tấn công ghi đè lên chương trình cơ sở của nó. Loại hệ thống kiểm soát này an toàn hơn một số loại được sử dụng ở Hoa Kỳ một cách đáng ngạc nhiên vì chúng có tường lửa mạnh mẽ ngăn cách

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

chúng từ các mạng kinh doanh của trung tâm điều khiển.

Các chính phủ trên khắp thế giới đã có kế hoạch sẵn sàng để giải quyết hậu quả của thiên tai, nhưng không có kế hoạch cứu trợ thiên tai nào đối với lưới điện bị sập. Rõ ràng, điều này phải thay đổi. Chính quyền địa phương và tiểu bang phải làm việc cùng với các đối tác quốc gia của họ để sản xuất và nhanh chóng thực hiện các kế hoạch giải quyết các cuộc tấn công trong tương lai. Ví dụ về các cơ sở hạ tầng quan trọng khác đã bị xâm phạm bao gồm:

* Tập đoàn điều hành hạt nhân Wolf Creek, Kansas, Hoa Kỳ—các kỹ thuật lừa đảo trực tuyến đã được sử dụng để nhắm mục tiêu vào các cá nhân có quyền truy cập vào các quyền kiểm soát quan trọng của nhà máy
* Rye Brooke, NY Dam—đã tấn công hệ thống chỉ huy và kiểm soát bằng modem di động
* Trạm biến áp Pivichna gần Kiev, Ukraine—cuộc tấn công mạng vào việc kiểm soát giám sát và thu thập dữ liệu đã gây ra sự cố mất điện kéo dài một giờ đối với các khu vực có nắng

Để đối phó với số lượng các cuộc tấn công mạng ngày càng tăng trong thập kỷ qua, Ủy ban liên Mỹ

Chống khủng bố (CICTE) đã ban hành một tuyên bố chính thức để bảo vệ cơ sở hạ tầng quan trọng khỏi các mối đe dọa mới nổi và một sắc lệnh hành pháp của Tổng thống đã được ký vào tháng 5 năm 2017 để tăng cường an ninh mạng của các mạng Liên bang và cơ sở hạ tầng quan trọng . Năm quốc gia thể hiện cam kết cao nhất đối với an ninh mạng là Vương quốc Anh, Hoa Kỳ, Pháp, Litva và Estonia.

sở hữu trí tuệ\_(IP) đang gia tăng. Điều này đặc biệt đáng lo ngại vì sở hữu trí tuệ có thể chiếm hơn 80% giá trị của một công ty và do đó là một phần quan trọng của tất cả các tổ chức trong thế kỷ 21. Mất dữ liệu khách hàng cho tin tặc có thể tốn kém và đáng xấu hổ nhưng mất IP, thường được gọi là bí mật thương mại, không thể đe dọa sự tồn tại của công ty. Ở cấp quốc gia, các chủ thể quốc gia-nhà nước tiếp tục thực hiện các cuộc tấn công vào IP để lấy thông tin có giá trị từ các quốc gia khác, quân đội và các công ty tư nhân của họ.

Sở hữu trí tuệ là một tác phẩm hoặc phát minh là kết quả của sự sáng tạo có giá trị thương mại, bao gồm tài sản có bản quyền như bản thiết kế, bản thảo hoặc thiết kế và được pháp luật bảo vệ khỏi việc sử dụng trái phép của người khác. 

Trộm cắp IP luôn là mối đe dọa từ các nốt ruồi công ty, nhân viên bất mãn và những người trong cuộc khác. Mặc dù một số IP vẫn có thể có được độc quyền thông qua các phương tiện vật lý nhưng số hóa đã khiến hành vi trộm cắp trở nên dễ dàng hơn. Những tiến bộ trong công nghệ, tăng tính di động, toàn cầu hóa nhanh chóng và bản chất ẩn danh của Internet tạo ra những thách thức ngày càng tăng trong việc bảo vệ IP. Phương thức hoạt động ưa thích của tin tặc là đột nhập vào thiết bị di động của nhân viên và đột nhập vào mạng của người sử dụng lao động—đánh cắp bí mật thương mại mà không để lại dấu vết.

Các chuyên gia an ninh mạng và quan chức chính phủ ngày càng lo ngại về các vi phạm từ các quốc gia khác vào mạng của công ty và chính phủ thông qua thiết bị di động hoặc các phương tiện khác. Ví dụ, Bộ An ninh Nhà nước Trung Quốc và Amy Giải phóng Nhân dân (PLA) có nhiệm vụ đánh cắp Hoa Kỳ. bí mật công nghiệp và thương mại và đã đặc biệt hiệu quả trong các cuộc tấn công phi công này chống lại UniteclSiates. Hiện tại không có dấu hiệu nào cho thấy các mối đe dọa đối với tài sản kỹ thuật số và IP của Hoa Kỳ đang chậm lại (Underwood„2019).

Vào tháng 5 năm 2016, Tổng thống Barack Obama đã ký Đạo luật Bảo vệ Bí mật Trqde (DTSA) cho phép "'chủ sở hữu bí mật thương mại khởi kiện dân sự lên tòa án liên bang về hành vi biển thủ bí mật thương mại" (Gibson Dunn, 2016). Cho đến khi DTSA được ký kết, các tập đoàn phải dựa vào luật tiểu bang liên quan đến bí mật thương mại. Bây giờ, mọi công ty Mỹ đều được bảo vệ như nhau theo luật liên bang. Hơn nữa, nó mở rộng quyền lực của chính phủ liên bang trong việc điều chỉnh các bí mật thương mại thông qua thương mại giữa các tiểu bang và nước ngoài trong khi vẫn duy trì các luật bí mật thương mại hiện hành. 

Một ví dụ kinh điển về hành vi trộm cắp IP là cuộc tấn công APT có tên là Chiến dịch Aurora nhằm vào Google và được mô tả trong IT at Work 5.3 .

CNTT tại nơi làm việc 5.3

#### Chiến dịch Aurora nhắm vào các mạng công ty tài chính, quốc phòng và công nghệ lớn

Chiến dịch Aurora là một chiến dịch phản gián do chính phủ Trung Quốc điều hành. Đó là một loạt các cuộc tấn công mạng được thực hiện bởi APTS có quan hệ với Amy Giải phóng Nhân dân ở Trung Quốc. Attacke1S đã truy cập thành công cơ sở dữ liệu gắn cờ các tài khoản Gmail được đánh dấu là nghe lén theo lệnh của tòa án để hiểu rõ hơn về các cuộc điều tra tích cực đang được tiến hành bởi FBI và các cơ quan thực thi pháp luật khác liên quan đến các đặc vụ bí mật của Trung Quốc.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

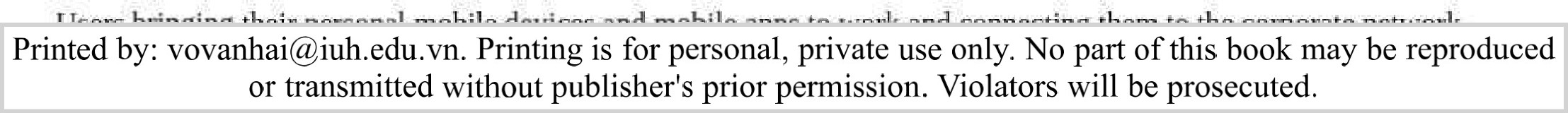
|  |
| --- |
| Để truy cập IP, Chiến dịch Aurora đã khai thác các lỗ hổng bảo mật trong tệp đính kèm email để lẻn vào mạng của các công ty tài chính, quốc phòng và công nghệ lớn cũng như các tổ chức nghiên cứu ở Hoa Kỳ bằng cách thực hiện sáu bước, như được mô tả trong Ví dụ 5.9 . Các công nghệ bảo mật CNTT tiêu chuẩn tại Google đã không thể ngăn sáu bước này xảy ra và cả Google cũng như chủ tài khoản Gmail của Google đều không biết rằng họ đã bị tấn công.  FIGURE  Once  Reportedly,  Operation  Aurora.  Hầu hết các hoạt động hack không trở thành tiêu điểm cho đến khi !nçidents được phát hiện và báo cáo. Ngay cả khi đó, các công ty là nạn nhân vẫn miễn cưỡng thảo luận về chúng, vì vậy số liệu thống kê rất khan hiếm. Trong trường hợp của Chiến dịch Aurora, cuộc tấn công không được phát hiện cho đến gần một năm sau. sự thật!  Nguồn: Tổng hợp từ Corbin ( 2013 ), Schwartz ( 2013 ), Gordon (2014) và Cyware ( 2016 ), |

##### Hành vi trộm cắp danh tính

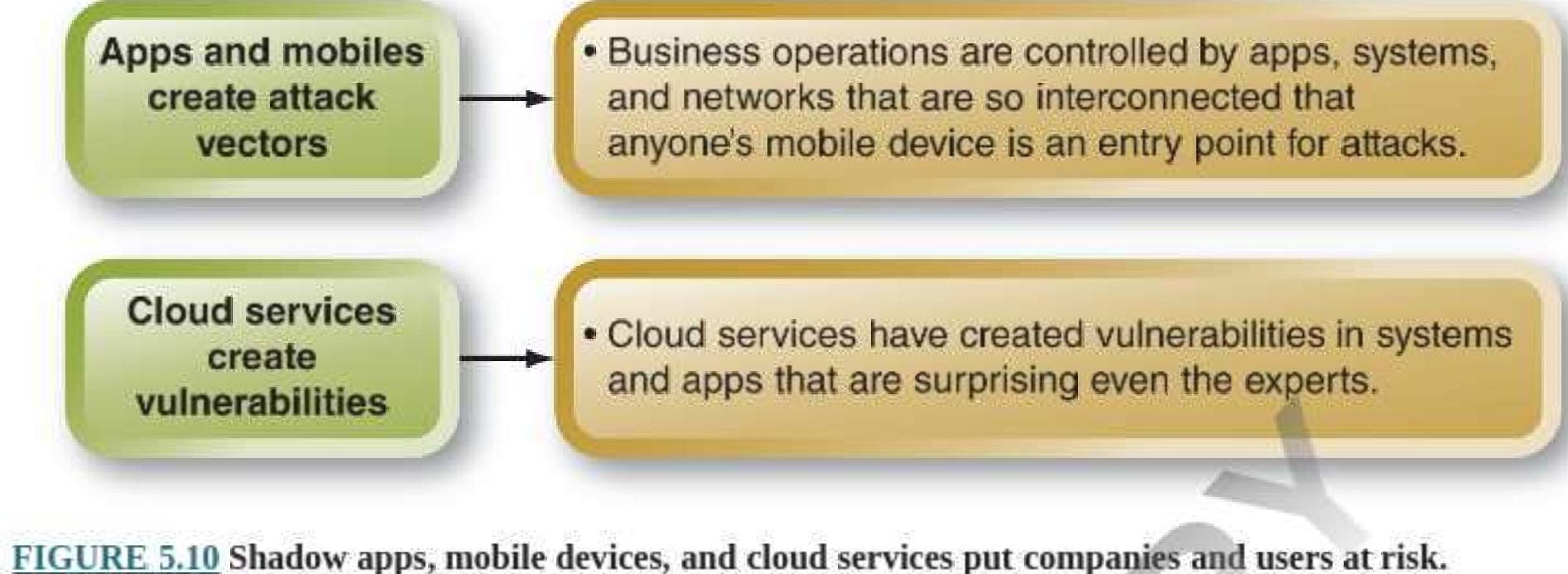
Hành vi trộm cắp danh tính cũng đang gia tăng. Các vụ trộm mà số An sinh xã hội và số thẻ tín dụng của cá nhân bị kẻ trộm đánh cắp và sử dụng là không có: mới. Tội phạm luôn có được thông tin về người khác—bằng cách ăn cắp ví hoặc lặn thùng rác. Nhưng chia sẻ điện tử và cơ sở dữ liệu rộng rãi đã làm cho tội phạm tồi tệ hơn. Vì các tổ chức tài chính, công ty xử lý dữ liệu và doanh nghiệp bán lẻ không muốn tiết lộ các sự cố trong đó thông tin tài chính cá nhân của khách hàng của họ có thể đã bị đánh cắp, bị mất hoặc bị xâm phạm nên các luật tiếp tục được thông qua buộc những thông báo đó Việc đánh cắp danh tính có thể dẫn đến sự thất vọng và gây bất tiện cho nạn nhân về mặt lãng phí thời gian và nguồn lực.

CNTT ẩn, đôi khi được gọi là CNTT tàng hình gây ra các rủi ro bảo mật khi phần cứng và phần mềm không được hỗ trợ được sử dụng bởi các cá nhân hoặc bộ phận phá vỡ các biện pháp bảo mật CNTT áp dụng cho công nghệ được phê duyệt. Ban đầu, CNTT bóng tối bao gồm các mục dễ kiểm soát như macro Microsoft Excel không được phê duyệt và phần mềm đóng hộp mà nhân viên mua tại nhà cung cấp văn phòng store để sử dụng tại nơi làm việc là một số ví dụ đơn giản về Shadow IT. Ngày nay, CNTT bóng tối đã phát triển để bao gồm các ứng dụng đám mây nằm ngoài tường lửa của tổ chức, như Dropbox và Google Tài liệu để chia sẻ tệp và lưu trữ dữ liệu cũng như Twitter, Facebook, WhatsApp WebEx, Salesforce và Google Hangouts Chat để tạo điều kiện cộng tác giữa các thành viên trong nhóm.

CNTT ngoài luồng là việc sử dụng phần cứng hoặc phần mềm liên quan đến CNTT bởi một cá nhân hoặc một bộ phận mà bộ phận CNTT trong tổ chức không hề hay biết.



Người dùng mang thiết bị di động cá nhân và ứng dụng di động của họ đi làm và kết nối chúng với mạng công ty là một phần của xu hướng lớn hơn nhằm tiêu dùng công nghệ thông tin và là một vấn đề quan trọng liên quan đến CNTT ẩn liên quan đến phần cứng. Khi phần cứng CNTT như điện thoại cá nhân, ổ cứng di động, máy tính bảng và ổ USB dung lượng lớn không được bộ phận CNTT chỉ định và triển khai, dữ liệu của một tổ chức có thể đặc biệt dễ bị tấn công và nâng cao các vấn đề tuân thủ khi dữ liệu của công ty không được lưu trữ trong một vị trí an toàn. Các mối quan tâm khác của tổ chức liên quan đến CNTT ngầm bao gồm các tác động tiêu cực đến băng thông và tạo xung đột giao thức ứng dụng mạng và phần mềm. Hình 5.10 tóm tắt cách các ứng dụng CNTT ẩn, thiết bị di động và dịch vụ đám mây có thể đặt các tổ chức vào nguy cơ bị tấn công mạng cao hơn.



FIGURE

5.10

Shadow

apps,

mobile

devices,

and

cloud

services

put

companies

and

users

risk.

Ý kiến về Shadow IT được trộn lẫn. Một mặt, ban quản lý lo lắng rằng ngoài các vấn đề bảo mật, nó sẽ tạo ra các kho chứa dữ liệu của người dùng cuối và hạn chế luồng thông tin tự do trong toàn tổ chức. Những người khác tin rằng CNTT bóng tối có thể hữu ích trong thế giới kinh doanh thay đổi nhanh chóng và CNTT phải thừa nhận rằng nó tồn tại và tạo ra các chính sách sử dụng chấp nhận được để giám sát và sử dụng nó. Những tiến bộ đang được thực hiện trong lĩnh vực này với việc giới thiệu các chính sách CNTT ngầm.

Khoảng 87% các tổ chức của Hoa Kỳ đang sử dụng hoặc có kế hoạch cho phép nhân viên "mang theo thiết bị của riêng bạn"—BYOD. Đó là một khái niệm hấp dẫn vì BYOD cho phép các công ty cắt giảm chi phí bằng cách không phải mua và bảo trì thiết bị di động của nhân viên. Thật không may, nhiều công ty đã lao vào þt mà không xem xét các chính sách này liên quan như thế nào đến bảo mật CNTT. Các thiết bị di động trở thành mục tiêu dễ dàng vì chúng hiếm khi có xác thực mạnh, kiểm soát truy cập và mã hóa ngay cả khi chúng kết nối với các dịch vụ đám mây và dữ liệu tối quan trọng.

Xu hướng BYOD được thúc đẩy bởi các nhân viên sử dụng thiết bị của riêng họ cho mục đích kinh doanh vì chúng mạnh hơn những thiết bị mà công ty đã cung cấp. Một yếu tố khác là tính di động, Trước đây và trước khi có BYOD, nhân viên làm việc tại bàn của họ trên điện thoại cố định và trên máy tính cắm vào tường bằng cáp mạng. Sự thay đổi về mức độ rủi ro này đòi hỏi đầu tư nhiều hơn để chống lại BYODJisks. Khi ngày càng có nhiều người làm việc tại nhà và khi đang di chuyển, ngày làm việc truyền thống từ 9 đến 5 giờ ở văn phòng đã trở thành dĩ vãng.

##### BYOD nêu lên các vấn đề quan ngại nghiêm trọng và hợp pháp 4

Các doanh nghiệp chấp nhận rủi ro với các phương pháp BYOD mà họ sẽ không bao giờ cân nhắc thực hiện với các thiết bị máy tính thông thường. Một lý do có thể là các thiết bị, ứng dụng và Hệ thống mới đã được triển khai quá nhanh. Do đó, điện thoại thông minh không được quản lý như một thiết bị an toàn. Trên thực tế, nhân viên mong đợi sự chấp thuận ngay lập tức (hoặc ít nhất là không phản đối) và hỗ trợ cho máy tính bảng mới của họ trong vòng vài giờ sau khi sản phẩm được phát hành.

Tin tặc đột nhập vào thiết bị di động của nhân viên và đột nhập vào mạng của nhà tuyển dụng—đánh cắp bí mật mà không để lại dấu vết. Các lỗ hổng mới được tạo ra khi dữ liệu và thông tin liên lạc của cá nhân và doanh nghiệp được trộn lẫn với nhau. Tất cả các biện pháp kiểm soát an ninh mạng—xác thực, kiểm soát truy cập, bảo mật dữ liệu và phát hiện xâm nhập—được triển khai trên các tài nguyên thuộc sở hữu của công ty có thể trở nên vô dụng bởi một thiết bị do nhân viên sở hữu. Cơ sở hạ tầng di động của tập đoàn có thể không hỗ trợ được sự gia tăng lưu lượng truy cập mạng di động và xử lý dữ liệu, gây ra sự chậm trễ không thể chấp nhận được hoặc yêu cầu đầu tư bổ sung.

Một vấn đề nghiêm trọng khác phát sinh khi thiết bị di động của nhân viên bị mất hoặc bị đánh cắp. Công ty có thể bị vi phạm dữ liệu nếu thiết bị không được bảo mật đầy đủ bằng mật khẩu mạnh và dữ liệu trên BYOD không được mã hóa.

Các cuộc tấn công mạng trên mạng xã hội được dự đoán sẽ tiếp tục là mối đe dọa lớn đối với doanh nghiệp (Walker, 2019 ). Các công ty Y thực hành bảo mật mạng xã hội kém khiến thương hiệu, khách hàng, giám đốc điều hành và toàn bộ tổ chức của họ gặp rủi ro nghiêm trọng. Mạng xã hội và điện toán đám mây làm gia tăng các lỗ hổng bằng cách cung cấp một điểm thất bại và tấn công duy nhất cho

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

mạng lưới tội phạm có tổ chức. Thông tin quan trọng, nhạy cảm và riêng tư có nguy cơ gặp rủi ro và giống như các xu hướng CNTT trước đây, chẳng hạn như mạng không dây, mục tiêu kết nối, được ưu tiên hơn mối quan tâm về bảo mật. Khi các mạng xã hội tăng dịch vụ của họ, khoảng cách giữa các dịch vụ và bảo mật thông tin cũng tăng lên. Ví dụ: các cuộc tấn công của vi-rút và phần mềm độc hại vào một dịch vụ được thiết lập tốt như e-mail đã giảm do bảo mật e-mail đã được cải thiện trong những năm qua. Thật không may, phần mềm độc hại vẫn đang tìm cách phá vỡ thành công các dịch vụ và thiết bị mới, chẳng hạn như máy đọc sách điện tử, netbook, Chrome OS của Google, Facebook, YouTube, Twitter, Linkedlnt và các mạng truyền thông xã hội dựa trên đám mây khác .

Ví dụ: trong Twitter và Facebook, nơi người dùng xây dựng mối quan hệ với những người dùng khác, tội phạm mạng đang tấn công bằng cách sử dụng thông tin đăng nhập bị đánh cắp. Những kiểu tấn công lợi dụng lòng tin của người dùng rất khó bị phát hiện. Facebook gần đây đã báo cáo rằng họ đã vô hiệu hóa gần 1,3 tỷ tài khoản giả mạo, Twitter đã đình chỉ 70 triệu tài khoản và

Linkedln công khai thừa nhận họ không có hệ thống đáng tin cậy để xác định và đếm các tài khoản lừa đảo trùng lặp. Để chống lại các loại mối đe dọa trực tuyến này, lọc Web, giáo dục người dùng và các chính sách nghiêm ngặt là chìa khóa để ngăn chặn sự bùng phát trên diện rộng.

Mạng và Dịch vụ Tăng Khả năng Tiếp xúc với Rủi ro Lý do quan trọng nhất khiến các mạng và dịch vụ tăng khả năng tiếp xúc với rủi ro là do sự lợi dụng không ngừng của phần mềm gián điệp và vi-rút di động tinh vi ngày nay. Thời gian đó đã rút ngắn từ vài tháng xuống còn vài phút nên nhân viên CNTT có khung thời gian ngắn hơn bao giờ hết để tìm và sửa lỗi trước khi chúng bị xâm phạm bởi một cuộc tấn công. Một số cuộc tấn công tồn tại trong ít nhất hai giờ, điều đó có nghĩa là các hệ thống bảo mật CNTT của doanh nghiệp phải có khả năng bảo vệ theo thời gian thực.

Thời gian để khai thác là thời gian trôi qua giữa khi một lỗ hổng được phát hiện và khi nó được khai thác.

Khi các lỗ hổng mới được tìm thấy trong hệ điều hành, ứng dụng hoặc mạng có dây và không dây, các bản vá lỗi sẽ được nhà cung cấp hoặc tổ chức bảo mật phát hành. Ví dụ: Microsoft phát hành các bản vá mà họ gọi là các gói dịch vụ để cập nhật và khắc phục các lỗ hổng trong hệ điều hành của mình"; bao gồm Vista và các ứng dụng, bao gồm cả Office 2016, Gói dịch vụ có thể được tải xuống từ Trung tâm Cập nhật và Gói Dịch vụ của Microsoft (https ://support.microsoft.com/enus/help/14162/windows-service-pack-and-update-center).

Bản vá là một chương trình phần mềm mà người dùng tải xuống và cài đặt để khắc phục lỗ hổng.

Mặc dù có những biện pháp phòng vệ bằng công nghệ tốt nhất, sự cố bảo mật thông tin vẫn thường xảy ra do người dùng không tuân theo các quy trình và quy trình sử dụng máy tính an toàn.

##### câu hỏi

I. Cơ sở hạ tầng trọng yếu là gì?

1. Liệt kê ba loại cơ sở hạ tầng quan trọng.
2. Làm thế nào để các mạng xã hội và đám mây kết nối làm tăng tính dễ bị tổn thương?

4, Tại sao cần có các bản vá lỗi và gói dịch vụ?

1. Tại sao việc bảo vệ IP lại quan trọng?
2. Động cơ của 'hacktivist và APT khác nhau như thế nào?
3. Giải thích tại sao dữ liệu trên máy tính xách tay và máy tính cần được mã hóa.
4. Giải thích cách hành vi trộm danh tính có thể xảy ra:

Thảo luận video hoạt hình bảng trắng về Chương 5 Học tập Mục tiêu 2 và 3



### 5.4 Bảo vệ chống lại các cuộc tấn công mạng và quản lý rủi ro

L05.4 Xác định sáu chiến lược phòng thủ không gian mạng và bốn phương pháp tiếp cận quản lý rủi ro và các công cụ phòng thủ CNTT có thể được sử dụng để bảo vệ các tổ chức khỏi các cuộc tấn công mạng.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Các nhóm tội phạm có tổ chức nhanh chóng nhận ra rằng tội phạm mạng có kết quả tốt hơn với rủi ro đối với tính mạng, tay chân và quyền tự do thấp hơn đáng kể so với các hoạt động khác như buôn người, buôn lậu, tống tiền và buôn bán ma túy. Họ hầu như không thể chạm tới bởi cơ quan thực thi pháp luật vì thường không ai nhìn thấy tội phạm và nếu tội phạm được xác định, việc thiếu các hiệp ước và hợp tác quốc tế khiến việc bắt giữ và xét xử giữa các quốc gia không dẫn độ đó hầu như không thể. Vì điều này, không có gì ngạc nhiên khi hầu hết mọi cuộc khảo sát đều xác định cùng một xu hướng đáng lo ngại—chi phí khôi phục và tần suất tội phạm mạng ngày càng tăng trong khi chi phí thực hiện đang giảm. Chỉ hai ví dụ về điều này là vi phạm an ninh năm 2013 đối với cơ sở dữ liệu của Target Corporation, trong đó thông tin cá nhân của hàng triệu khách hàng đã bị đánh cắp dẫn đến việc công ty đồng ý trả 18,5 triệu đô la để giải quyết cuộc điều tra của hàng chục tiểu bang và vụ kiện hàng tỷ đô la và cuộc điều tra quy định chống lại Equifax. Để ngăn chặn các cuộc tấn công mạng, các công ty phải coi trọng vấn đề bảo mật dữ liệu của mình hơn và triển khai các biện pháp phòng thủ và thực hành bảo mật CNTT mạnh mẽ hơn.

Để bảo vệ hiệu quả chống lại các cuộc tấn công mạng, ban lãnh đạo cao nhất phải tài trợ và thúc đẩy các sáng kiến bảo mật và tài trợ cho chúng như một ưu tiên hàng đầu. Điều mà hầu hết các nhà lãnh đạo doanh nghiệp không hiểu là làm thế nào để thiết kế, thực hiện; và quản lý các chiến lược an ninh mạng và kế hoạch quản lý rủi ro hiệu quả để ngăn chặn vi phạm dữ liệu và bảo vệ CNTT và tài nguyên kinh doanh. Các cuộc tấn công mạng vào các công ty công nghệ cao như Yahoo, Linkedln, Google, Amazon, eBay và Sony cũng như các cơ quan an ninh hàng đầu như CIA và FBI là bằng chứng cho thấy không ai được an toàn.

Ở cấp độ toàn cầu, Báo cáo Điều tra Vi phạm Dữ liệu năm 2019 của Verizon (Verizon, 2019) đã kiểm tra 41.686 sự cố, trong đó 2.013 sự cố đã được xác nhận là vi phạm dữ liệu. Trong số này, 71% có động cơ tài chính và 25% có động cơ đạt được lợi thế cạnh tranh. Báo cáo cũng cho thấy 69% các trường hợp được thực hiện bởi các nguồn bên ngoài, 39% được thúc đẩy bởi các nhóm tội phạm có tổ chức và 56% các vụ vi phạm phải mất nhiều tháng hoặc lâu hơn mới được phát hiện. Vào thời điểm các lỗi bảo mật được khắc phục, thiệt hại đã được thực hiện.

Theo quan điểm này, các nhà quản lý không còn phải đặt câu hỏi 'liệu mạng của họ có phải là mục tiêu của một cuộc tấn công mạng hay không, mà thay vào đó họ cần xác định "khi nào nó sẽ xảy ra?" "thiệt hại sẽ là bao nhiêu?", "cuộc điều tra sẽ kéo dài bao lâu ?", "chi phí điều tra và tiền phạt sẽ cao đến mức nào?" và quan trọng nhất là "làm cách nào để chúng tôi bảo vệ hệ thống của mình khỏi bị tấn công?"

Diễn đàn bảo mật thông tin (https://www.securityforum.org/), cơ quan hàng đầu về mạng, bảo mật thông tin và quản lý rủi ro bao gồm nhiều công ty trong danh sách Fortune 100, đã biên soạn một danh sách các vấn đề bảo mật thông tin hàng đầu và phát hiện ra rằng chín trong số 10 sự cố hàng đầu có thể được tóm tắt trong ba yếu tố rủi ro:

* Lỗi hoặc lỗi của con người dẫn đến hệ thống, ứng dụng hoặc mạng bị định cấu hình sai

• Hệ thống trục trặc

* Không vá lỗi hoặc bảo trì phần mềm đúng cách trên hệ thống hiện có'

Bước đầu tiên trong sáng kiến an ninh mạng là chọn một chiến lược phòng thủ không gian mạng, sau đó áp dụng các chiến lược giảm thiểu rủi ro dành riêng cho các loại tài sản khác nhau và triển khai các biện pháp bảo mật mạnh mẽ. Đây không chỉ là trách nhiệm của bộ phận CNTT và ban quản lý cấp cao mà còn là nhiệm vụ liên tục của mọi người trong một hệ thống. tổ chức Lĩnh vực an ninh mạng—như thể thao và luật—có thuật ngữ riêng, được tóm tắt để tham khảo nhanh trong bản 5.5 .

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | BẢNG 5.5 | | | |  |
| Thuật ngữ an ninh mạng | | | |
| thuật ngữ định nghĩa | | | |
| Kiểm soát truy cập | | Tính năng bảo mật được thiết kế để hạn chế người có quyền truy cập vào mạng, IS hoặc dữ liệu | |
| Tài sản | | Thứ gì đó có giá trị cần được bảo vệ, chẳng hạn như dữ liệu khách hàng, bí mật thương mại, công thức độc quyền | |
| Kiểm toán | | Quy trình tạo, ghi và xem xét bản ghi thời gian của các sự kiện hệ thống để xác định độ chính xác của chúng | |
| xác thực | | Phương pháp (thường dựa trên tên người dùng và mật khẩu) mà IS xác thực hoặc xác minh rằng người dùng thực sự là người mà họ tuyên bố là | |
| sinh trắc học | | Các phương pháp nhận dạng một người dựa trên đặc điểm sinh học, chẳng hạn như dấu vân tay hoặc võng mạc | |
| Ciphenext | | văn bản được mã hóa | |
| mã hóa | | Chuyển đổi dữ liệu thành mã được mã hóa để bảo vệ chúng khỏi bị hiểu trái phép | |
| Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố. | | | | | | |
|  | | người dùng | |
| Khai thác | | Một chương trình (mã) cho phép kẻ tấn công tự động xâm nhập vào hệ thống thông qua một lỗ hổng | |
| Phơi bày | | Ước tính chi phí, tổn thất hoặc thiệt hại có thể xảy ra nếu mối đe dọa khai thác lỗ hổng | |
| khả năng chịu lỗi | | Khả năng IS tiếp tục hoạt động khi xảy ra lỗi, nhưng thường trong một thời gian giới hạn hoặc ở mức độ giảm | |
| Bức tường lửa | | Phần mềm hoặc thiết bị kiểm soát quyền truy cập vào mạng riêng từ mạng công cộng (Intemet) bằng cách phân tích các gói dữ liệu vào hoặc ra khỏi mạng đó | |
| Bản rõ hoặc văn bản rõ ràng | | văn bản có thể đọc được | |
| Rủi ro | | Xác suất của một mối đe dọa khai thác lỗ hổng và chi phí phát sinh củaAoss, thiệt hại, gián đoạn hoặc rủi ro phá hủy là một chức năng của mối đe dọa, lỗ hổng và chi phí tác động | |

#### Chiến lược phòng thủ mạng

Mục tiêu chính của quản lý bảo mật CNTT là bảo vệ tất cả các thành phần của hệ thống thông tin, cụ thể là dữ liệu, ứng dụng phần mềm, phần cứng và mạng chống lại các cuộc tấn công. Để làm được điều này, một công ty phải thu thập thông tin tình báo chiến lược và chiến thuật để phát triển hệ thống phòng thủ an ninh mạng tùy chỉnh . Trí thông minh chiến lược cho biết CÁCH một tổ chức sẽ tự bảo vệ mình. Điều này bao gồm việc phân tích các lỗ hổng trong quy trình và công cụ an ninh mạng của một tổ chức để đảm bảo họ có thể tự bảo vệ mình một cách đầy đủ trước mối đe dọa mạng hung hăng và giúp tổ chức dễ dàng phát hiện ra các mối đe dọa trước khi chúng xảy ra: Trí thông minh chiến thuật cho biết NHỮNG GÌ tổ chức cần làm khi nó xảy ra bị tấn công. Điều này có thể bao gồm xác định các miền, phần mềm độc hại và địa chỉ IP đe dọa, đồng thời lấy thông tin từ các tổ chức khác đã hứng chịu các cuộc tấn công mạng tương tự.

Trước khi thành lập một nhà máy tùy chỉnh, nhân viên an ninh mạng phải hiểu các yêu cầu và hoạt động của doanh nghiệp. Chiến lược bảo vệ được lựa chọn phụ thuộc vào những gì cần được bảo vệ và chi phí—phân tích lợi ích của tài sản và hậu quả của việc bảo vệ nó. Nghĩa là, các công ty không nên đầu tư quá mức cũng như không đầu tư quá mức. Khi lựa chọn chiến lược phòng thủ mạng, công ty phải ghi nhớ các mục tiêu chính của mình, xem Bảng 5.6 ).

|  |
| --- |
|  |
| Chiến lược phòng thủ mạng |
| Phòng ngừa và răn đe   * Các biện pháp kiểm soát được thiết kế phù hợp có thể ngăn ngừa lỗi xảy ra, ngăn chặn tội phạm tấn công hệ thống và tốt hơn nữa là từ chối quyền truy cập của những người không được phép. Đây là những điều khiển mong muốn nhất.   phát hiện  Cuộc tấn công được phát hiện càng sớm thì càng dễ chiến đấu và càng ít thiệt hại. Việc phát hiện có thể được thực hiện trong nhiều trường hợp bằng cách sử dụng phần mềm chẩn đoán đặc biệt với chi phí tối thiểu.  ngăn chặn   * Giảm thiểu hoặc hạn chế tổn thất khi xảy ra sự cố. Nó còn được gọi là kiểm soát thiệt hại. Điều này có thể được thực hiện, ví dụ, bằng cách bao gồm một hệ thống chịu lỗi cho phép hoạt động ở chế độ xuống cấp cho đến khi phục hồi hoàn toàn. Nếu một hệ thống chịu lỗi không tồn tại, thì việc khôi phục nhanh chóng và có thể tốn kém phải diễn ra. Người dùng muốn hệ thống của họ hoạt động trở lại nhanh nhất có thể. Sự hồi phục * Kế hoạch khôi phục giải thích cách khắc phục hệ thống thông tin bị hỏng nhanh nhất có thể. Thay thế thay vì sửa chữa các thành phần là một cách để phục hồi nhanh chóng     Điều chỉnh     * Việc khắc phục nguyên nhân khiến hệ thống bị hư hỏng có thể ngăn sự cố tái diễn. Nhận thức/Tuân thủ * Tất cả các thành viên của tổ chức phải được nhận thức và giáo dục về các mối nguy hiểm và phải tuân thủ các quy tắc và quy định về an ninh. |
|

##### Quản lý rủi ro

Giá trị của tài sản đối với công ty và tội phạm mạng càng cao thì rủi ro đối với công ty và

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

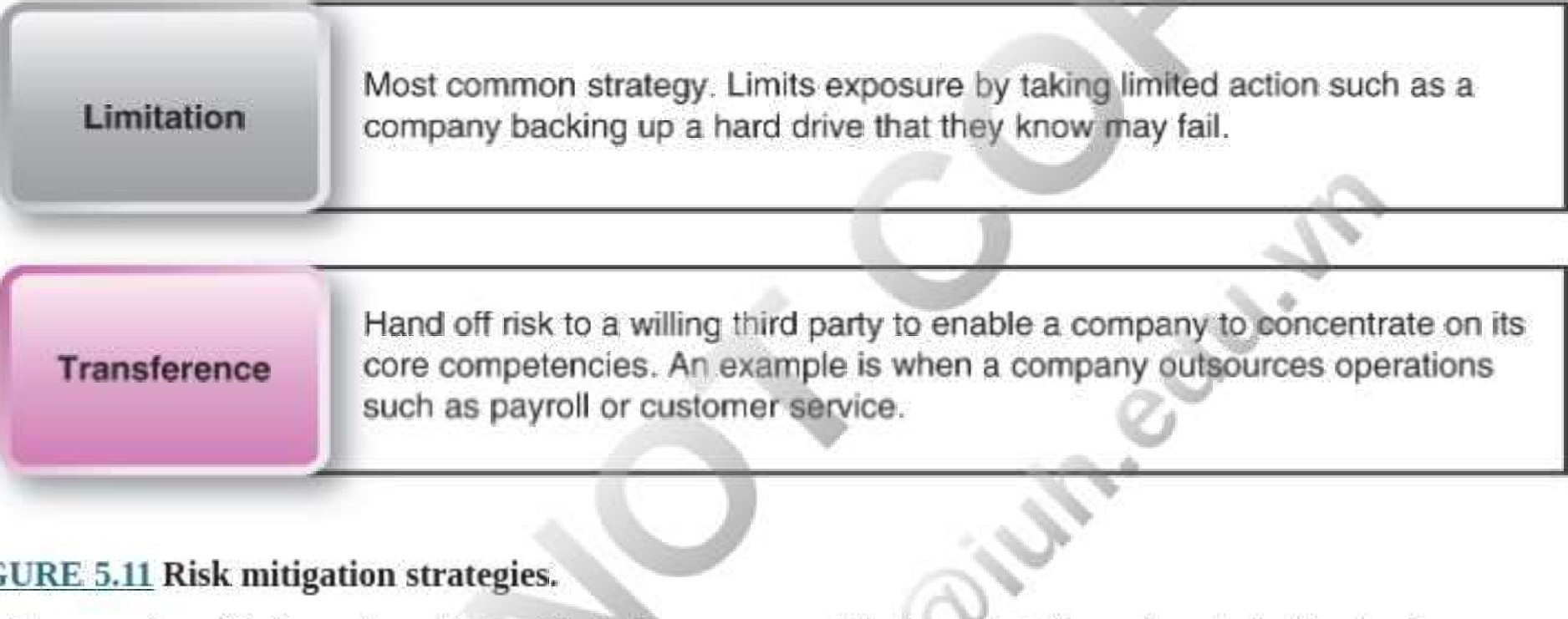
mức độ bảo mật cần phải cao hơn. Để làm được điều này, một công ty có thể sử dụng một trong bốn phương pháp quản lý rủi ro để đánh giá mức độ chấp nhận rủi ro của mình so với các tài nguyên máy tính khác nhau và môi trường của chúng.

Rủi ro là một tình huống liên quan đến việc tiếp xúc với nguy hiểm.

Ví dụ 5.11 xác định và mô tả bốn chiến lược giảm thiểu rủi ro khác nhau áp dụng cho hoạt động kinh doanh liên tục và khắc phục thảm họa. Chúng là sự chấp nhận, tránh né, hạn chế và chuyển giao.

Giảm thiểu rủi ro là hành động được thực hiện để giảm thiểu các mối đe dọa và đảm bảo khả năng phục hồi

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  |  | | --- | --- | |  | Không làm giảm ảnh hưởng bất lợi. Có thể chấp nhận rủi ro không có khả năng xảy ra cao, ví dụ công ty xác định sẽ không xảy ra thiên tai | |
| |  | | --- | | Tránh bất kỳ rủi ro nào. Một ví dụ có thể là chạy các hệ thống song song hoặc bỏ qua các cảnh báo rõ ràng. Cách tiếp cận này có thể rất tốn kém. | |



FIGURE

Không phải tất cả các công ty sẽ chọn giảm thiểu rủi ro theo cùng một cách. Điều quan trọng là mỗi tổ chức phải chọn một hoặc nhiều chiến lược giảm thiểu rủi ro phù hợp nhất với nhu cầu của mình. Cách tiếp cận tốt nhất LÀ chọn chiến lược giảm thiểu rủi ro phù hợp cho phép công ty bảo vệ thành công tài sản quý giá nhất của mình thay vì cố gắng bảo vệ tất cả tài sản theo cùng một cách.

#### Hệ thống bảo mật

An ninh mạng là một quá trình liên tục, không có hồi kết—tương tự như việc sơn Cầu Cổng Vàng ở San Francisco—và không phải là vấn đề có thể dễ dàng giải quyết chỉ bằng phần cứng hoặc phần mềm. Các biện pháp phòng vệ an ninh phần cứng và phần mềm không thể bảo vệ chống lại các hoạt động kinh doanh thiếu trách nhiệm. Việc coi an ninh mạng là ưu tiên hàng đầu đang trở nên quan trọng hơn bao giờ hết khi sự phát triển của công nghệ di động và 10T đe dọa mang đến cho những kẻ tấn công những cơ hội mới.

##### Công cụ phòng thủ mạng

Vì bọn tội phạm mạng sử dụng nhiều phương thức và chiến lược tấn công nên cần có nhiều công cụ để phát hiện chúng và/hoặc vô hiệu hóa tác động của chúng. Bốn công cụ phòng thủ mạng hiệu quả là:

1. Phần mềm chống vi-rút Các công cụ chống phần mềm độc hại được thiết kế để phát hiện các mã độc hại và ngăn người dùng tải chúng xuống. Họ cũng có thể quét các hệ thống để tìm sự hiện diện của sâu, trojan và các loại mối đe dọa khác. Công nghệ này không cung cấp khả năng bảo vệ hoàn toàn vì nó không thể chống lại việc khai thác zero-day.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Phần mềm chống phần mềm độc hại có thể không phát hiện được cách khai thác chưa biết trước đó.

1. Hệ thống phát hiện xâm nhập ( IDS ) Như tên ngụ ý, IDS quét tìm lưu lượng truy cập bất thường hoặc đáng ngờ. IDS có thể xác định giai đoạn tấn công DOS theo mẫu lưu lượng, cảnh báo cho quản trị viên mạng thực hiện hành động phòng thủ, chẳng hạn như chuyển sang địa chỉ IP khác và chuyển hướng các máy chủ quan trọng khỏi đường tấn công.
2. Hệ thống ngăn chặn xâm nhập ( IPS ) Một IPS được thiết kế để thực hiện hành động ngay lập tức—chẳng hạn như chặn các địa chỉ IP cụ thể—bất cứ khi nào phát hiện thấy sự bất thường của luồng lưu lượng. IPS dựa trên mạch tích hợp dành riêng cho ứng dụng (ASIC) có sức mạnh và khả năng phân tích để phát hiện và chặn các cuộc tấn công từ chối dịch vụ ( DDoS ) phân tán , hoạt động giống như một bộ ngắt mạch tự động.
3. Dịch vụ thông minh IP. Khả năng phát hiện và chặn các mối đe dọa trực tuyến trước khi chúng xảy ra là một lợi thế rất lớn trong việc bảo vệ mạng khỏi bị tấn công. Cung cấp dịch vụ thông minh IP1S có thể giúp các tổ chức giảm đáng kể hoạt động mạng độc hạiO giảm đáng kể rủi ro gian lận trực tuyến, giảm thiểu rủi ro tuân thủ giảm thiểu thời gian và công sức xử lý lưu lượng xấu và tăng hiệu quả của trung tâm dữ liệu.

###### Bảo vệ chống tái nhiễm phần mềm độc hại, chữ ký, đột biến và biến thể

Phần mềm độc hại rất khó xóa khỏi máy tính bị nhiễm. Khi máy tính chủ bị nhiễm, các nỗ lực xóa phần mềm độc hại có thể không thành công và phần mềm độc hại có thể lây nhiễm lại máy chủ vì hai lý do:

1. Phần mềm độc hại bị bắt trong các bản sao lưu hoặc kho lưu trữ Khôi phục bản sao lưu bị nhiễm cũng đồng thời khôi phục phần mềm độc hại.
2. Phần mềm độc hại lây nhiễm vào phương tiện lưu động Hàng tháng hoặc nhiều năm sau lần lây nhiễm đầu tiên, phương tiện lưu động có thể bị



được truy cập và có thể cố gắng lây nhiễm máy chủ. r)

Hầu hết các phần mềm chống vi-rút (AV) đều dựa vào bản chất của phần mềm độc hại để xác định và: sau đó chặn phần mềm độc hại. Việc phát hiện và ngăn chặn sự lây nhiễm từ hàng triệu chữ ký phần mềm độc hại hiện có KHÔNG phải lúc nào cũng khả thi. Zero-day y exp loits —phần mềm độc hại mới nên chữ ký của chúng vẫn chưa được biết đến — là một ví dụ. Phần mềm độc hại auth01S cũng trốn tránh sự phát hiện của phần mềm AV và tường lửa bằng cách thay đổi mã phần mềm độc hại để tạo các biến thể có chữ ký mới. Nhưng không phải tất cả các quy trình hoặc công cụ AV đều có thể xóa mọi dấu vết của phần mềm độc hại. Ngay cả khi các phần độc hại của sự lây nhiễm có thể được làm sạch khỏi hệ thống, các đoạn mã còn lại có thể làm cho hệ thống không ổn định hoặc dễ bị lây nhiễm trong tương lai.

Chữ ký phần mềm độc hại là một giá trị duy nhất cho biết sự hiện diện củamalicious.code.

khai thác zero-day là phần mềm độc hại làm lộ lỗ hổng trong phần cứng hoặc phần cứng và có thể tạo ra các sự cố phức tạp trước khi bất kỳ ai phát hiện ra.

CNTT tại nơi làm việc 5.4 mô tả cách một công ty ngăn chặn thành công cuộc tấn công của phần mềm độc hại độc hại cũng như bí mật theo dõi và phân tích cuộc tấn công đó.

CNTT tại nơi làm việc 5.4

##### Bayer ngăn chặn thành công phần mềm độc hại tấn công bởi lính đánh thuê



Nhà sản xuất dược phẩm Bayer của Đức (https://www.bayer.com/) đã ngăn chặn một cuộc tấn công mạng mà họ tin rằng có nguồn gốc từ Trung Quốc. Bayer đã tìm thấy phần mềm độc hại trên mạng máy tính của mình và bí mật theo dõi và phân tích nó trong một năm. Sau một năm tự do thám, Bayer đã loại bỏ mối đe dọa khỏi hệ thống của mình và tiết lộ cuộc tấn công. Bayer xác nhận "một nỗ lực hack đáng kể" đã diễn ra nhưng dường như không có bằng chứng về việc đánh cắp dữ liệu hoặc dữ liệu cá nhân đã bị xâm phạm.



Các tin tặc được cho là một phần của nhóm Wicked Panda có trụ sở tại Trung Quốc, nhưng Gerhard Schindler, cựu giám đốc cơ quan tình báo nước ngoài BIND của Đức cho biết rất khó xác định vị trí của tin tặc. Nhóm này đã cài đặt phần mềm độc hại WINNTI vào các hệ thống của Bayer để theo dõi Bayer, cung cấp bằng chứng rõ ràng rằng phần mềm phức tạp và tinh vi đã được sử dụng trong một nỗ lực gián điệp có mục tiêu và bền vững. Trích dẫn ít nhất bốn cuộc tấn công WINNTI khác ở Đức, Andreas Rohr của DCSO, một nhóm an ninh mạng, cho biết Nhóm Gấu trúc xấu xa là một nhóm tin tặc rất tích cực có thể thực hiện đồng thời nhiều cuộc tấn công quốc tế. Mặc dù không thể nói chắc chắn rằng Gấu trúc xấu xa chịu trách nhiệm cho cuộc tấn công của Bayer, Rohr cho biết phương pháp được sử dụng mang dấu ấn của lính đánh thuê Trung Quốc, những người thực hiện các cuộc tấn công mạng có chủ đích và các chiến dịch kiếm tiền.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Nguồn: Tổng hợp từ Anonymous ( 2019a ), Hashim (2019 ) và Weiss and Burger ( 2012 ).

###### Bảo vệ thiết bị di động

Ở mức tối thiểu, có một số biện pháp bảo vệ an ninh phải được áp dụng cho thiết bị di động, bao gồm sinh trắc học di động, sinh trắc học giọng nói, giám sát ứng dụng lừa đảo, khả năng xóa từ xa và mã hóa.

* Sinh trắc học di động như sinh trắc học giọng nói và dấu vân tay, có thể cải thiện đáng kể tính bảo mật của thiết bị vật lý và cung cấp xác thực mạnh mẽ hơn cho truy cập từ xa hoặc dịch vụ đám mây. Kiểm soát sinh trắc học đã được tích hợp vào các sản phẩm phần cứng và phần mềm kinh doanh điện tử. Kiểm soát sinh trắc học có một số hạn chế: Chúng không chính xác trong một số trường hợp nhất định và một số người coi chúng là xâm phạm quyền riêng tư. Hầu hết các hệ thống sinh trắc học khớp với một số đặc điểm cá nhân dựa trên hồ sơ được lưu trữ.

Kiểm soát sinh trắc học là một phương pháp tự động xác minh danh tính của một người, dựa trên các đặc điểm thể chất hoặc hành vi. Sinh trắc học phổ biến nhất là dấu vân tay hoặc dấu vân tay, giọng nói; quét võng mạc và chữ ký.

* Sinh trắc học giọng nói là một giải pháp xác thực hiệu quả trên nhiều loại thiết bị tiêu dùng bao gồm điện thoại thông minh, máy tính bảng và TV. Các thiết bị di động trong tương lai dự kiến sẽ có cảm biến vân tay để thêm một yếu tố xác thực khác. Khi Apple mua lại Siri, Inc., trợ lý cá nhân dựa trên giọng nói Sfri đã được tích hợp vào hệ điều hành của Apple; Siri đã cho Apple khả năng chuyển sang lĩnh vực sinh trắc học giọng nói.
* Rog ue a pp lication monitorin g được sử dụng để phát hiện và tiêu diệt các ứng dụng độc hại. Một số nhà cung cấp cung cấp dịch vụ giám sát và phát hiện 24/7 để giám sát các cửa hàng ứng dụng lớn và tắt các ứng dụng giả mạo để giảm thiểu khả năng bị lộ và thiệt hại.
* Công tắc tiêu diệt di động hoặc khả năng xóa sạch từ xa cũng như khả năng mã hóa là cần thiết trong trường hợp mất hoặc bị đánh cắp thiết bị . Tất cả các nền tảng điện thoại thông minh chính đều có tùy chọn mã hóa và khả năng xóa từ xa.
* Mã hóa là quá trình tập hợp thông tin hoặc dữ liệu thành mã và là điều cần thiết để ngăn chặn truy cập trái phép vào thông tin nhạy cảm được truyền trực tuyến.



Trong trường hợp nhân viên đi công tác, các Riles do-no-calTY có thể là một biện pháp bảo vệ cần thiết bổ sung. Để đối phó với các mối đe dọa bảo mật trên thiết bị di động, nhiều công ty và cơ quan chính phủ của Hoa Kỳ đang áp đặt các quy tắc không được làm trên điện thoại di động để ngăn chặn sự thỏa hiệp. Khách du lịch chỉ có thể mang theo "các thiết bị rõ ràng và bị cấm kết nối với mạng của chính phủ khi ở nước ngoài.

###### Phát triển quy tắc không mang theo

Phòng Thương mại Hoa Kỳ đã không biết rằng họ và các tổ chức thành viên là nạn nhân của một vụ trộm mạng trong nhiều tháng cho đến khi FBI thông báo cho Phòng rằng các máy chủ ở Trung Quốc đang đánh cắp dữ liệu từ bốn chuyên gia chính sách châu Á của họ, những cá nhân thường xuyên đi du lịch Châu Á. Nhiều khả năng, các thiết bị di động của xperts đã bị nhiễm

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

với phần mềm độc hại đang truyền thông tin và tệp trở lại tin tặc. Vào thời điểm Phòng tăng cường (bảo mật) các mạng của nó, tin tặc đã đánh cắp ít nhất sáu tuần e-mail, hầu hết trong số đó là thông tin liên lạc với các tập đoàn lớn nhất của Hoa Kỳ. Thậm chí sau này, Phòng còn biết được rằng máy in văn phòng và máy điều hòa nhiệt độ tại một trong những căn hộ của công ty đang liên lạc với một địa chỉ Internet ở Trung Quốc. Phòng không tiết lộ cách tin tặc xâm nhập vào hệ thống của họ, nhưng bước đầu tiên là thực hiện các quy tắc không mang theo.

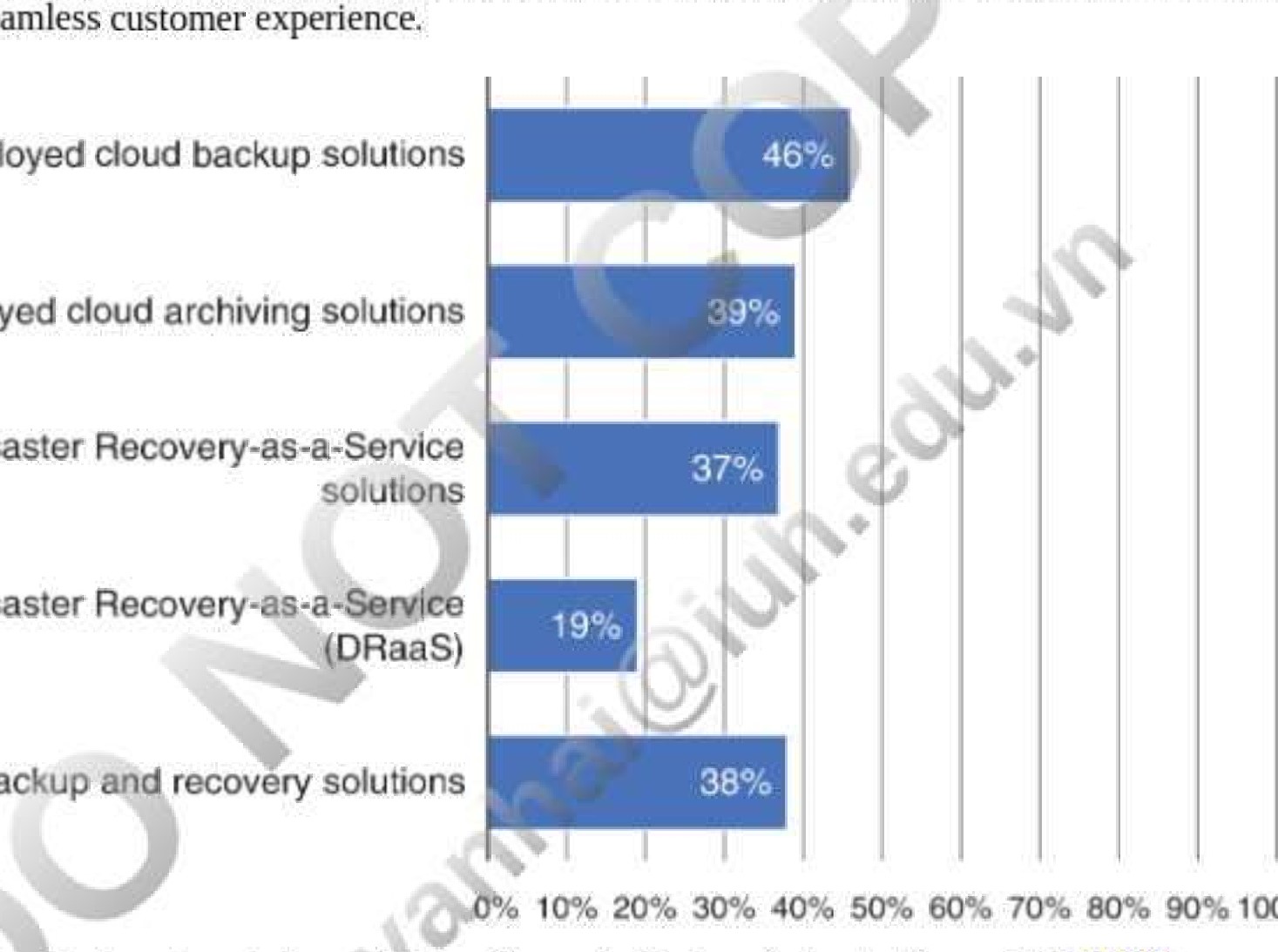
CHÚNG TA. Mike Rogers, chủ tịch hiện tại của Ủy ban Tình báo Hạ viện cho biết các công ty, cơ quan chính phủ và tổ chức hiện đang áp đặt các quy tắc không mang theo người , giả định rằng các thiết bị chắc chắn sẽ bị xâm phạm. Ví dụ: các thành viên Hạ viện chỉ mang theo các thiết bị "sạch" và bị cấm kết nối với mạng của chính phủ khi ở nước ngoài. Rogers cho biết anh đi du lịch "khỏa thân bằng điện tử" để đảm bảo an ninh mạng trong và sau chuyến đi.

###### Trở nên linh hoạt về CNTT

Khả năng phục hồi CNTT liên quan đến việc giảm thiểu rủi ro một cách hiệu quả đối với dữ liệu và ứng dụng dưới mọi hình thức gián đoạn có kế hoạch hoặc không có kế hoạch. Một cuộc khảo sát gần đây do IDC (CIO, 2019 ) thực hiện cho thấy rằng trong khi hầu hết các công ty coi khả năng phục hồi CNTT là điều kiện tiên quyết cần thiết để đạt được chuyển đổi kỹ thuật số thành công, thì 90% trong số họ không coi mình là có khả năng phục hồi CNTT và rất ít doanh nghiệp có các sáng kiến phục hồi CNTT hiện có hoặc đã lên kế hoạch (Ejg theo 5.12) . Nghịch lý về khả năng phục hồi CNTT này phần nào giống với nghịch lý về quyền riêng tư đã thảo luận trước đó trong chương và cũng gây bối rối không kém.

Khả năng phục hồi CNTT là khả năng bảo vệ dữ liệu và ứng dụng khỏi mọi sự gián đoạn có kế hoạch hoặc không có kế hoạch nhằm loại bỏ rủi ro

Kế hoạch triển khai Thảm họa



downtime

to

maintain

a

seamless

Have

deployed

Have

deployed

Have

deployed

Disaster

Plan

to

deploy

new

backup

100%

HÌNH 5.12 Các công ty đã triển khai và lên kế hoạch cho các sáng kiến phục hồi CNTT (điều chỉnh từ CIO, 2019) .

#### Sao lưu và phục hồi

Sao lưu và phục hồi IS và dữ liệu là hoạt động bảo mật cần thiết cho bất kỳ doanh nghiệp nào. Trong hơn hai mươi năm trở lại đây, hệ thống băng từ thường là công nghệ sao lưu, nhưng việc sử dụng nó đòi hỏi sự can thiệp của nhân viên CNTT thường xuyên bị quá tải để nhận ra sự cố, chẩn đoán sự cố, đưa ra giải pháp hiệu quả, thực hiện hành động kịp thời, và đảm bảo các nỗ lực phục hồi thành công. Sự can thiệp thủ công này cần có thời gian và khiến tổ chức gặp rủi ro, Để chống lại các cuộc tấn công mạng trong các công ty phần mềm thời gian thực, như Zerto (www.zerto.com) và Veritas

(www.veritas.com)không cung cấp các bộ ứng dụng và công cụ phục hồi CNTT tự động hành động để bảo vệ dữ liệu và ứng dụng khỏi bất kỳ loại tấn công mạng nào.

Tuy nhiên, trở nên linh hoạt về CNTT không chỉ liên quan đến công nghệ. Nó liên quan nhiều đến con người cũng như về công nghệ. Ngoài việc đảm bảo rằng công nghệ phù hợp được áp dụng, tổ chức cần những người hiểu rõ vai trò của họ

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

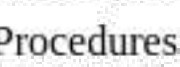
đồng thời làm rõ các chính sách và thủ tục để hướng dẫn họ cách ứng phó với sự gián đoạn hoặc thảm họa nhằm đưa tổ chức hoạt động trở lại nhanh nhất có thể. Một chiến lược phục hồi CNTT hiệu quả nên bao gồm bốn yếu tố:

* Tính khả dụng—giúp khách hàng luôn kết nối với dữ liệu và ứng dụng của họ.
* Tính di động—có thể di chuyển các ứng dụng và khối lượng công việc trong khi vẫn bảo vệ chúng hoàn toàn.

• Linh hoạt—duy trì quyền tự do lựa chọn đám mây của riêng bạn và có thể di chuyển đến, từ và giữa các đám mây.

* Đào tạo—Nhân viên CNTT và không phải CNTT phải hiểu vai trò của họ trong trường hợp xảy ra gián đoạn hoặc thảm họa và được đào tạo về cách ứng phó.

Việc đo lường khả năng phục hồi của CNTT có thể khó khăn, nhưng đó là điều mà hầu hết các công ty đều muốn đạt được và ngày càng trở nên quan trọng trước các báo cáo gần như hàng ngày về các cuộc tấn công mạng có thể gây ra hậu quả tàn khốc đối với những người không chuẩn bị sẵn sàng để ứng phó hiệu quả với chúng .

Chính sách và khả năng phục hồi CNTT và khắc phục thảm họa.

Chính sách kinh doanh, quy trình và kế hoạch khắc phục thảm họa xung quanh tài nguyên máy tính là rất quan trọng đối với khả năng phục hồi CNTT và an ninh mạng. Ví dụ: các sự cố nội bộ có thể được giảm thiểu bằng chiến lược phòng thủ chuyên sâu theo lớp bao gồm các quy trình bảo mật, chính sách sử dụng bảng ace p (Al-JP) và kiểm soát công nghệ. Tại Hoa Kỳ, giám đốc Cục Bảo vệ Người tiêu dùng tại Ủy ban Thương mại Liên bang (FTC) tuyên bố rằng cơ quan này sẽ thực hiện hành động cưỡng chế đối với bất kỳ doanh nghiệp nhỏ nào thiếu các chính sách và thủ tục đầy đủ để bảo vệ dữ liệu của người tiêu dùng. Bảng 5.7 liệt kê các đặc điểm của một chương trình an ninh mạng hiệu quả.

Chính sách sử dụng được chấp nhận là một tài liệu liệt kê các ràng buộc và thông lệ mà người dùng phải đồng ý để truy cập vào mạng công ty hoặc Internet.

|  |
| --- |
|  |
| Đặc điểm của một chương trình an ninh mạng hiệu quả |
| Cung cấp dữ liệu và tài liệu và có thể truy cập 24/7 đồng thời hạn chế quyền truy cập: |
| Triển khai và thực thi các quy trình và AUP đối với dữ liệu, mạng, phần cứng và phần mềm thuộc sở hữu của công ty hoặc nhân viên, như đã thảo luận trong trường hợp mở đầu. |
| Thúc đẩy chia sẻ thông tin an toàn và hợp pháp giữa những người và đối tác được ủy quyền. |
| Đảm bảo tuân thủ các quy định của chính phủ và pháp luật. |
| Ngăn chặn các cuộc tấn công bằng cách có hệ thống phòng thủ trong mạng. |
| Phát hiện, chẩn đoán và ứng phó với các sự cố và cuộc tấn công trong thời gian thực. |
| Duy trì kiểm soát nội bộ để ngăn chặn việc thay đổi trái phép hồ sơ dữ liệu. |
| Phục hồi sau thảm họa và gián đoạn kinh doanh một cách nhanh chóng. |

#### kế hoạch kinh doanh liên tục

Quản lý rủi ro sẽ không hoàn chỉnh nếu không có y\_p lan tiếp tục kinh doanh đã được thử nghiệm để xác minh rằng nó hoạt động. Tính liên tục trong kinh doanh đề cập đến việc duy trì các chức năng kinh doanh hoặc khôi phục chúng một cách nhanh chóng khi có sự gián đoạn lớn. Kế hoạch bao gồm các quy trình kinh doanh, tập hợp, nguồn nhân lực, đối tác kinh doanh, v.v. Hỏa hoạn, động đất, lũ lụt, mất điện, tấn công độc hại và các loại thảm họa khác tấn công trung tâm dữ liệu. Tuy nhiên, khả năng lập kế hoạch kinh doanh liên tục có thể khó bán vì chúng không đóng góp vào điểm mấu chốt—nghĩa là, cho đến khi quá muộn. So sánh chúng với một hợp đồng bảo hiểm; Nếu và chỉ khi thảm họa xảy ra, số tiền đó đã được chi tiêu hợp lý. Và việc chi tiêu cho việc chuẩn bị cho hoạt động kinh doanh liên tục là một quá trình liên tục vì luôn có nhiều việc có thể được thực hiện để chuẩn bị tốt hơn'

Mục đích của kế hoạch kinh doanh liên tục là để duy trì hoạt động kinh doanh sau khi thảm họa xảy ra. Mỗi chức năng trong doanh nghiệp nên có một kế hoạch dự phòng khả thi. Ví dụ: nếu trung tâm dịch vụ khách hàng hoặc tổng đài bị bão phá hủy hoặc mất toàn bộ điện, liệu có ai biết các đại diện sẽ tiếp tục trả lời các cuộc gọi của khách hàng như thế nào không? Kế hoạch dự phòng có thể xác định cách cung cấp quyền truy cập mạng cần thiết để cho phép doanh nghiệp tiếp tục hoạt động. Thỉnh thoảng, điều quan trọng là phải xem xét lại kế hoạch kinh doanh liên tục và thực hiện các điều chỉnh phản ánh tình trạng hiện tại của

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

kinh doanh và môi trường của nó.

Để bổ sung và củng cố kế hoạch kinh doanh liên tục, các chiến lược sau đây có thể được áp dụng để giúp giảm tác động của thảm họa hoặc sự gián đoạn

* Chỉ đạo từng nhân viên thực hiện sao lưu thường xuyên các tệp của họ bên ngoài trang web để có thể truy cập từ xa bằng tên người dùng và mật khẩu an toàn

• Triển khai Giải pháp Email liên tục dựa trên đám mây, như Securence (https://www.securence.com/solution/emailcontinuity-solution/), để cung cấp khả năng truy cập email không bị gián đoạn.

* Đảm bảo rằng bạn có khả năng tương thích phần mềm trên nhiều thiết bị để hoạt động kinh doanh có thể tiếp tục trên thiết bị di động của nhân viên.

• Hợp nhất thông tin liên lạc trên một máy chủ đám mây an toàn bên ngoài cơ sở sẽ tiếp tục hoạt động trong trường hợp mất điện, thiên tai hoặc các gián đoạn khác,

* Thiết lập thỏa thuận cấp độ dịch vụ với nhà cung cấp của bạn để cung cấp hỗ trợ nhanh, sao lưu khẩn cấp và định tuyến đến các máy chủ thay thế khi cần thiết.
* Đưa ra các quy trình để đảm bảo rằng các nhóm CNTT có thể hành động nhanh chóng mà không cần phê duyệt trong trường hợp xảy ra thảm họa hoặc gián đoạn.

Đảm bảo đủ tài nguyên được phân bổ trong ngân sách CNTT cho các dịch vụ khắc phục thảm họa và liên tục kinh doanh đầy đủ

#### Dịch vụ khắc phục thảm họa

Một cách hiệu quả khác để khôi phục các hoạt động bình thường của máy tính và mạng bị gián đoạn do thiên tai hoặc thảm họa khác như bão, động đất hoặc vụ nổ là thiết lập một không gian khôi phục thảm họa an toàn, bên ngoài. Các địa điểm có thể cố định hoặc di động, chẳng hạn như một xe moóc được trang bị sẵn có thể được thiết lập trong khu vực xảy ra thảm họa.

Để đảm bảo tính liên tục trong kinh doanh, một tổ chức có thể xây dựng và vận hành địa điểm khôi phục nội bộ của riêng mình hoặc thuê địa điểm bên ngoài từ bên thứ ba. Nếu một tổ chức không có kinh phí hoặc nguồn lực để xây dựng địa điểm khắc phục thảm họa của riêng mình, thì việc duy trì hợp đồng với dịch vụ khắc phục thảm họa thương mại là một cách hiệu quả để bảo vệ trước những gián đoạn kinh doanh lớn. Ví dụ: nếu một trung tâm dữ liệu không thể hoạt động, một công ty có thể nhanh chóng và dễ dàng di chuyển các hoạt động xử lý dữ liệu của mình sang một trong ba loại trang web thảm họa và tiếp tục hoạt động bình thường . Ba loại trang web là: 

Một trang web nóng có tất cả các thiết bị cần thiết bao gồm không gian văn phòng, nội thất, khả năng liên lạc và thiết bị máy tính. Nó cũng bao gồm nhân sự để quản lý và giám sát thiết bị. Do đó, một trang web nóng hoàn toàn



chức năng và cho phép khôi phục ngay lập tức sau thảm họa. Nó cũng là đắt nhất.

Một trang web ấm áp cung cấp một trung tâm dữ liệu vật lý được trang bị đầy đủ, nhưng nó không có dữ liệu khách hàng. Trang web wam là một tùy chọn ít tốn kém hơn so với trang web nóng và thường được sử dụng khi các trung tâm dữ liệu chính bị tấn công. Sau sự cố gián đoạn tại trung tâm dữ liệu chính, một tổ chức giới thiệu dữ liệu khách hàng của chính mình để khôi phục hoạt động kinh doanh bình thường. Trang web ấm áp mất nhiều thời gian hơn để triển khai hơn trang web nóng, nhưng ít thời gian hơn trang web lạnh.

Một địa điểm lạnh cung cấp không gian văn phòng nhưng yêu cầu' khách hàng cung cấp và lắp đặt các thiết bị cần thiết để tiếp tục hoạt động. Đây là lựa chọn ít tốn kém nhất, nhưng phải mất nhiều thời gian hơn để đưa một tổ chức trở lại hoạt động bình thường. Một trang web lạnh là một lựa chọn tốt khi thời gian phục hồi không quan trọng.

Ngoài ra, đối với phí dịch vụ hàng tháng được thiết lập theo hợp đồng hàng năm, phí hàng ngày và các khoản phí phát sinh khác cũng được tính cho việc sử dụng tất cả các trang web. Một số công ty này cũng cung cấp dịch vụ sao lưu dữ liệu có hoặc không có hợp đồng trang web nóng, ấm hoặc lạnh.

Cho dù một tổ chức sử dụng một địa điểm khắc phục thảm họa bên trong hay bên ngoài thì điều quan trọng là nó phải ở một khoảng cách đủ xa so với các hoạt động chính của tổ chức để nó không bị ảnh hưởng bởi cùng một thảm họa. Điều cần thiết là nó không nằm trên cùng một lưới điện.

#### câu hỏi

1. Giải thích lý do tại sao việc ưu tiên quản lý rủi ro mạng trở nên quan trọng hơn đối với các tổ chức?

2. Kể tên ba công cụ bảo vệ CNTT.

3. Mục đích của giám sát ứng dụng lừa đảo là gì?

4, Tại sao công tắc tiêu diệt di động hoặc khả năng xóa từ xa lại là một phần quan trọng trong việc quản lý rủi ro mạng?

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

5, Tại sao tổ chức cần phải có kế hoạch kinh doanh liên tục?

6. Kể tên ba biện pháp bảo vệ an ninh mạng thiết yếu.

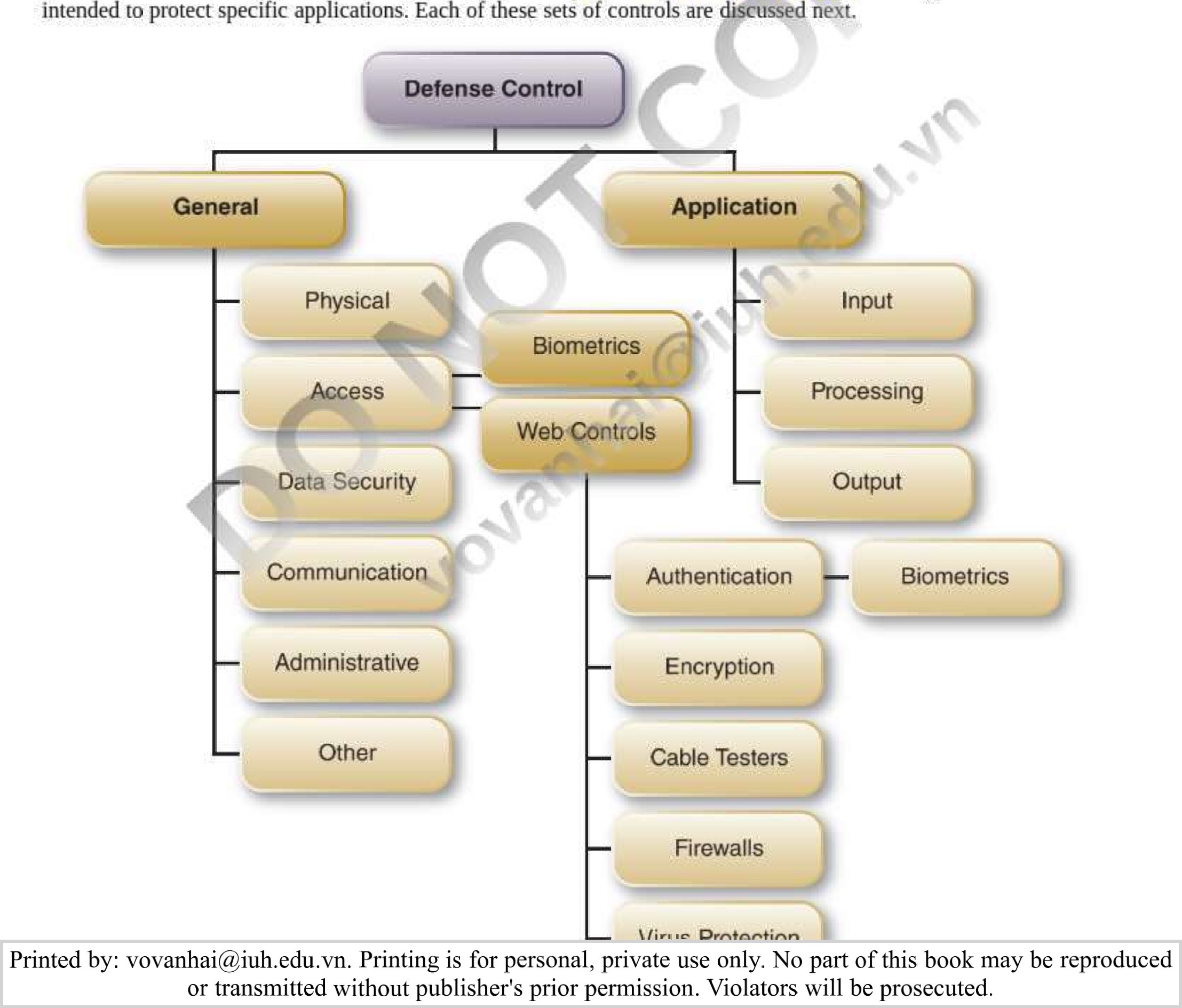
7. Sự khác biệt giữa các điểm nóng, ấm và lạnh là gì?

8. Khi nào và tại sao các công ty áp đặt các Quy tắc không được thực hiện?



#### 5.5 Các biện pháp kiểm soát, khuôn khổ và mô hình theo quy định

|  |
| --- |
| L05.5 Xác định năm biện pháp kiểm soát phòng thủ chung chính, tám biện pháp kiểm soát phòng thủ ứng dụng chính cũng như các quy định và khuôn khổ an ninh mạng giúp bảo vệ người tiêu dùng và hướng dẫn quản trị CNTT. |

Để duy trì một môi trường máy tính an toàn, điều quan trọng là các tổ chức phải thiết lập một bộ kiểm soát bảo mật dành riêng cho tài nguyên và môi trường của nó. Ví dụ 5.13 minh họa ba loại kiểm soát phòng thủ mạng chính được sử dụng để hướng dẫn thực hiện chiến lược phòng thủ mạng. Kiểm soát phòng thủ chung được thiết lập để bảo vệ hệ thống bất kể ứng dụng cụ thể. Ví dụ: bảo vệ phần cứng và truy cập thông tin liên lạc vào trung tâm dữ liệu độc lập với ứng dụng cụ thể. Kiểm soát bảo vệ cấp phép ứng dụng là các biện pháp bảo vệ nhằm bảo vệ các ứng dụng cụ thể. Mỗi bộ điều khiển này sẽ được thảo luận tiếp theo.

Chống vi-rút J



HÌNH 5.13 Các biện pháp kiểm soát phòng thủ không gian mạng chính.

##### Kiểm soát quốc phòng chung

Năm loại kiểm soát phòng thủ chung chính là kiểm soát vật lý, kiểm soát truy cập, kiểm soát bảo mật dữ liệu, kiểm soát truyền thông và kiểm soát hành chính.

Kiểm soát vật lý bảo vệ các cơ sở và tài nguyên máy tính vật lý. Điều này bao gồm bảo vệ máy tính, trung tâm dữ liệu, phần mềm, hướng dẫn sử dụng và mạng. Chúng cung cấp sự bảo vệ chống lại hầu hết các mối nguy hiểm tự nhiên cũng như chống lại một số mối nguy hiểm của con người. An ninh vật lý phù hợp có thể bao gồm một số biện pháp kiểm soát vật lý như:

• Thiết kế trung tâm dữ liệu phù hợp. Ví dụ, trung tâm dữ liệu phải không cháy và không thấm nước.

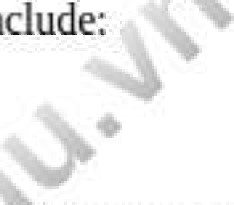
* Lá chắn chống lại các trường điện từ.

được thiết kế tốt , bao gồm hệ thống phun nước, máy bơm nước và các phương tiện thoát nước phù hợp.

• Ngắt điện khẩn cấp và pin dự phòng, phải được duy trì trong tình trạng hoạt động.

* Hệ thống điều hòa không khí được thiết kế và bảo trì đúng cách.
* Báo động phát hiện chuyển động phát hiện sự xâm nhập vật lý.

• Phù hiệu cho người được ủy quyền.

Kiểm soát truy cập là tuyến phòng thủ chính chống lại những người bên trong cũng như bên ngoài trái phép. Đó là một kỹ thuật bảo mật cho phép ai được phép sử dụng tài nguyên máy tính của một tổ chức. Một ví dụ về điều khiển truy cập là danh sách truy cập chỉ định ai có thể truy cập mạng, cơ sở dữ liệu, tệp hoặc dữ liệu. Quyền truy cập bị hạn chế đạt được thông qua quy trình hai bước gồm (l) xác thực người dùng để xác định những người dùng khác nhau trên mạng và (2) ủy quyền người dùng cấp hoặc từ chối các quyền truy cập cụ thể. Các phương thức xác thực bao gồm:

* Thứ gì đó chỉ người dùng biết, chẳng hạn như mật khẩu 
* Thứ gì đó chỉ người dùng mới có, chẳng hạn như thẻ thông minh hoặc mã thông báo

Thứ gì đó chỉ có người dùng, chẳng hạn như chữ ký, giọng nói, dấu vân tay hoặc quét võng mạc (mắt); được thực hiện thông qua kiểm soát sinh trắc học, có thể là vật lý hoặc hành vi

Phương pháp ủy quyền có thể tùy ý, bắt buộc hoặc dựa trên vai trò.



Cần có các biện pháp kiểm soát bảo mật dữ liệu để bảo vệ d'Åta nhạy cảm trong suốt năm giai đoạn trong vòng đời của nó từ khi tạo đến khi hủy bỏ. Khi tạo, dữ liệu phải được phân loại dựa trên mức độ quan trọng và nhạy cảm của nó và chủ sở hữu dữ liệu phải được chỉ định. Trong quá trình phân phối, "dữ liệu đang chuyển động" rất dễ bị xâm phạm và các biện pháp bảo vệ thích hợp như mã hóa hoặc công nghệ ngăn ngừa mất dữ liệu cần được sử dụng để ngăn chặn việc vô tình hoặc cố ý phân phối trái phép dữ liệu nhạy cảm. Trong quá trình sử dụng, dữ liệu phải được kiểm soát\*ó để dữ liệu chỉ có thể được truy cập trên các hệ thống được phân loại bởi những người dùng được ủy quyền có quyền thích hợp. Khi dữ liệu được lưu trữ hoặc "ở trạng thái nghỉ ngơi", các biện pháp kiểm soát thích hợp phải được triển khai và kiểm tra thường xuyên để đảm bảo rằng tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu được đảm bảo trong quá trình lưu trữ và dữ liệu được sao lưu một cách thích hợp và thường xuyên. Trong quá trình xử lý—giai đoạn cuối cùng của vòng đời dữ liệu—các biện pháp kiểm soát cần chỉ định cách dữ liệu sẽ được hủy đúng cách theo các chính sách lưu giữ và xử lý của công ty và theo quy định. Nếu không có các biện pháp kiểm soát bảo mật dữ liệu phù hợp, các tổ chức sẽ dễ bị kiện và bị phạt về quyền riêng tư dữ liệu theo quy định.

Kiểm soát truyền thông hạn chế quyền truy cập vào các thiết bị trên mạng đối với các thiết bị đầu cuối tuân thủ chính sách bảo mật của tổ chức và bảo mật luồng dữ liệu trên các mạng. Các biện pháp kiểm soát mạng truyền thông điển hình bao gồm tường lửa, hệ thống chống phần mềm độc hại, mã hóa và mạng riêng ảo.

Các biện pháp kiểm soát hành chính liên quan đến việc ban hành các nguyên tắc và giám sát việc tuân thủ các nguyên tắc bảo mật của tổ chức. Ví dụ về hành chính là:

* Lựa chọn, đào tạo và giám sát nhân viên một cách phù hợp, đặc biệt là trong hệ thống thông tin và kế toán

• Thúc đẩy lòng trung thành của công ty

* Ngay lập tức thu hồi đặc quyền truy cập của nhân viên bị sa thải, thôi việc hoặc thuyên chuyển
* sửa đổi các điều khiển truy cập, chẳng hạn như Dasswords

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.



* Phát triển các tiêu chuẩn lập trình và tài liệu để giúp việc kiểm tra dễ dàng hơn và sử dụng các tiêu chuẩn làm hướng dẫn cho nhân viên
* Nhấn mạnh vào trái phiếu bảo đảm hoặc bảo hiểm sơ suất cho nhân viên chủ chốt

• Phân chia nhiệm vụ, cụ thể là phân chia các nhiệm vụ máy tính nhạy cảm cho càng nhiều nhân viên càng tốt về mặt kinh tế để giảm nguy cơ thiệt hại cố ý hoặc không chủ ý • Thực hiện kiểm tra ngẫu nhiên định kỳ hệ thống

##### Kiểm soát bảo vệ ứng dụng

Kiểm soát bảo vệ ứng dụng là một biện pháp bảo mật chặn hoặc hạn chế các ứng dụng chưa được xác thực thực thi theo cách gây rủi ro cho dữ liệu. Kiểm soát này đảm bảo quyền riêng tư và bảo mật của dữ liệu được nhập, xử lý và truyền giữa các ứng dụng và hạn chế việc sử dụng đối với người dùng được ủy quyền . Kiểm soát ứng dụng bao gồm:

• Kiểm tra tính đầy đủ để đảm bảo quá trình xử lý IQcords từ đầu đến cuối

* Kiểm tra tính hợp lệ để đảm bảo chỉ dữ liệu hợp lệ được nhập hoặc xử lý
* Xác thực để xác định người dùng
* Ủy quyền để đảm bảo quyền thích hợp

Kiểm soát đầu vào để đảm bảo tính toàn vẹn dữ liệu của tất cả dữ liệu đã nhập

Tính khả dụng để đảm bảo rằng ứng dụng có sẵn khi cần

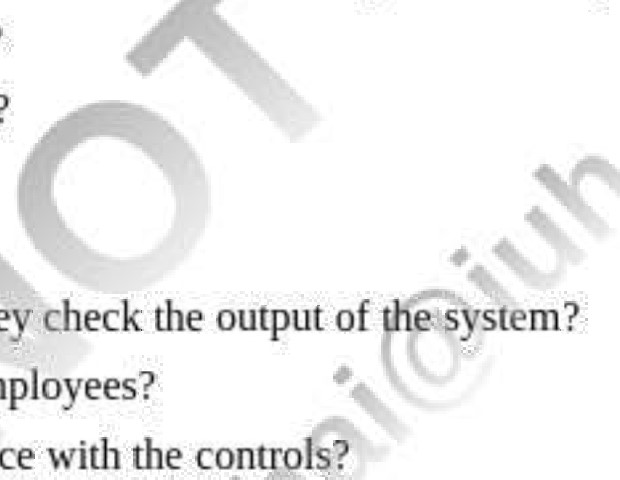
* Lập danh sách trắng để ghi lại các ứng dụng phù hợp

• Lập danh sách đen để chặn các ứng dụng không phù hợp

###### Hệ thống thông tin kiểm toán

Kiểm toán là một hình thức kiểm soát khác. Một số công ty dựa vào kiểm toán bất ngờ. Nhưng việc chủ động tìm kiếm các vấn đề sẽ hiệu quả hơn và có thể ngừng sử dụng được phép sớm trước khi tổn thất gia tăng. Kiểm toán là một phần quan trọng của bất kỳ hệ thống kiểm soát nào. Kiểm toán có thể được xem như một lớp kiểm soát hoặc biện pháp bảo vệ bổ sung. Nó được coi là một biện pháp ngăn chặn các hành động tội phạm, đặc biệt là đối với những người trong cuộc, Kiểm toán viên cố gắng trả lời các câu hỏi như sau:

Có đủ điều khiển trong hệ thống không?

Những khu vực nào không được kiểm soát?

Kiểm soát nào là không cần thiết?

* Các biện pháp kiểm soát có được thực hiện hợp lý không

Các biện pháp kiểm soát có hiệu quả không? Đó làVdo họ kiểm tra đầu ra của

* Có sự phân chia rõ ràng về nhiệm vụ của nhân viên không?

Có các thủ tục để đảm bảo tuân thủ các biện pháp kiểm soát không?

Có các thủ tục tò mò để đảm bảo báo cáo và hành động đối phó trong trường hợp vi phạm các biện pháp kiểm soát không?

Kiểm tra một trang web là một biện pháp phòng ngừa tốt để quản lý rủi ro pháp lý Rủi ro pháp lý rất quan trọng trong bất kỳ hệ thống CNTT nào, nhưng trong các hệ thống Web, điều này thậm chí còn quan trọng hơn do nội dung của trang web có thể xúc phạm mọi người hoặc vi phạm luật bản quyền hoặc các quy định khác L@g., bảo vệ quyền riêng tư). Kiểm toán thương mại điện tử cũng phức tạp hơn vì ngoài trang web, người ta cần kiểm tra việc nhận đơn đặt hàng, thực hiện đơn hàng và tất cả các hệ thống hỗ trợ. Hiệp hội kiểm toán và kiểm soát hệ thống thông tin (www.isaca.org) cung cấp lộ trình kiểm toán chi tiết để kiểm toán viên tuân theo.

###### Quy định của chính phủ

Khi các mối đe dọa mạng tiếp tục phát triển và đạt được động lực trong các ngành công nghiệp khác, ngày càng có nhiều dự luật pháp lý được đề xuất. Ở cấp liên bang, tại Hoa Kỳ, nhiều quy định về quyền riêng tư đã thảo luận trước đây trong chương này (xem Ví dụ 5.2 ), có một thành phần an ninh mạng. Những vấn đề khác tập trung cụ thể hơn vào các mối quan tâm về an ninh mạng bao gồm Đạo luật bảo mật thông tin liên bang\_Uana gernent ( FISMA ) yêu cầu các cơ quan liên bang phát triển, lập tài liệu và triển khai chương trình bảo vệ và bảo mật thông tin. Nhiều bang cũng đang ưu tiên cao hơn các biện pháp an ninh mạng. Hội nghị toàn quốc của các cơ quan lập pháp bang đã báo cáo rằng trong

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Kể từ năm 2019, ít nhất 43 tiểu bang của Hoa Kỳ đã đưa ra các dự luật xử lý đáng kể vấn đề an ninh mạng. Trong số này, 31 bang đã ban hành luật an ninh mạng. Các lĩnh vực chính được quy định trong luật mới yêu cầu các cơ quan chính phủ và/hoặc doanh nghiệp phải:

Thực hiện đào tạo hoặc các loại chính sách và thực hành bảo mật cụ thể. Thành lập các lực lượng đặc nhiệm và ủy ban an ninh mạng.

* Tái cấu trúc chính phủ để cải thiện an ninh.
* Cung cấp sự an toàn của các tiện ích và cơ sở hạ tầng quan trọng,

Nghiên cứu việc sử dụng blockchain cho an ninh mạng.

* Giải quyết vấn đề bảo mật của các thiết bị được kết nối.

Giải quyết các mối đe dọa an ninh mạng đối với các cuộc bầu cử.

* Cung cấp kinh phí cho các biện pháp an ninh được cải thiện.

Đạo luật quản lý bảo mật thông tin liên bang (FISMA)

Để đảm bảo tuân thủ các quy định tại Hoa Kỳ, Ủy ban Giao dịch Chứng khoán (SEC) và FTC đã khuyến cáo rằng họ sẽ áp dụng các khoản tiền phạt rất lớn đối với các vi phạm dữ liệu để ngăn chặn các công ty đầu tư vào bảo vệ dữ liệu. các quy định về an ninh mạng sẽ cần phải đánh giá các khả năng và lỗ hổng bảo mật mạng hiện tại của họ, đồng thời xác định cách triển khai các biện pháp kiểm soát bảo mật như mã hóa, xác thực, ủy quyền và khắc phục thảm họa.

###### Khung quản lý rủi ro và quản trị CNTT

Hai khuôn khổ được chấp nhận rộng rãi để hướng dẫn quản lý rủi ro và quản lý CNTT là Rủi ro gia tăng

Mục tiêu khung và kiểm soát đối với Khung thông tin và công nghệ liên quan ( COBIT 2019 ).

Khung quản lý rủi ro doanh nghiệp ERM là một cách tiếp cận dựa trên rủi ro để quản lý doanh nghiệp do Ủy ban các tổ chức bảo trợ của Ủy ban Treadway (COSO) phát triển. 4 ERM bao gồm tám thành phần, được liệt kê trong Bảng 5.8 .

|  |  |
| --- | --- |
|  | |
| Các thành phần khung quản lý rủi ro doanh nghiệp | |
| Thành phần | Sự miêu tả |
| Môi trường bên trong | Đánh giá triết lý và văn hóa quản lý rủi ro |
| Thiết lập mục tiêu | Xác định mối quan hệ của rủi ro với các mục tiêu của tổ chức |
| nhận dạng sự kiện | Phân biệt rủi ro và cơ hội; tác động tiêu cực/tích cực |
| Đánh giá rủi ro | Đánh giá xác suất rủi ro và tác động |
| phản ứng rủi ro | Xác định và đánh giá các phản ứng rủi ro |
| Hoạt động kiểm soát | Xây dựng các chính sách và thủ tục để đảm bảo thực hiện các biện pháp ứng phó rủi ro |
| Thông tin và giao tiếp | Xác định, nắm bắt và truyền đạt thông tin |
| Giám sát | Tiến hành đánh giá liên tục và riêng biệt các hoạt động liên quan đến rủi ro |

Tám thành phần này có thể được xem xét từ góc độ chiến lược, hoạt động, báo cáo và tuân thủ ở tất cả các cấp của tổ chức. Với quan điểm rủi ro theo danh mục đầu tư, ban quản lý phải xem xét các rủi ro riêng lẻ có mối liên hệ với nhau như thế nào và áp dụng một hệ thống kiểm soát nội bộ mạnh mẽ để đảm bảo quản lý rủi ro doanh nghiệp hiệu quả. Những người tham gia vào ERM bao gồm quản lý, Hội đồng quản trị, Cán bộ quản lý rủi ro và kiểm toán viên nội bộ. ERM được dự định là một phần của quy trình lập kế hoạch thông thường hơn là một sáng kiến riêng biệt. Nơi lý tưởng để bắt đầu là có sự ủng hộ và cam kết từ hội đồng quản trị và lãnh đạo cấp cao.

Khung COBIT 2019. COBIT 2019 là một khung quản trị được công nhận trên toàn cầu, tích hợp bảo mật, quản lý rủi ro và quản trị CNTT được phát triển bởi ISACA—Hiệp hội Kiểm toán và Kiểm soát Hệ thống Quốc tế

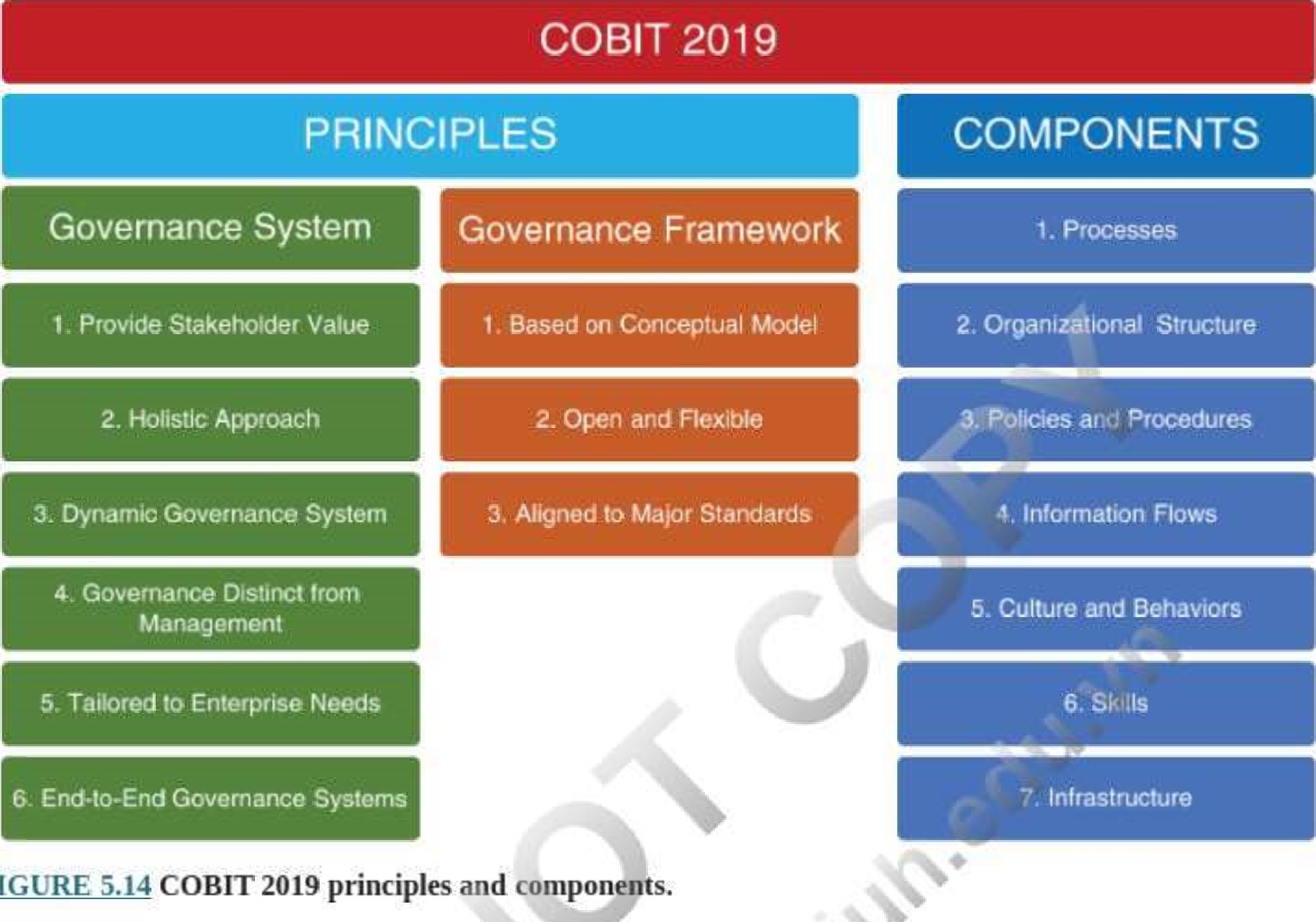
|  |  |
| --- | --- |
|  | www.isaca.org) @ Nó đề cập đến xu hướng thử nghiệm , công nghệ , và nhu cầu bảo mật của các tổ chức tổ chức và kết nối CNTT với  Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố. |
|  |

anu uccu» mục tiêu kinh doanh, để mang lại giá trị và quản lý rủi ro liên quan. Mục đích của nó là cho phép quản lý, người dùng và kiểm tra IS, kiểm soát và thực hành bảo mật1S để thu hẹp khoảng cách giữa các yêu cầu kiểm soát, vấn đề kỹ thuật và rủi ro kinh doanh .



latc»t.

Khung COBIT 2019 có 40 mục tiêu quản trị và quản lý để thiết lập chương trình quản trị CNTT và dựa trên mô hình khái niệm về sáu hệ thống quản trị và ba nguyên tắc khung quản trị và bảy thành phần cần thiết để xây dựng và duy trì chương trình quản trị. Nó mở và linh hoạt và phù hợp với các tiêu chuẩn chính khác. Chín nguyên tắc và bảy thành phần của COBIT 2019 được minh họa trong Hình 5.14 .



FIGURE

COBIT 2019 cũng bao gồm các lĩnh vực trọng tâm và các yếu tố thiết kế cho phép tổ chức mang lại cho tổ chức sự linh hoạt cao hơn để điều chỉnh hệ thống quản trị CNTT theo nhu cầu riêng của mình. Nó cũng bổ sung nhiều tính năng mới và lợi ích cho người dùng như tài nguyên triển khai, hướng dẫn và hiểu biết thực tế cũng như cơ hội đào tạo toàn diện.

Các nguyên tắc COBIT 2019 áp dụng nhiều nhất cho an ninh mạng:

1. Cần phải có một hệ thống xem xét và đáp ứng hiệu quả các yêu cầu bảo mật thông tin doanh nghiệp . Ở mức tối thiểu, điều này sẽ bao gồm các số liệu về số lượng vai trò bảo mật chính được xác định rõ ràng và số lượng sự cố liên quan đến bảo mật được báo cáo.
2. Một kế hoạch bảo mật đã thiết lập đã được chấp nhận và truyền đạt trong toàn tổ chức, Điều này sẽ bao gồm mức độ hài lòng của các bên liên quan với'kế hoạch bảo mật, số lượng giải pháp bảo mật khác với các giải pháp trong kế hoạch và số lượng giải pháp bảo mật khác với kiến trúc bảo mật doanh nghiệp mà có thể dẫn đến lỗ hổng bảo mật và có khả năng kéo dài thời gian giải quyết các vấn đề về bảo mật hoặc tuân thủ.
3. Các giải pháp bảo mật thông tin được triển khai trong toàn tổ chức. Chúng nên bao gồm số lượng dịch vụ và giải pháp phù hợp với kế hoạch bảo mật và các sự cố bảo mật do không tuân thủ kế hoạch bảo mật gây ra.

Bằng cách tuân theo ba nguyên tắc này, sử dụng một bộ quy trình hỗ trợ CNTT được chỉ định và thực hiện các bước bổ sung để chuyển từ trọng tâm tập trung vào ứng dụng sang tập trung vào dữ liệu, các tổ chức sử dụng COBIT 2019 có thể cải thiện việc quản trị và bảo vệ dữ liệu của họ và thông tin.

Mặc dù COBIT 2019 cung cấp các đề xuất cải tiến hợp lý và toàn diện để bắt đầu cuộc hành trình quản trị bảo mật, nhưng các tổ chức rõ ràng cần phải vượt ra khỏi sự tuân thủ và bảo mật mang tính phản ứng để chủ động bắt buộc nhu cầu về quyền riêng tư và bảo mật dữ liệu trên toàn doanh nghiệp. Trong wavdata này luôn được bảo vệ.

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.



ERM và COBIT 2019 có thể được sử dụng riêng hoặc kết hợp. Như với hầu hết các phương pháp cải tiến, chìa khóa thành công là bắt đầu sử dụng chúng từng bước một.

##### Tiêu chuẩn an ninh công nghiệp

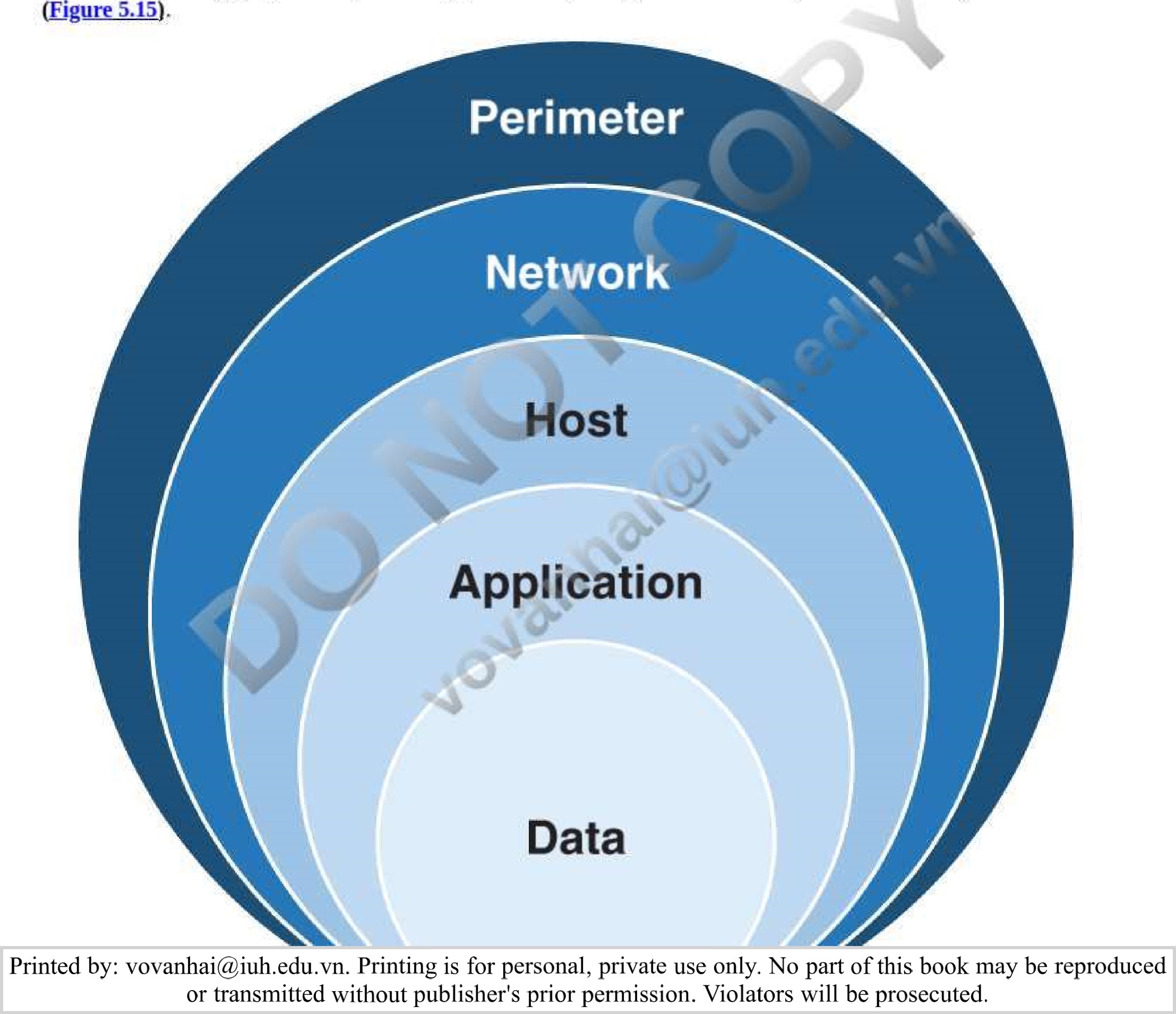
Các nhóm ngành áp đặt các tiêu chuẩn riêng của họ để bảo vệ khách hàng và hình ảnh thương hiệu cũng như doanh thu của các thành viên.

Một ví dụ là Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) do Visa, MasterCard, American Express và Discover tạo ra. PCI dành cho tất cả các thành viên, người bán hoặc nhà cung cấp dịch vụ lưu trữ, xử lý hoặc truyền dữ liệu chủ thẻ. PCI DSS yêu cầu người bán và nhà cung cấp dịch vụ thanh toán thẻ đảm bảo rằng các ứng dụng Web của họ được bảo mật. Nếu được thực hiện đúng cách, điều này có thể làm giảm số vụ vi phạm bảo mật liên quan đến Web.

Mục đích của PCI DSS là cải thiện lòng tin của khách hàng khi nói đến thanh toán trực tuyến và tăng cường bảo mật Web của người bán trực tuyến. Để thúc đẩy tuân theo các tiêu chuẩn này, các hình phạt đối với việc không tuân thủ rất nghiêm khắc. Các thương hiệu thẻ có thể phạt nhà bán lẻ và tăng phí giao dịch cho mỗi giao dịch thẻ tín dụng hoặc thẻ ghi nợ Phát hiện ra sự không tuân thủ có thể là cơ sở cho các vụ kiện.

###### Mô hình phòng thủ chuyên sâu về bảo mật CNTT

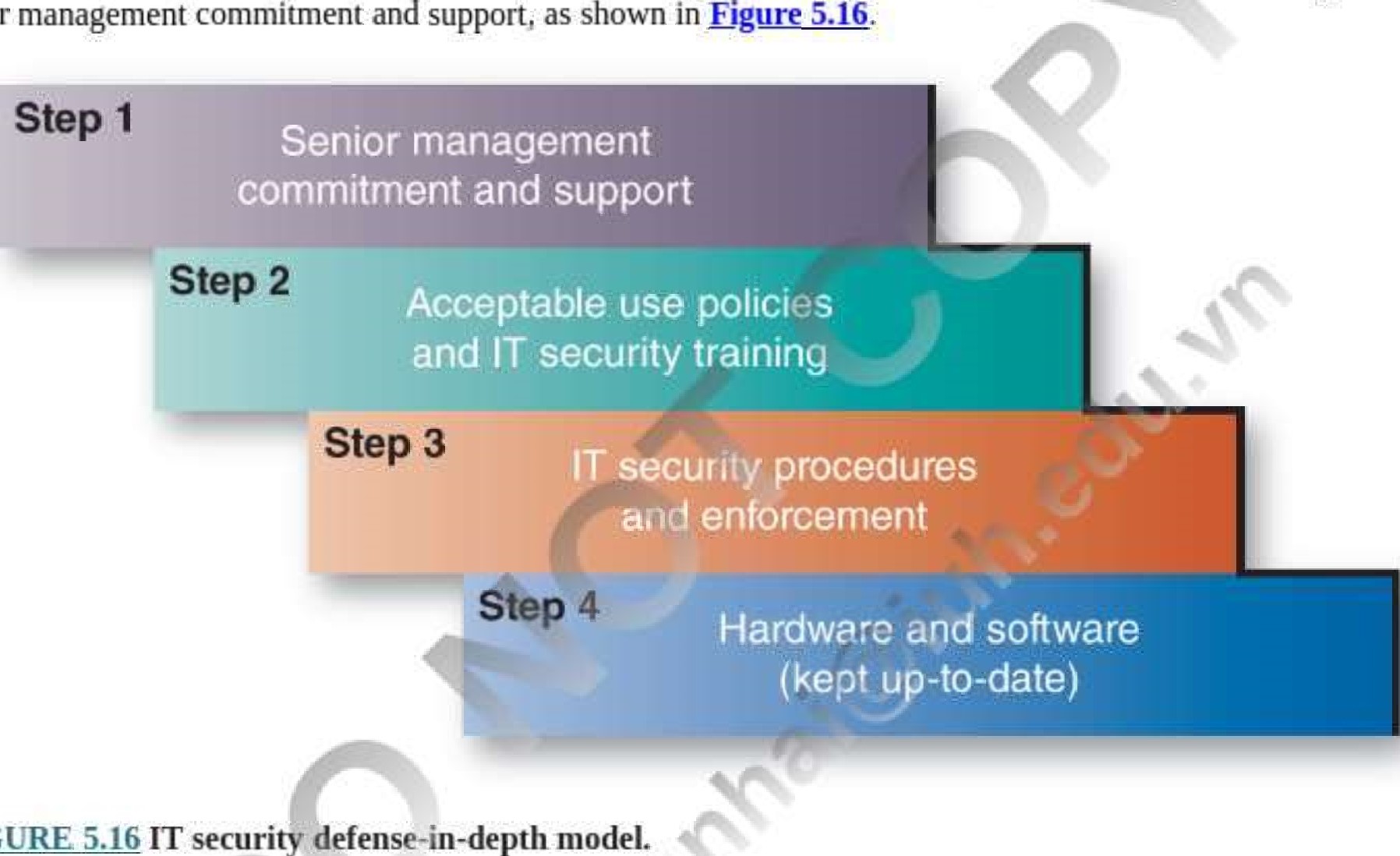
Mô hình phòng thủ chuyên sâu dựa trên tiền đề rằng không có tổ chức nào có thể được bảo vệ hoàn toàn bởi một lớp bảo mật duy nhất. Tuy nhiên, khi có nhiều cấp độ bảo vệ an ninh như xác thực và ủy quyền, tường lửa, trình quét phần mềm độc hại, hệ thống phát hiện xâm nhập, mã hóa dữ liệu, cơ chế kiểm tra và các chương trình đào tạo bảo mật người dùng thì các lỗ hổng do một cấp độ bảo mật duy nhất tạo ra có thể được khắc phục hiệu quả. loại bỏ





HÌNH 5.15 Nhiều lớp bảo vệ.

Mục tiêu của Mô hình là cung cấp dự phòng để giúp tổ chức có thêm thời gian trong trường hợp bị tấn công mạng hoặc lỗ hổng khác và liên quan đến con người, quy trình, công nghệ và môi trường vật lý của hệ thống. Nguyên tắc cơ bản là khi một lớp bảo vệ bị lỗi, lớp khác sẽ cung cấp sự bảo vệ . Ví dụ: nếu bảo mật của mạng không dây bị xâm phạm, thì dữ liệu được mã hóa vẫn sẽ bảo vệ dữ liệu, với điều kiện là kẻ trộm không thể giải mã được.

Sự thành công của bất kỳ loại dự án CNTT nào đều phụ thuộc vào cam kết và sự tham gia của ban quản lý điều hành, còn được gọi là giọng điệu của cấp trên. Điều này cũng đúng với bảo mật CNTT. Lập trường bảo mật thông tin của một tổ chức giúp người dùng nhận thức được rằng các hành vi và sai lầm không an toàn sẽ không được dung thứ. Do đó, một mô hình bảo mật CNTT bắt đầu với sự cam kết và hỗ trợ của quản lý cấp cao, như được trình bày trong Ví dụ 5.16 .

HÌNH 5.16 Mô hình phòng thủ chuyên sâu về bảo mật CNTT.

Để sử dụng Mô hình phòng thủ chuyên sâu, một tổ chức phải thực hiện bốn bước chính:

Bước 1: Nhận được sự cam kết và hỗ trợ của quản lý cấp cao

Ảnh hưởng của các nhà quản lý cấp cao là cần thiết để thực hiện và duy trì an ninh, tiêu chuẩn đạo đức, thực hành quyền riêng tư và kiểm soát nội bộ. Bảo mật CNTT là tốt nhất khi nó được định hướng hàng đầu. Các nhà quản lý cấp cao quyết định mức độ nghiêm ngặt của các chính sách và thực tiễn bảo mật thông tin để tuân thủ luật pháp và quy định. Ví dụ: các tổ chức tài chính phải tuân theo các quy tắc bảo mật và chống rửa tiền (AML) nghiêm ngặt vì họ phải đối mặt với nhiều quy định quốc gia và quốc tế cũng như có dữ liệu có giá trị cao. Các đại lý quảng cáo và công ty ít bị quản lý hơn có xu hướng áp dụng các quy tắc dễ dãi hơn. Các yếu tố khác ảnh hưởng đến chính sách bảo mật thông tin là văn hóa của công ty và dữ liệu của họ có giá trị như thế nào đối với bọn tội phạm.

Chẳng hạn, ban quản lý có thể quyết định cấm nhân viên sử dụng tài khoản e-mail của công ty cho các mục đích không liên quan đến công việc, truy cập mạng xã hội trong giờ làm việc hoặc truy cập các trang web đánh bạc. Những quyết định này sau đó sẽ trở thành các quy tắc được nêu trong chính sách của công ty, được tích hợp vào các quy trình và được thực hiện với các biện pháp phòng vệ công nghệ. Ví dụ, các trang web bị cấm có thể bị chặn bởi tường lửa,

###### Bước 2: Phát triển Chính sách Sử dụng Chấp nhận được và Đào tạo Bảo mật CNTT

Các tổ chức cần đưa ra các chính sách và quy trình mạnh mẽ để làm rõ trách nhiệm và trách nhiệm giải trình đối với tất cả nhân viên. Chính sách sử dụng được chấp nhận (AUP) giải thích những gì ban quản lý đã quyết định là các hoạt động được chấp nhận và không được chấp nhận cũng như hậu quả của việc không tuân thủ. Các quy tắc về tweet, nhắn tin, mạng xã hội, e-mail,

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

PI x L = 0,02 x 0,1 x lây nhiễm bắt nguồn từ một nhân viên sử dụng điện thoại thông minh không được bảo vệ kết nối với mạng công ty, các chính sách đối với



hạn chế hoặc cấm những kết nối đó có thể được khuyến khích.

###### Bước 3: Tạo và Thực thi Quy trình và Thực thi Bảo mật CNTT

Các thủ tục an toàn xác định cách các chính sách sẽ được thực thi, cách ngăn chặn sự cố và cách ứng phó với sự cố. Dưới đây là các thủ tục an toàn cơ bản cần áp dụng;

1. Xác định các thủ tục thực thi Các quy tắc được xác định trong AUP phải được thực thi và các thủ tục thực thi phải được áp dụng nhất quán. Các quy trình giám sát việc sử dụng Internet và mạng của nhân viên được xác định ở giai đoạn này.
2. Chỉ định và trao quyền cho một nhóm ứng phó sự cố nội bộ (IRT) IRT thường bao gồm CISC), cố vấn pháp lý, quản lý cấp cao, nhà truyền thông có kinh nghiệm và nhân viên điều hành chính. Giảm thiểu quy mô nhóm và bộ máy quan liêu có thể đẩy nhanh quá trình ra quyết định và phản hồi. Vì có thể có các vấn đề trách nhiệm pháp lý nghiêm trọng, cố vấn pháp lý cần tham gia vào việc lập kế hoạch và liên lạc ứng phó sự cố.
3. Xác định thủ tục thông báo Khi vi phạm dữ liệu xảy ra, sở cảnh sát địa phương, văn phòng địa phương của FBI, Ủy ban Chứng khoán và Giao dịch (SEC), Cơ quan Mật vụ Hoa Kỳ hoặc cơ quan liên quan khác cần được thông báo ngay lập tức. Luật liên bang và tiểu bang hoặc các quy định của ngành có thể xác định cách thức và thời điểm những người bị ảnh hưởng cần được thông báo.
4. Xác định kế hoạch truyền thông ứng phó với vi phạm Các kế hoạch truyền thông ứng phó với sự cố hiệu quả bao gồm nhân sự và quy trình với các danh sách, kênh và phương tiện truyền thông xã hội cần thiết để thực hiện tất cả các hoạt động truyền thông có thể cần thiết.
5. Theo dõi thông tin và các nguồn truyền thông xã hội Theo dõi Twitter, mạng xã hội và tin tức như một quy trình chuẩn để hiểu cách mọi người phản ứng với sự cố và chỉ trích công ty. Các thủ tục kiểm soát trang có thể cần thiết.

Khi xảy ra sự cố, tổ chức 01 sẵn sàng ứng phó một cách thông minh — có chính sách phù hợp để trung thực„ cởi mở và có trách nhiệm, đồng thời giao tiếp với người tiêu dùng1S và các đối tượng quan trọng khác nhanh nhất có thể.

Bước 4: Triển khai các công cụ bảo mật: Phần cứng và phần mềm

Bước cuối cùng trong mô hình là triển khai phần mềm và phần cứng cần thiết để hỗ trợ và thực thi AUP và thực hành bảo mật. Việc lựa chọn các biện pháp bảo vệ phần cứng và phần mềm dựa trên yisk, ngân sách bảo mật, AUF' và các thủ tục bảo mật. Mọi thiết bị kết nối với mạng của một tổ chức; mọi hoạt động trực tuyến và ứng dụng di động của nhân viên; và mỗi tệp được gửi hoặc nhận là các điểm truy cập. Cơ chế phòng thủ và công nghệ cần phải:

* có thể cung cấp khả năng kiểm soát angaccess xác thực mạnh ở cấp công nghiệp
* phù hợp với các loại mạng và hệ điều hành,
* đã cài đặt và cấu hình đúng
* kiểm tra nghiêm ngặt
* duy trì thường xuyên

Bất kể khuôn khổ, tiêu chuẩn và biện pháp kiểm soát nào được sử dụng để đánh giá, giám sát và kiểm soát rủi ro mạng, thì phải sử dụng một cách tiếp cận cân bằng để đo lường chi phí trực tiếp và tác động vô hình liên quan đến các cuộc tấn công mạng nhằm vẽ ra một bức tranh chính xác về thiệt hại phải gánh chịu và hướng dẫn tạo ra các biện pháp an ninh gia tăng trong tương lai. Bạn có thể thấy một số lợi ích có thể đạt được từ việc thông qua các quy định về bảo mật dữ liệu và an ninh mạng trong CNTT tại nơi làm việc 5.5 .

### CNTT tại nơi làm việc 5.5

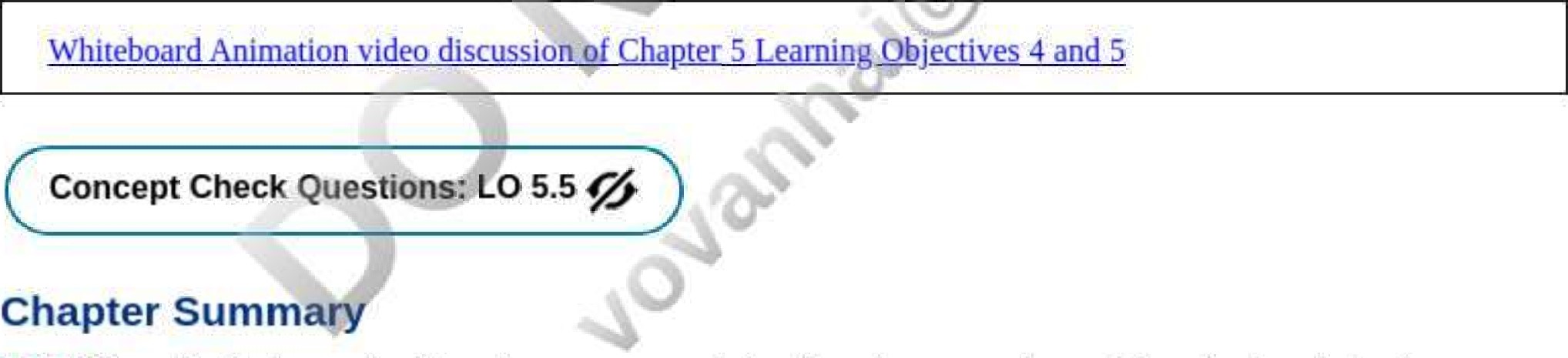
Kenya đang tăng cường bảo vệ dữ liệu kỹ thuật số của công dân

Từ lâu, người ta đã thừa nhận rằng các chính phủ và công ty châu Phi ít quan tâm đến bảo mật dữ liệu.

Nhu cầu về ber securi đã trở nên cấp thiết hơn với sự gia tăng nhanh chóng về số lượng thiết bị di động và

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

|  |
| --- |
| ứng dụng và số lượng ngày càng tăng của các cuộc tấn công nhằm vào người tiêu dùng đang đăng ký tín dụng trực tuyến. Sự thiếu quan tâm này đã tạo điều kiện cho các gã khổng lồ truyền thông xã hội Facebook, WhatsApp và Google, những người bị hạn chế ở các nơi khác trên thế giới bởi các quy định về bảo mật dữ liệu và an ninh mạng hiện hành, có quyền truy cập dễ dàng vào thông tin cá nhân của người tiêu dùng trên khắp Châu Phi.    Tình trạng này đã thay đổi vào tháng 11 năm 2019 khi tổng thống Kenya Uhuru Kenyatta bắt tay và phê chuẩn luật bảo vệ dữ liệu mới lấy cảm hứng từ Liên minh Châu Âu. Luật này đang thiết lập một tiêu chuẩn cao cho phần còn lại của lục địa châu Phi. Luật mới tuân thủ GDPR của EU và đưa ra các hạn chế đối với việc xử lý và chia sẻ dữ liệu của chính phủ và các tập đoàn Kenya. Các công ty như Kenya Airways và các khách sạn cũng như công ty cho vay qua điện thoại Safaricom sẽ phải tuân thủ luật bảo vệ dữ liệu mới khi xử lý dữ liệu cá nhân từ khách hàng của họ.    Bất kỳ hành vi vi phạm luật mới nào sẽ bị điều tra bởi một văn phòng độc lập với những người vi phạm phải đối mặt với án tù hai năm hoặc mức phạt tối đa là 29.000 đô la.  Chính phủ cảm thấy rằng luật mới rất quan trọng trong việc khuyến khích đầu tư mới, đặc biệt là trong lĩnh vực tài chính. Nó đã tăng cường đầu tư vào lĩnh vực CNTT của mình. Amazon Web Services đã xác nhận kế hoạch xây dựng một số cơ sở hạ tầng của mình ở Kenya và mở rộng hoạt động. Bảo vệ dữ liệu nghiêm ngặt hơn cũng mang lại lợi ích cho chính phủ Kenya bằng cách xua tan những lo ngại về cách họ lưu trữ và xử lý dữ liệu công dân, đồng thời giúp vượt qua những chỉ trích rộng rãi về kế hoạch số hóa danh tính công dân của họ.        câu hỏi  1. Mục đích của việc kiểm soát phòng thủ chung là gì?  2  Mục đích của kiểm soát bảo vệ ứng dụng là gì? 3   1. Đặt tên cho năm loại chính của kiểm soát chung.      1. Đặt tên cho bốn điều khiển ứng dụng.     Giải thích xác thực và đặt tên cho hai phương pháp xác thực.  6v Sáu mục tiêu chính của chiến lược phòng thủ là gì?  7. Mục đích của PCI DSS là gì?  Các yếu tố chính trong COBIT 2019 là gì?  9. Bốn thành phần nào tạo nên mô hình chuyên sâu về phòng thủ bảo mật CNTT?'  Nguồn: Tổng hợp từ Anonymous ( 2019 ), Kazeem( 2019 ), Obulutsa và Miriri ( 2019 ), và Reuters ( 2019 )' |



L05.1 Mô tả bốn mối quan ngại chính về quyền riêng tư dữ liệu, xác định nghịch lý về quyền riêng tư và mô tả cách quyền riêng tư dữ liệu





các quy định đang bảo vệ người tiêu dùng.

Các vấn đề về quyền riêng tư dữ liệu có thể phát triển xung quanh dữ liệu từ nhiều nguồn. Bốn mối quan tâm chính về quyền riêng tư của dữ liệu là cách dữ liệu được chia sẻ, thu thập, sử dụng và quản lý. Nghịch lý về quyền riêng tư xảy ra khi mọi người nói rằng họ quan tâm đến tính bảo mật của dữ liệu nhưng lại không làm gì để ngăn dữ liệu bị lộ và trên thực tế, hành xử theo cách làm trầm trọng thêm vấn đề. Các quy định về quyền riêng tư đối với dữ liệu người tiêu dùng của Hoa Kỳ bao gồm những quy định liên quan đến chăm sóc sức khỏe, tài chính, chính phủ, giấy phép và tín dụng. Ở cấp liên bang, Ủy ban Thương mại Liên bang (FTC) chịu trách nhiệm ban hành và thực thi luật bảo vệ dữ liệu của Hoa Kỳ, nhưng trách nhiệm tuân thủ các luật đó thuộc về Tổng chưởng lý Tiểu bang. Các quy định chính của liên bang Hoa Kỳ hiện đang áp dụng bao gồm Bảo hiểm Y tế

|  |
| --- |
| tha  Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố. |

Đạo luật về tính di động và trách nhiệm giải trình (HIPAA), Đạo luật Gramm-Leach-Bliley, Đạo luật bảo vệ quyền riêng tư năm 1980, Đạo luật bảo vệ quyền riêng tư của người lái xe (DPPA) và Đạo luật báo cáo tín dụng công bằng. Ở cấp tiểu bang, luật bảo vệ quyền riêng tư dữ liệu mạnh mẽ nhất là Đạo luật về quyền riêng tư của người tiêu dùng California (CCPA).

Ở cấp độ toàn cầu, quy định nghiêm ngặt nhất về quyền riêng tư dữ liệu đối với sách tại thời điểm hiện tại là Quy tắc bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR)e Bộ hoặc quy định mới được ban hành này trao quyền cho người tiêu dùng EU bằng cách buộc các nhà bán lẻ, nhà tiếp thị và những người khác phải tư vấn rõ ràng cho người tiêu dùng cách họ thu thập, sử dụng và lưu trữ dữ liệu người tiêu dùng, GDPR thống nhất luật bảo vệ dữ liệu đối với 28 quốc gia EU cộng với Ireland, Lichtenstein, Na Uy và Thụy Sĩ để cung cấp cho người tiêu dùng nhiều quyền hơn và kiểm soát thông tin của họ. Mức phạt tối đa có thể áp dụng đối với hành vi vi phạm GDPR là mức cao nhất trong số các quy định về quyền riêng tư dữ liệu. Hoa Kỳ hiện không có luật riêng tư đầy đủ, không tuân thủ các yêu cầu của GDPR và hiện phải khắc phục sự thiếu sót này bằng cách tuân thủ Lá chắn bảo mật EU-Hoa Kỳ và Thụy Sĩ-Hoa Kỳ. Các yêu cầu về Bảo vệ quyền riêng tư.

L05.2Xác định mức độ và chi phí của các cuộc tấn công mạng và 12 loại đe dọa mạng có chủ ý và không chủ ý khác nhau.

Ngày càng có nhiều cuộc tấn công mạng được báo cáo hàng ngày trên toàn thế giới và một tỷ lệ lớn ở Hoa Kỳ. người tiêu dùng cảm thấy rằng dữ liệu của họ kém an toàn hơn so với 5 năm trước. Ví dụ về các lỗ hổng trong một tổ chức có thể dẫn đến các cuộc tấn công mạng bao gồm việc thiếu kiểm soát đối với con người, quy trình và công nghệ. Một số mối đe dọa mạng không chủ ý và cố ý là nguyên nhân của hầu hết các cuộc tấn công mạng. Các mối đe dọa không chủ ý trên mạng bao gồm lỗi của con người, các mối nguy môi trường và lỗi hệ thống máy tính. Các mối đe dọa mạng có chủ ý bao gồm: hack, lừa đảo, cài đặt một số loại phần mềm độc hại xâm nhập và độc hại, botnet, ransomware, cryptojacking, SQL 'injection, tấn công trung gian, từ chối dịch vụ, đe dọa nội bộ, trộm cắp hoặc mất mát vật lý, và các lỗi linh tinh.

L05.3 Thảo luận về sáu mục tiêu nguy hiểm nhất của các cuộc tấn công mạng và đưa ra ví dụ về tác động của từng mục tiêu đối với người tiêu dùng và tổ chức.

Sáu mục tiêu nguy hiểm và phổ biến nhất mà tội phạm mạng tấn công vào các công ty và cơ quan chính phủ bao gồm: mật khẩu yếu, cơ sở hạ tầng quan trọng, đánh cắp IP, hành vi trộm cắp nhận dạng, mang theo thiết bị của riêng bạn (BYOD) và phương tiện truyền thông xã hội. Mật khẩu yếu là một trong những điểm yếu lớn nhất có thể được sử dụng để thực hiện nhiều loại mối đe dọa mạng. Các cuộc tấn công vào cơ sở hạ tầng quan trọng có thể làm gián đoạn đáng kể các mục tiêu của chính phủ và ngành, thậm chí có thể làm tổn hại đến các dịch vụ thiết yếu trong toàn bộ quốc gia hoặc khu vực. • Hành vi trộm cắp tài sản trí tuệ đang gia tăng và đặc biệt đáng lo ngại vì hành vi này có thể đe dọa sự tồn tại của một công ty hoặc phơi bày các chính sách và hoạt động tình báo của một quốc gia thủ tục. Hành vi trộm cắp danh tính cũng đang gia tăng và có thể dẫn đến sự bất tiện cũng như mất thời gian và nguồn lực. Một mối quan tâm khác đối với các tổ chức là lỗ hổng gây ra khi nhân viên mang thiết bị của riêng họ (BYOD) đi làm. Các thiết bị di động là mục tiêu dễ dàng của bọn tội phạm mạng vì khả năng xác thực yếu, thiếu kiểm soát truy cập và mã hóa không đầy đủ hoặc không tồn tại. BYOD cho phép hacke1S đột nhập vào thiết bị di động và vượt qua mạng của nhà tuyển dụng để đánh cắp dữ liệu nhạy cảm và bí mật của công ty. Ngoài ra, cơ sở hạ tầng di động của tập đoàn có thể không hỗ trợ được sự gia tăng lưu lượng mạng di động gây ra sự chậm trễ không thể chấp nhận được hoặc yêu cầu đầu tư vào các nguồn lực bổ sung để theo kịp nhu cầu. Cuối cùng, các cuộc tấn công trên mạng xã hội được dự đoán sẽ tiếp tục là mối đe dọa lớn đối với các doanh nghiệp. Mạng xã hội và điện toán đám mây làm gia tăng các lỗ hổng bằng cách cung cấp một điểm lỗi duy nhất khiến nó dễ bị cài đặt phần mềm độc hại và các loại tấn công mạng khó phát hiện khác. Những điều này khiến tổ chức và dữ liệu khách hàng của tổ chức có nguy cơ bị lộ và bị đánh cắp.

L05.4Xác định sáu chiến lược phòng thủ không gian mạng, bốn phương pháp quản lý rủi ro và ba công cụ phòng thủ CNTT thiết yếu. 

Có sáu chiến lược phòng thủ hiệu quả trước các cuộc tấn công mạng. Đó là: phòng ngừa và răn đe, phát hiện, ngăn chặn, phục hồi, khắc phục và nhận thức/tuân thủ. Khi xác định chiến lược phòng thủ, một công ty phải xác định mức độ' rủi ro mà công ty sẵn sàng chấp nhận để chống lại các cuộc tấn công mạng. Có bốn phương pháp giảm thiểu rủi ro có thể được thực hiện: chấp nhận, hạn chế, tránh hoặc chuyển nhượng, tùy thuộc vào giá trị của tài sản được bảo vệ và hậu quả nếu dữ liệu liên quan bị xâm phạm. Ba công cụ bảo vệ CNTT thiết yếu hữu ích trong việc bảo vệ chống lại các cuộc tấn công mạng . Đó là: phần mềm chống vi-rút, hệ thống phát hiện xâm nhập và hệ thống ngăn chặn xâm nhập. Phần mềm chống vi-rút được thiết kế để phát hiện các mã độc hại và ngăn người dùng tải chúng xuống cũng như quét hệ thống để tìm sâu, trojan và các loại mối đe dọa mạng khác. Các hệ thống phát hiện xâm nhập quét các lưu lượng truy cập mạng bất thường hoặc đáng ngờ để cảnh báo cho nhân viên mạng thực hiện hành động phòng thủ. Hệ thống ngăn chặn xâm nhập được thiết kế để thực hiện hành động ngay lập tức, chẳng hạn như chặn địa chỉ IP và chặn các cuộc tấn công DDoS.

L05.5Xác định năm biện pháp kiểm soát phòng thủ chung chính, tám biện pháp kiểm soát phòng thủ ứng dụng chính cũng như các quy định và khuôn khổ an ninh mạng giúp bảo vệ người tiêu dùng và hướng dẫn quản trị CNTT.

Năm biện pháp kiểm soát phòng thủ chung chính là vật lý, truy cập, bảo mật dữ liệu, liên lạc và hành chính. Tám điều khiển bảo vệ ứng dụng chính là tính đầy đủ; hiệu lực, xác thực, ủy quyền, kiểm soát đầu vào, tính khả dụng, danh sách trắng và danh sách đen. Các quy định về an ninh mạng đã được đưa ra để bảo vệ người tiêu dùng và bảo vệ các công ty khỏi các vụ kiện do vi phạm dữ liệu và các loại tấn công mạng khác. Các quy định đã được phát triển ở cấp liên bang và tiểu bang. Đạo luật quản lý bảo mật thông tin liên bang (FISMA) yêu cầu các cơ quan liên bang phát triển, lập tài liệu và triển khai chương trình bảo vệ và bảo mật thông tin, trong khi

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Khung quản lý rủi ro doanh nghiệp (ERM) và COBIT 2019 tập trung vào các vấn đề quản lý rủi ro và quản trị CNTT. Mô hình Phòng thủ Chuyên sâu Bảo mật CNTT tổng thể là một cách tiếp cận nhiều lớp để bảo vệ an ninh bao gồm xác thực, ủy quyền, tường lửa, trình quét phần mềm độc hại, hệ thống phát hiện xâm nhập, mã hóa dữ liệu, v.v. được kích hoạt ở nhiều lớp khác nhau của hệ thống để cung cấp các phương án dự phòng đến một lớp bảo vệ khác trong trường hợp bị tấn công mạng

#### Điều khoản quan trọng

chính sách sử dụng được chấp nhận Kiểm soát truy cập nâng cao mối đe dọa liên tục ( APT )

Phần mềm quảng cáo



App

lication

breach

of

business

business

Control

kiểm tra vectơ tấn công

Cửa sau

Botnet kiểm soát sinh trắc học

trang web lạnh

tin tặc hợp đồng

Bánh quy

Cơ sở hạ tầng quan trọng Tiền điện tử xác nhận các cuộc tấn công mạng An ninh mạng Các mối đe dọa mạng Vi phạm dữ liệu Bảo mật dữ liệu Dữ liệu giả mạo tấn công từ chối dịch vụ phân tán ( DDoS ) các quy tắc không mang theo Rủi ro

An ninh thông tin liên bang và gian lận

Kiểm soát phòng thủ chung

Màu xám trang web Hackin g hacktivists

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

Kiểm soát nội bộ trí tuệ (ICI Phát hiện xâm nhập

Ngăn chặn xâm nhập ( IPSs ) \_

IT g overnance IT khả năng phục hồi phần mềm độc hại si g natures Man-in-the-middle itM) Mobile biometrics p aches pay load Phishin g



Rogue

khiển P\_by \_sical p rivac y\_p aradox Ransomware Truy cập từ xa từ xa xóa khả năng giảm thiểu rủi ro rủi ro

rootkit

Gói dịch vụ Shadow IT social en g ineerin g spam

Sp tai p hihin g

Phần mềm gián điệp SQL Inj ection tàng hình Trojan IT time-to-ex p loitation

Vi-rút

Lỗ hổng sinh trắc giọng nói Trang web ấm Mũ trắng

Sâu

kinh nghiệm bằng không

#### Bài tập tương tác

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

##### Thảo luận: Câu hỏi Tư duy Phản biện

1, Vì sao tội phạm mạng ngày càng bành trướng nhanh chóng? Thảo luận về một số giải pháp khả thi.

2. Ngoài hacke1S, các tổ chức cần bảo vệ chống lại những loại tội phạm mạng nào?

3, Động cơ chính của tội phạm mạng là gì?

4, Người dùng dễ bị tội phạm mạng tấn công bằng những cách nào?

5, Tại sao những người tạo phần mềm độc hại thay đổi phần mềm độc hại của họ?

6, Tại sao bạn nên đặt mật khẩu riêng cho từng trang web, dịch vụ và thiết bị mà bạn sử dụng?

7. Làm cách nào để ngăn chặn ransomware đánh cắp hoặc tiết lộ dữ liệu từ mạng của một tổ chức?

8. Những khoản tiền phạt khổng lồ có thể ảnh hưởng như thế nào đến ngân sách của công ty dành cho việc bảo vệ an ninh CNTT?

9. Tại sao các quy tắc BYOD, BYOA và không mang theo lại quan trọng đối với bảo mật CNTT? Tại sao người dùng có thể chống lại các quy tắc như vậy?

1. Tại sao người dùng từ chối sử dụng mật khẩu mạnh mặc dù họ biết mật khẩu yếu nguy hiểm như thế nào?
2. Những yếu tố nào các công ty nên xem xét khi họ đang lựa chọn một chiến lược quản lý rủi ro?
3. Tại sao việc kiểm soát và bảo mật thông tin phải được ban lãnh đạo quan tâm hàng đầu?
4. Giải thích những gì tường lửa bảo vệ và những gì chúng không bảo vệ.

14, Tại sao xác thực và phân quyền lại quan trọng trong thương mại điện tử?

15, Một số công ty bảo hiểm sẽ không bảo hiểm cho một doanh nghiệp trừ khi công ty đó có kế hoạch khắc phục thảm họa máy tính. Giải thích vì sao.

16. Giải thích lý do tại sao quản lý rủi ro nên liên quan đến các yếu tố sau: các mối đe dọa, mức độ phơi bày liên quan đến từng mối đe dọa, rủi ro xảy ra với từng mối đe dọa, chi phí kiểm soát và đánh giá hiệu quả của chúng.

##### Khám phá: Bài tập trực tuyến và tương tác



1. Truy cập https://www.watchguard.com/wgrd-resource-center/security-rep01t-q3-2019. Đọc hai trang

Giới thiệu, Tóm tắt nội dung và Báo cáo Điểm nổi bật của Báo cáo bảo mật Internet quý 3 năm 2019 của WatchGuard T. Tóm tắt những gì bạn đã học được và viết một bài luận ý kiến về số liệu thống kê về tấn công mạng được báo cáo.

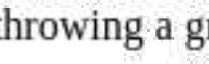
2, Truy cập https://www.zdnet.com/articlelthis-new-ransomware-is-targeting-health-and-tech-companies-acrosseurope-and-north-america/.

1. Xem video và đọc bài viết về các cuộc tấn công ransomware nhắm vào các công ty công nghệ và chăm sóc sức khỏe ở Châu Âu, Hoa Kỳ và Canada.
2. Giải thích lý do cho những vi phạm này và thảo luận làm thế nào chúng có thể tránh được.

3. Truy cập https://iwww.identityforce.com/resources/quiz và làm bài Trắc nghiệm Trộm danh tính. Điểm số của bạn là gì? Giải thích những cách mà bạn có thể cải thiện điểm số của mình để bạn không có nhiều nguy cơ bị đánh cắp danh tính,

4. Truy cập https://www.cshub.com/content-hubfincident-of-the-week và chọn một trong những vi phạm dữ liệu chính được liệt kê. Đọc về vi phạm dữ liệu mà bạn đã chọn. Những bài học bạn đã học được từ bài viết? Mô tả phản ứng của bạn với những gì bạn đọc.

##### Phân tích & Quyết định: Áp dụng các khái niệm CNTT vào các quyết định kinh doanh

1. Nhiều công ty tập trung vào các câu hỏi sai và kết thúc bằng rất nhiều tiền bạc và thời gian với rủi ro bảo mật tối thiểu trong khi bỏ qua các lỗ hổng lớn. Tại sao?
2. Việc đánh giá một công ty có nghĩa vụ pháp lý phải đầu tư bao nhiêu vào an ninh mạng vẫn là một thách thức. Vì không có thứ gọi là bảo mật hoàn hảo (nghĩa là bạn luôn có thể làm được nhiều hơn thế), nên việc giải quyết những câu hỏi này có thể ảnh hưởng đáng kể đến chi phí.
   1. Khi nào các biện pháp an ninh của công ty đủ để tuân thủ các nghĩa vụ của công ty? Ví dụ: việc cài đặt tường lửa và sử dụng phần mềm phát hiện vi-rút có đáp ứng các nghĩa vụ pháp lý của công ty không?
   2. Tổ chức có cần mã hóa tất cả dữ liệu của mình không?
3. Giả sử rằng xác suất xảy ra một trận động đất lớn hàng ngày ở Los Angeles là 0,07%. Cơ hội của máy tính của bạn

Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.

trung tâm bị hư hại trong một trận động đất như vậy là 5 0 /0. Nếu trung tâm bị hư hại, thiệt hại ước tính trung bình sẽ là SIS triệu.

1. Tính tổn thất dự kiến (bằng đô la),
2. Một đại lý bảo hiểm sẵn sàng bảo hiểm cho cơ sở của bạn với mức phí hàng năm là 15.000 đô la. Phân tích lời đề nghị và thảo luận xem có nên chấp nhận nó hay không.

4. Người sử dụng lao động có nên thông báo cho nhân viên rằng việc sử dụng máy tính của họ đang bị theo dõi không? Tại sao hay tại sao không?

5. 25.000 tin nhắn đến một tổ chức mỗi năm. Hiện tại, không có tường lửa. Trung bình, 1,2 vụ hack thành công xảy ra mỗi năm. Mỗi cuộc tấn công hack thành công dẫn đến tổn thất khoảng 130.000 đô la cho công ty. Một tường lửa lớn được đề xuất với chi phí 66.000 USD. Thời gian sử dụng hữu ích ước tính là ba năm. Cơ hội để kẻ xâm nhập vượt qua tường lửa là 0,0002. Trong trường hợp như vậy, thiệt hại sẽ là $100.000 (30%),

$200.000 (50%), nếu không sẽ không có thiệt hại. Có chi phí bảo trì hàng năm là 20.000 đô la cho tường lửa.

1. Ban quản lý có nên mua tường lửa không?
2. Hiện có một tường lửa cải tiến có hiệu quả 99,9988% và có giá 84.000 đô la, với tuổi thọ ba năm và chi phí bảo trì hàng năm là 16.000 đô la. Tường lửa này có nên thay vì cái đầu tiên không? Củng cố: Đảm bảo bạn hiểu các Điều khoản chính

Giải ô chữ trực tuyến được cung cấp cho chương này.

##### Tài nguyên web

Tài nguyên nốt ruồi và công cụ học tập được đặt trên trang web của sinh viên. Bạn sẽ tìm thấy các liên kết Web hữu ích và các câu đố tự kiểm tra cung cấp phản hồi cho từng cá nhân.

|  |
| --- |
| Trường hợp 5.2  Trường hợp kinh doanh: Các khách sạn Marriott đa quốc gia có thể phải đối mặt với phản ứng dữ dội của người tiêu dùng và khoản tiền phạt theo quy định và chi phí kiện tụng lên tới 1 tỷ đô la hoặc vi phạm dữ liệu lớn  Marriott là nhà điều hành khách sạn lớn nhất thế giới với khoảng 9.000 khách sạn tại 127 quốc gia trên thế giới. Vào tháng 12 năm 2018, Marriott đã phát hiện và báo cáo một cuộc tấn công vào mạng đặt phòng Stanyood đã xảy ra trong khoảng thời gian bốn năm! Từ 2014 đến 2018ihe chi tiết cá nhân lên tới 500 triệu  Khách của khách sạn Marriott đã bị lộ khiến nó trở thành một trong những cuộc tấn công mạng lớn nhất được báo cáo. Khoảng 387 triệu chứa thông tin cá nhân nhạy cảm như e-mail, ngày sinh, số hộ chiếu, địa chỉ thực và chi tiết thẻ tín dụng. Mặc dù Marriott tuyên bố rằng các chi tiết như số thẻ tín dụng đã được mã hóa nhưng người ta tin rằng có đủ thông tin chi tiết để những kẻ tấn công giải mã thông tin. Sau khi tiết lộ về việc cổ phiếu của attacOIarriott đã giảm 5,6 0 / 0 trong giao dịch trước giờ mở cửa và các nạn nhân của vụ tấn công đã lên tiếng phàn nàn trên mạng xã hội sau khi biết được tình hình qua báo chí trước khi nhận được bất kỳ thông báo nào từ Marriott.    Mặc dù quy mô của cuộc tấn công không thể so sánh với quy mô của Yahoo được mô tả trong trường hợp mở đầu, nhưng thiệt hại đối với danh tiếng của Marriott là đặc biệt nghiêm trọng. Khách của nó dựa vào chuỗi khách sạn để giữ cho họ an toàn và bảo mật trong thế giới thực và cuộc tấn công dường như cho thấy rằng Maniott không có khả năng đảm bảo an toàn và bảo mật kỹ thuật số cho khách của mình. Để tăng thêm sự xúc phạm cho thương tích, công ty có thể phải đối mặt với khoản tiền phạt theo quy định và chi phí kiện tụng lên tới 1 tỷ đô la. Để cố gắng giảm thiểu tác động của vụ tấn công, Arne Sorenson, giám đốc điều hành của Marriott đã liên hệ với những người bị ảnh hưởng bằng cách nói rằng "Chúng tôi vô cùng lấy làm tiếc vì sự cố đã xảy ra. Chúng tôi đã không đáp ứng được những gì khách hàng xứng đáng được nhận và những gì chúng tôi mong đợi ở chính mình. Chúng tôi đang làm tất cả những gì chúng tôi có thể để hỗ trợ khách và sử dụng các bài học để trở nên tốt hơn trong tương lai."  Cuộc tấn công mới nhất này không phải là lần đầu tiên đối với Marriott. Rất lâu trước khi Man-iott International tiết lộ cuộc tấn công mạng gần đây nhất, gã khổng lồ khách sạn này đã nổi tiếng là mục tiêu dễ dàng của tin tặc. Tin tặc đã đánh cắp thẻ tín dụng, cướp tài khoản khách hàng thân thiết, thực hiện các kế hoạch phức tạp để lừa nhân viên Marriott tải xuống phần mềm độc hại và trong một cuộc tấn công đặc biệt nguy hiểm có tên là 'Khách sạn đen', mạng tại các cơ sở kinh doanh riêng lẻ của Marriott đã bị tấn công để cho phép tin tặc theo dõi các giám đốc điều hành của công ty và chính trị gia. Trong một cuộc tấn công khác, bọn tội phạm mạng đã khóa các phòng bằng cách giành quyền kiểm soát hệ thống ra vào không cần chìa khóa và sẽ không mở khóa cho đến khi chủ sở hữu Marriott trả tiền chuộc. |

|  |
| --- |
| Ngay trước khi xảy ra vụ vi phạm, Marriott cho biết họ đã bắt đầu tăng cường đầu tư vào an ninh mạng và đã thuê một giám đốc an ninh thông tin mới. Cuộc tấn công mạng vào chuỗi khách sạn Marriott được cho là do các tin tặc làm việc cho Bộ An ninh Nhà nước Trung Quốc, cơ quan gián điệp dân sự do cộng sản kiểm soát, thực hiện. Nỗ lực thu thập thông tin tình báo cũng đã tấn công các công ty bảo hiểm y tế và hồ sơ thông quan an ninh của hàng triệu người Mỹ khác đã không được quảng cáo trên các thị trường tội phạm. Đây có thể là một sự an ủi đối với Marriott, người có thể phải đối mặt với việc kinh doanh thua lỗ do phản ứng dữ dội hơn từ chính họ.      khách.  Nhìn chung, ngành công nghiệp khách sạn1Y không được biết đến là có công nghệ bảo mật mạng mạnh mẽ. Đây là ngành được nhắm mục tiêu nhiều thứ ba sau bán lẻ và tài chính. Hilton, Hyatt, Intercontinental, Trump, Radisson và Mandarin  Oriental đều là mục tiêu trong các cuộc tấn công từng phần. Khi các công ty khách sạn thử nghiệm với VOIP và các phòng kết nối Internet có thể dẫn đến việc thu thập và lưu trữ nhiều thông tin cá nhân hơn, nguy cơ tấn công mạng thậm chí còn cao hơn.  câu hỏi   1. Marriott đã hứng chịu một số cuộc tấn công mạng trước cuộc tấn công được mô tả ở đây,-Bạn có nghĩ rằng nó vẫn dễ bị tấn công trước cuộc tấn công hiện tại không?      1. Đưa ra ba lý do tại sao bạn cho rằng Marriott đã không phát hiện ra vi phạm dữ liệu hiện tại trong gần bốn năm, Liệu việc bán dữ liệu cá nhân trên thị trường tội phạm có ảnh hưởng đến tác động của vi phạm dữ liệu này đối với danh tiếng của Marriott không? Giải thích.     4. Nếu bạn là khách hàng của Marriott và được thông báo về hóa đơn dữ liệu cá nhân của bạn, bạn sẽ cảm thấy thế nào và bạn sẽ làm gì?  Nguồn: Bhaktavatsalam và Tumer tổng hợp ( 2018 ), Clark ( 2018 ), Davies ( 2018 hOFlaherty ( 2018) và Kiesnoski (2019). |
| IT Too lbox  0.  Tiến hành Phân tích Chi phí-Lợi ích  Việc chuẩn bị bảo vệ chống lại mọi mối đe dọa có thể xảy ra thường không kinh tế. Do đó, một chương trình bảo mật CNTT phải cung cấp quy trình đánh giá các mối đe dọa và quyết định chuẩn bị đối phó với mối đe dọa nào, bỏ qua mối đe dọa nào và giảm khả năng bảo vệ chống lại mối đe dọa nào. Hai công cụ phân tích chi phí-lợi ích thường được sử dụng là đánh giá rủi ro và đánh giá rủi ro kinh doanh. Đánh giá rủi ro chỉ dựa trên các thước đo định lượng, trong khi phân tích tác động kinh doanh xem xét cả các chỉ số định tính và định lượng.  • Đánh giá rủi ro Đánh giá rủi ro được thực hiện bằng ứng dụng hoặc bảng tính. Các tính toán cơ bản được hiển thị ở đây:  tổn thất dự kiến  Ở đâu    PI xác suất tấn công (ước tính, dựa trên phán đoán) P2 xác suất tấn công thành công (ước tính, dựa trên phán đoán)      L xảy ra nếu tấn công thành công Mất dự kiếnPI x P2 >QL  Ví dụ:    Một tổ chức ước tính rằng xác suất xảy ra một cuộc tấn công mạng là 2% và cuộc tấn công chỉ có 10% cơ hội thành công. Nếu cuộc tấn công thành công, công ty ước tính sẽ mất 1 triệu USD.  Điều này sẽ được thể hiện như sau: |
| PI 0,02, P2 — 0,10, L =    Sau đó, tổn thất dự kiến từ cuộc tấn công cụ thể này là  PI x P2 x L = 0,02 x 0,1 $2.000  • Phân tích tác động kinh doanh    hành động tác động kinh doanh ( BIA ) ước tính hậu quả của việc gián đoạn chức năng kinh doanh và thu thập dữ liệu để phát triển các chiến lược phục hồi.  Các kịch bản tổn thất tiềm năng được xác định đầu tiên trong quá trình đánh giá rủi ro. Các hoạt động cũng có thể bị gián đoạn do lỗi của nhà cung cấp hàng hóa hoặc dịch vụ hoặc việc giao hàng bị chậm trễ. Có nhiều kịch bản có thể xảy ra cần được xem xét,    BIA xác định các tác động về mặt vận hành và tài chính do sự gián đoạn gây ra. Các tác động tài chính dễ đánh giá hơn, nhưng các tác động hoạt động khó xác định hơn do tính chất định tính của chúng. Một số ví dụ về tác động hoạt động và tài chính cần xem xét được trình bày trong Bảng  Các tổn thất được đánh giá bằng hai phương pháp này nên được so sánh với chi phí cho các chiến lược phục hồi khả thi để xác định rủi ro ròng. Báo cáo BIA cũng nên ưu tiên thứ tự các sự kiện khôi phục hoạt động kinh doanh, trong đó các quy trình có tác động tài chính và hoạt động lớn nhất sẽ được khôi phục trước.   |  |  |  | | --- | --- | --- | |  | | | | Gián đoạn kinh doanh Tác động định tính và định lượng | | | | Loại số liệu | | Sự miêu tả | | Tài chính | Định lượng | Mất doanh thu và thu nhập  Doanh thu hoặc thu nhập bị trì hoãn  Chi phí gia tăng (ví dụ: lao động làm thêm giờ, thuê ngoài, chi phí xúc tiến) Tiền phạt theo quy định  Phạt hợp đồng hoặc mất tiền thưởng hợp đồng | | hoạt động | định tính | Khách hàng không hài lòng hoặc rời bỏ Kế hoạch kinh doanh mới bị trì hoãn | |

#### Tài liệu tham khảo (Q

Vô danh. "Kenya thông qua luật bảo vệ dữ liệu để đảm bảo an ninh Digitai." Tài chính Quốc tế, ngày 15 tháng 11 năm 2019a.

Vô danh. "Tấn công lừa đảo ảnh hưởng đến 645.000 khách hàng của Oregon DHS." Prilock, ngày 20 tháng 6 năm 2019b.

Vô danh. "Bayer Nạn nhân của một cuộc tấn công mạng: Truyền thông Đức." PhysOrg, ngày 4 tháng 4 năm 2019.

Auxier, B., L.. Andersons M., Perrin, A. -Kumar, M., và Turner, E. "Người Mỹ và Quyền riêng tư: Lo lắng, Bối rối và Cảm thấy Thiếu Kiểm soát Thông tin Cá nhân của Họ." Báo cáo nghiên cứu của Pew, ngày 15 tháng 11 năm 2019.

Balakrishnan, A. "Chúng tôi buộc tội Nga hack Yahoo." CNBC, ngày 15 tháng 3 năm 2017.

Bhaktavatsalam, S. và Turner, G. "Cuộc tấn công mạng của Marriott khiến dữ liệu của 500 triệu người gặp rủi ro." Quản lý nhà cung cấp dịch vụ, ngày 30 tháng 11 năm 2018.

Tin tứcBloomberg. "Google bị phạt 56,8 triệu đô la từ GDPR của El-I." DigitalC Commerce360, ngày 21 tháng 1 năm 2019.

Bodoni, S. "Pháp sử dụng Luật bảo mật mới của EU để phạt Google 56,8 triệu USD:' Bloomberg, ngày 21 tháng 1 năm 2019.

Brooks, R. "Luật bảo mật dữ liệu của tiểu bang. Phương pháp tiếp cận bảo vệ quyền riêng tư của Hoa Kỳ." Netwrix, ngày 27 tháng 8 năm 2019.

Chaffin, C. "Vi phạm dữ liệu hàng loạt của DHS đặt ra câu hỏi về các giao thức an ninh mạng của Oregon . " Người Oregonian, ngày 24 tháng 6 năm 2019.

Cimpanu, C, "Dữ liệu của 645.000 người dân Oregon bị lộ sau khi chín nhân viên của DHS bị tấn công lừa đảo." ZD Net, ngày 21 tháng 6 năm 2019.

CIO. "Số liệu trong 'Khảo sát về khả năng phục hồi của State of1T' của IDC." Giám đốc điều hành, 2019.

Clark, P. "Marriott Breach bộc lộ điểm yếu trong phòng thủ mạng cho khách sạn." Bloomberg, ngày 14 tháng 12 năm 2018.

Colby, C. "Vi phạm dữ liệu của Yahoo: Cách gửi $358 trở lên dưới dạng Pan giải quyết khiếu nại." C/Net, ngày 15 tháng 10 năm 2019.

Corbin, K. "Những kẻ tấn công mạng Aurora thực sự đang chạy phản công." CIO, ngày 22 tháng 4 năm 2013.

phần mềm mạng. "Mọi thứ bạn cần biết về Chiến dịch Aurora," Cyware, 2019.

Nhân viên đọc sách tối. "Satya Nadella: Quyền riêng tư là quyền của con người." Đọc tối, ngày 25 tháng 1 năm 2019.

Davies, T. "Chuỗi khách sạn Marriott tiết lộ cuộc tấn công mạng lớn." Báo cáo PrivSec, ngày 3 tháng 12 năm 2018.

Davis, J. "Breach Tally of Oregon DHS Phishing Attack tiếp cận 645 nghìn bệnh nhân." Sức khỏe An ninh CNTT, 2019a.

Davis, J. "350.000 bệnh nhân, 2 triệu email bị lộ trong cuộc tấn công lừa đảo của DHS Oregon." Sức khỏe An ninh CNTT, 2019b,

Enright, A. "GDPR ở đây." DigitalCommeme360, ngày 24 tháng 5 năm 2018,

Fiegeman, S. "Verizon cho biết vi phạm lớn của Yahoo có thể ảnh hưởng đến thỏa thuận." CNN, ngày 13 tháng 10 năm 20

Fogg, S. "GDPR là gì? Khái niệm cơ bản về Quy định bảo vệ dữ liệu chung của EU." Hạn 26/6/2019.

Fugairon, A. "Quy định về bảo vệ quyền riêng tư và GDPR có liên quan như thế nào—và ý nghĩa của chúng đối với doanh nghiệp của bạn." Bảo mật PivotPoint, ngày 31 tháng 1 năm 2019.

Germain, T. "Luật bảo mật của Califomia cuối cùng cũng có hiệu lực Bây giờ thì sao?" Báo cáo của người tiêu dùng, tháng 1 năm 2020

Grothaus, M. "Google đã bị phạt 56,8 triệu đô la vì vi phạm Quy tắc GDPR của EU" Fast Company, ngày 22 tháng 1 năm 2019.

Hackett, R. "Vụ vi phạm dữ liệu Titanic của Yahoo làm nổi bật rủi ro đối với M&A." Vận may, ngày 23 tháng 9 năm 2016a.

Hackett, R. "Linkedln đã mất 167 triệu thông tin xác thực tài khoản trong Data Fortune, ngày 18 tháng 5 năm 2016b.

Hashim, A. "Pharma Giant Bayer thực hiện cuộc tấn công mạng được cho là do một nhóm tin tặc Trung Quốc thực hiện." Tin tức Hacking mới nhất, ngày 8 tháng 4 năm 2019.

ITRC„"Vi phạm dữ liệu năm 2019." Có sẵn từ https://www.idtheftcenterlo g/2019-data-breaches/ được truy cập vào ngày 28 tháng 2 năm 2020. 

Kan, M. "Tin tặc hiện có một kho tàng dữ liệu người dùng với vi phạm Yahoo." Nhóm Dữ liệu Quốc tế, ngày 22 tháng 9 năm 2016.

Kazeem, Y. "Kenya đang tăng cường bảo vệ dữ liệu kỹ thuật số của công dân bằng Luật bảo vệ dữ liệu mới lấy cảm hứng từ EU," Quartz Châu Phi, ngày 12 tháng 11 năm 2019.



Kiesnoski, K. "5 vụ vi phạm dữ liệu lớn nhất trên " CNBC. Ngày 30 tháng 7 năm 1019. Truy cập từ https://www.cnbc.com/2019/07/30/ five-of•the-biggest-data-breaches-ever.html vào ngày 6 tháng 7 năm 2020.

Lee, D. "Tin tặc 'Nhà nước' đã đánh cắp dữ liệu từ 500 triệu người dùng." BBC, ngày 23 tháng 9 năm 2016.

Matwyshyn, A., và H.Bhargava. "Vi phạm dữ liệu của Yahoo sẽ giúp đại tu bảo mật trực tuyến?" Knowledge@Wharton: Đại học Pennsylvania, ngày 27 tháng 9 năm 2016. Truy cập từ http://knowledge.wharton.upenn.edu/article/will-yahoos-data-breach-helpoverhaul-online-security/ vào ngày 6 tháng 7 năm 2020.

Murgia, M. "Các chuyên gia mạng tìm đến những kẻ tình nghi thông thường trong vụ hack Yahoo." Thời báo Tài chính, ngày 25 tháng 9 năm 2016.

O'Flaherty, K. "Vi phạm Marriott—Chuyện gì đã xảy ra, nó nghiêm trọng đến mức nào và ai bị ảnh hưởng." Forbes, ngày 30 tháng 11 năm 2018.

Obulutsa, G. và Miriri, D, "Kenya thông qua Luật bảo vệ dữ liệu quan trọng đối với đầu tư công nghệ." Reuters, ngày 8 tháng 11 năm 2019.

Porter, J. "Google bị phạt 50 triệu euro vì vi phạm GDPR ở Pháp." The Verge, ngày 21 tháng 1 năm 2019.

Rajagopal, A. "Sự cố trong tuần: Mục tiêu tấn công lừa đảo của Oregon DHS." Trung tâm an ninh mạng, ngày 2 tháng 6 năm 2019.

Reuters. "Kenya thông qua luật bảo vệ dữ liệu quan trọng đối với đầu tư công nghệ." Kinh tế Thnes CISC), ngày 11 tháng 11 năm 2019.

Schechner, S. "Google bị phạt 57 triệu đô la trong khoản tiền phạt lớn nhất theo luật mới của châu Âu." Tạp chí Phố Wall, ngày 21 tháng 1 năm 2019.

Schwartz, M. "Google Aurora Hack là hoạt động phản gián của Trung Quốc." Đọc Tối, ngày 21 tháng 5 năm 2013.

Clement, J. "Số lượng bản ghi dữ liệu bị xâm phạm trong các vụ vi phạm dữ liệu được chọn kể từ tháng 5 năm 2019." Statista, ngày 22 tháng 7 năm 2019.

Tyko, K. "Dàn xếp vi phạm dữ liệu của Yahoo 2019: Cách nhận tới $358 hoặc Giám sát tín dụng miễn phí." USA Today, ngày 14 tháng 10 năm 2019.

Verizon. "Báo cáo điều tra vi phạm dữ liệu năm 2019." Được truy cập từ: https://enterprise.verizon.com/resources/reports/dbir/2019.

Walker, J. "Truyền thông xã hội đã trở thành một rủi ro an ninh mạng ngày càng tăng đối với chúng ta." SMPerth, ngày 22 tháng 4 năm 2019.

Warfield, C, "Lỗ hổng vi phạm Equifax xuất hiện dưới dạng Cuộc tấn công mạng hàng đầu vào (23 năm 2019." WatchGuard, ngày 11 tháng 12 năm 2019.

Weiss, P. và Burger, L. "Bayer Chứa Cuộc tấn công Mạng Nó nói Mang Dấu ấn Trung Quốc." Reuters, ngày 4 tháng 4 năm 2019.



Người in: vovanhai@iuh.edu.vn. Việc in chỉ dành cho mục đích sử dụng cá nhân, riêng tư. Không phần nào của cuốn sách này có thể được sao chép hoặc truyền đi mà không có sự cho phép trước của nhà xuất bản. Những người vi phạm sẽ bị truy tố.