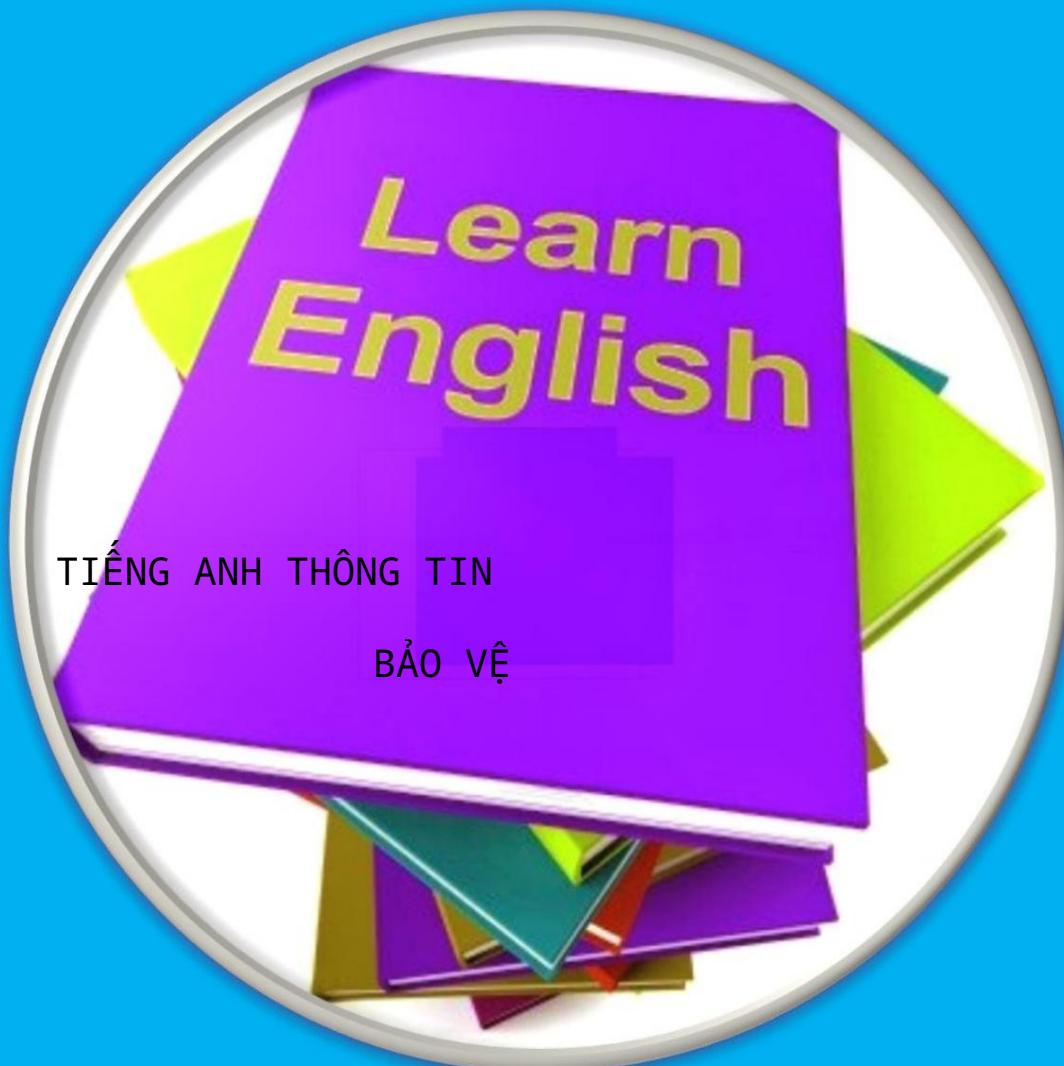


HỌC VIỆN KỸ THUẬT MẶT MẠI

ThS. MAI THỊ HÀO



HỌC VIỆN KỸ THUẬT MẶT MẠI

ThS. MAI THỊ HẢO

TIẾNG ANH AN TOÀN THÔNG TIN

(DÀNH CHO BẢN MẶT VÀ LƯU HÀNH NỘI BỘ)

MỤC LỤC

MỤC LỤC	tôi
---------------	-----

SỰ NHÌN NHẬN	v
GIỚI THIỆU.....	vii
BÀI 1: GIỚI THIỆU VỀ BẢO MẬT THÔNG TIN.....	1
Lịch sử bảo mật thông tin	1
Bảo mật là gì?	9
Các đặc tính quan trọng của thông tin	16
Các thành phần của an toàn thông tin	22
Vòng đời phát triển hệ thống	29
BÀI 2: NHU CẦU BẢO MẬT.....	33
Các môi đe dọa (1)	33
Đe dọa (2)	41
Các cuộc tấn công (1)	47
Các cuộc tấn công (2)	53
Tấn công mạng	60
BÀI 3: TƯ ỜNG LỬA	62
Tư ờng lửa	62
Tư ờng lửa được phân loại theo cấu trúc	67
Kiến trúc tư ờng lửa	72
Chế độ xử lý tư ờng lửa (1)	79
Các chế độ xử lý tư ờng lửa (2)	85
Bộ lọc nội dung	87
BÀI 4: CÔNG NGHỆ AN NINH	89
Hệ thống phát hiện và ngăn chặn xâm nhập	89
Hệ thống phát hiện xâm nhập mạng & Hệ thống phát hiện xâm nhập dựa trên máy chủ	94
Các phương pháp phát hiện IDPS	99
Honeypots, Honeypets và các hệ thống tέ bào đέm	104
BÀI 5: GIỚI THIỆU VỀ MẬT MẠI	110
Mật mã là gì?	110

Cơ sở của mật mã	135
Một số thuật ngữ và khái niệm cơ bản về mật mã	123
Người tham gia truyền thông	129
BÀI 6: MẬT MẠI HIỆN ĐẠI	135
Các hàm băm	135
Mã hóa đối xứng	141
Mã hóa bất đối xứng	146
Cơ sở hạ tầng khóa công khai	151
Các cuộc tấn công vào hệ thống mật mã	157
Chữ ký số	163
BÀI 7: AN NINH VẬT LÝ	166
Kiểm soát truy cập vật lý	167
An ninh và an toàn phòng cháy chữa cháy	178
Thất bại trong việc hỗ trợ các tiện ích và sụp đổ cấu trúc	185
Đánh chặn dữ liệu	194
ĐƠN VỊ 8: TRIỂN KHAI BẢO MẬT THÔNG TIN	201
Quản lý dự án an toàn thông tin	202
Các cản nhắc về lập kế hoạch dự án	208
Các khía cạnh kỹ thuật của việc thực hiện	216
danh sách các từ	223
Người giới thiệu	235

SỰ NHÌN NHẬN

Tác giả xin chân thành cảm ơn Khoa Thông tin

An ninh, các giảng viên trong khoa, các bác sĩ và chuyên gia chuyên ngành thông tin security vì đã giúp đỡ rất nhiều trong việc biên soạn giáo trình này. Ngoài ra, tôi muốn xin đặc biệt cảm ơn giáo sư, tiến sĩ triết học Lư ơng Thế Dũng
người đã cung cấp cho tôi những tài liệu rất hữu ích và giúp tôi hoàn thành đề tài nghiên cứu.

Tác giả cũng xin bày tỏ lòng biết ơn sâu sắc tới Ban lãnh đạo Công ty
Học viện Kỹ thuật Mật mã, Khoa Khoa học Cơ bản và
Khoa Tiếng Anh đã hỗ trợ tận tình trong việc biên soạn tài liệu này
sách khóa học.

Mặc dù giáo trình Tiếng Anh chuyên ngành An toàn thông tin được biên soạn cho lần thứ hai, không thể không mắc sai lầm ngoài ý muốn. Vì vậy, ý kiến từ tất cả các độc giả về cuốn sách này luôn được hoan nghênh và đánh giá cao.

Tác giả

GIỚI THIỆU

Đây là lần biên soạn thứ hai của bộ giáo trình Tiếng Anh chuyên ngành An toàn thông tin với những điểm mới và nổi bật. Thứ nhất, kiến thức trong sách không quá khó đối với học sinh và giáo viên. Thứ hai, các cấu trúc ngữ pháp, cấu tạo từ và kiến thức về các phần của bài phát biểu đư ợc cung cấp thông qua tiếng Anh tổng quát học trong tiếng Anh 1, tiếng Anh 2 và tiếng Anh 3 không đư ợc cung cấp. Thứ ba, cuốn sách này giúp học sinh cải thiện các kỹ năng ngôn ngữ khác nhau, trong đó đọc hiểu, dịch và nói là ưu tiên hàng đầu. Hơn nữa, các chủ đề trong sách rất gần gũi với học sinh, đặc biệt gần như liên quan đến kiến thức cơ bản trong lĩnh vực an toàn thông tin, giúp tạo động lực cho các em trong việc học tiếng Anh trên lớp. Cuối cùng, sự kết hợp khéo léo của bốn kỹ năng ngôn ngữ bao gồm Đọc, Nói, Nghe và Viết cũng đư ợc giới thiệu.

Giáo trình này đư ợc biên soạn dành cho sinh viên năm thứ tư Học viện Kỹ thuật Mật mã chuyên ngành An toàn thông tin đã hoàn thành giáo trình Tiếng Anh phổ thông.

Ngoài ra, tài liệu này còn cung cấp cho sinh viên một số lượnq lớn các bài văn với nhiều loại từ vựng cơ bản thư ờng dùng trong lĩnh vực an toàn thông tin, giúp sinh viên tiếp cận với các kiến thức chuyên ngành. Các hoạt động đư ợc đưa ra trư ớc, trong và sau mỗi văn bản để sinh viên có thể đọc, hiểu, thảo luận về các chủ đề chuyên ngành bằng tiếng Anh và tự tin giao tiếp với nhau, tránh cảm giác bỡ ngỡ, bỡ ngỡ khi thảo luận hoặc tham dự hội thảo bằng tiếng Anh. Bên cạnh đó, học sinh có thể thực hành tóm tắt các bài đọc bằng lời của mình và trình bày một cái nhìn nhanh về nội dung đư ợc cung cấp trên lớp.

Cuốn sách khóa học đư ợc chia thành 8 đơn vị với các chủ đề khác nhau. Mỗi đơn vị khoảng một cụ thể và tập trung vào các kỹ năng ngôn ngữ khác nhau như sau:

1. ĐỌC VÀ NÓI: Phần này có từ 3 đến 4 đoạn văn liên quan đến các chủ đề khác nhau. Nhiệm vụ đọc trư ớc với các câu hỏi khác nhau đư ợc đưa ra trư ớc mỗi văn bản, giúp học sinh làm quen với chủ đề của bài học mà các em sẽ giải quyết sau này. Các nhiệm vụ trong khi đọc và sau khi đọc với các hoạt động cũng đư ợc cung cấp sau mỗi văn bản nhằm giúp học sinh phát triển kỹ năng đọc hiểu và giao tiếp.

2. VIẾT VÀ NÓI: Phần này bao gồm các nhiệm vụ hoặc hoạt động liên quan đến các chủ đề và nội dung của từng đơn vị giúp học sinh phát triển kỹ năng viết và nói

3. LISTENING: Một số liên kết video đư ợc cung cấp ở cuối mỗi bài học để Học sinh không những đư ợc củng cố kiến thức trong bài học mà còn đư ợc cải thiện kỹ năng nghe của họ.

Tài liệu dùng để biên soạn giáo trình này đư ợc lấy từ sách của các tác giả Anh, Mỹ đảm bảo tính chính xác, văn phong chuẩn của người bản ngữ hoặc lấy từ các trang web, tạp chí học thuật.

BÀI 1: GIỚI THIỆU VỀ BẢO MẬT THÔNG TIN

ĐỌC VÀ NÓI 1

1. Thảo luận các câu hỏi

1. Thông tin có cần bảo vệ? Thông tin nào cần được bảo vệ?
2. Thông tin đó phải được bảo vệ khi nào?
3. Bạn nghĩ những lĩnh vực nào liên quan đến bảo mật thông tin?
4. An toàn thông tin ra đời khi nào?
5. Bạn nghĩ an toàn thông tin có những giai đoạn lịch sử nào có kinh nghiệm?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Lịch sử bảo mật thông tin

Lịch sử bảo mật thông tin bắt đầu với bảo mật máy tính. Nhu cầu về bảo mật máy tính - tức là nhu cầu bảo vệ các vị trí thực tế, phần cứng và phần mềm khỏi các mối đe dọa - nảy sinh trong Thế chiến II khi các máy tính lớn đầu tiên, được phát triển để hỗ trợ tính toán cho việc phá mã giao tiếp ([xem Hình 1-1](#)), được đưa vào sử dụng. Nhiều cấp độ bảo mật đã được triển khai để bảo vệ các máy tính lớn này và duy trì tính toàn vẹn của dữ liệu của chúng. Ví dụ, việc tiếp cận các địa điểm quân sự nhạy cảm được kiểm soát bằng huy hiệu, chìa khóa và nhận dạng khuôn mặt của nhân viên được ủy quyền bởi nhân viên bảo vệ. Nhu cầu ngày càng tăng để duy trì an ninh quốc gia cuối cùng đã dẫn đến các biện pháp bảo vệ an ninh máy tính phức tạp hơn và phức tạp hơn về mặt công nghệ.

Trong những năm đầu tiên này, bảo mật thông tin là một quy trình đơn giản bao gồm chủ yếu là bảo mật vật lý và các lược đồ phân loại tài liệu đơn giản. Các mối đe dọa chính đối với an ninh là hành vi trộm cắp thiết bị, gián điệp chống lại các sản phẩm của hệ thống và phá hoại. Một trong những sự cố bảo mật được ghi lại đầu tiên năm ngoài các danh mục này xảy ra vào đầu những năm 1960, khi một quản trị viên hệ thống đang làm việc trên tệp MOTD (tin nhắn trong ngày) và một quản trị viên khác đang chỉnh sửa tệp mật khẩu. Một trực trặc phần mềm đã trộn lẫn hai tệp và toàn bộ tệp mật khẩu được in trên mọi tệp đầu ra.



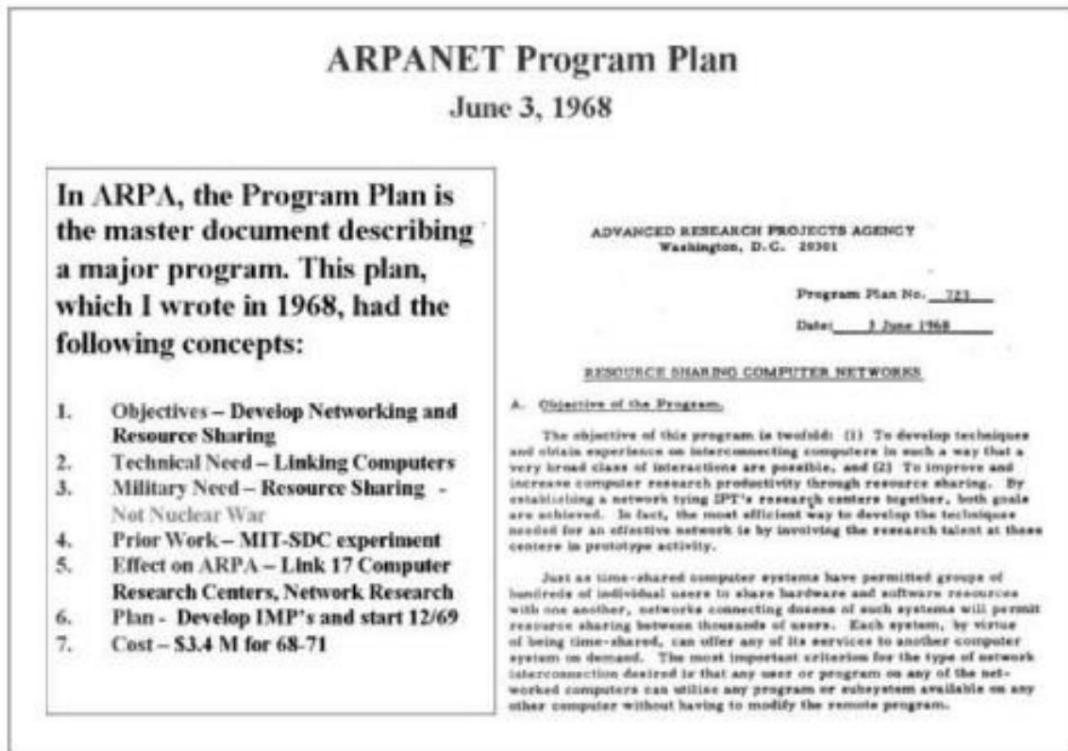
Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."¹

Hình 1-1. bí ẩn

Những năm 1960

Trong Chiến tranh Lạnh, nhiều máy tính lớn hơn đã được đưa lên mạng để thực hiện các nhiệm vụ phức tạp và phức tạp hơn. Điều cần thiết là phải cho phép các máy tính lớn này giao tiếp thông qua một quy trình ít rủi ro hơn so với việc gửi băng từ giữa các trung tâm máy tính. Để đáp ứng nhu cầu này, Cơ quan Dự án Nghiên cứu Tiên tiến của Bộ Quốc phòng (ARPA) bắt đầu kiểm tra tính khả thi của một hệ thống thông tin liên lạc nối mạng dự phòng để hỗ trợ trao đổi thông tin của quân đội. Larry Roberts, được biết đến là người sáng lập ra Internet, đã phát triển dự án có tên ARPANET ngay từ khi mới thành lập.

ARPANET là tiền thân của Internet (xem [hình 1-2](#). để biết ngoại lệ từ Kế hoạch Chu trình ARPA-NET).



Hình 1-2. Phát triển kế hoạch chung của chương trình ARPANET

Những năm 1970 và 80

Trong thập kỷ tiếp theo, ARPANET trở nên phổ biến và được sử dụng rộng rãi hơn, đồng thời khả năng lạm dụng nó ngày càng tăng. Vào tháng 12 năm 1973, Robert M. "Bob" Metcalfe, người đã phát triển Ethernet, một trong những giao thức mạng phổ biến nhất, đã xác định các vấn đề cơ bản với bảo mật ARPANET.

Các trang web từ xa riêng lẻ không có đủ quyền kiểm soát và biện pháp bảo vệ để bảo vệ dữ liệu khỏi những người dùng từ xa trái phép. Có rất nhiều vấn đề khác: lỗ hổng của cấu trúc và định dạng mật khẩu; thiếu các thủ tục an toàn cho các kết nối quay số; và không tồn tại nhận dạng người dùng và ủy quyền cho hệ thống. Các số điện thoại được phân phối rộng rãi và công khai trên tường của các bốt điện thoại, giúp tin tức dễ dàng truy cập ARPANET. Do phạm vi và tầm suất vi phạm an ninh máy tính cũng như sự bùng nổ về số lượng máy chủ và người dùng trên ARPANET, an ninh mạng được gọi là "mất an ninh mạng". Năm 1978, một nghiên cứu nổi tiếng mang tên "Phân tích bảo vệ: Báo cáo cuối cùng" đã được xuất bản. Nó tập trung vào một dự án do ARPA thực hiện để khám phá các lỗ hổng bảo mật của hệ điều hành. Đối với dòng thời gian bao gồm nghiên cứu này và các nghiên cứu quan trọng khác về bảo mật máy tính.

Phong trào hưng túc an ninh vượt ra ngoài việc bảo vệ các vị trí thực tế bắt đầu bằng một bài báo do Bộ Quốc phòng tài trợ, Báo cáo Rand R-609, đã có gắng xác định nhiều biện pháp kiểm soát và cơ chế cần thiết để bảo vệ hệ thống máy tính đa cấp. Tài liệu đã được phân loại trong gần mươi năm và hiện được coi là bài báo bắt đầu nghiên cứu về bảo mật máy tính.

Sự an toàn hoặc thiếu an ninh của các hệ thống chia sẻ tài nguyên bên trong Bộ Quốc phòng đã được các nhà nghiên cứu chú ý vào mùa xuân và mùa hè năm 1967. Vào thời điểm đó, các hệ thống đang được mua với tốc độ nhanh chóng và việc bảo vệ chúng là một nhiệm vụ cấp bách. Mọi quan tâm cho cả quân đội và các nhà thầu quốc phòng.

Vào tháng 6 năm 1967, Cơ quan Dự án Nghiên cứu Tiên tiến đã thành lập một nhóm đặc nhiệm để nghiên cứu quy trình bảo mật các hệ thống thông tin được phân loại. Lực lượng Đặc nhiệm được tập hợp vào tháng 10 năm 1967 và họp thường xuyên để đưa ra các khuyến nghị, những khuyến nghị này cuối cùng đã trở thành nội dung của Báo cáo Rand R-609.

Báo cáo Rand R-609 là tài liệu được công bố rộng rãi đầu tiên xác định vai trò của quản lý và các vấn đề chính sách trong bảo mật máy tính. Nó lưu ý rằng việc sử dụng rộng rãi các thành phần mạng trong các hệ thống thông tin trong quân đội đã gây ra các rủi ro bảo mật không thể giảm thiểu bằng các biện pháp thông thường sau đó được sử dụng để bảo mật các hệ thống này. Bài viết này báo hiệu một thời điểm quan trọng trong lịch sử bảo mật máy tính - khi phạm vi bảo mật máy tính được mở rộng đáng kể từ sự an toàn của các vị trí thực tế và phần cứng để bao gồm những điều sau:

- Bảo mật dữ liệu
- Hạn chế truy cập ngẫu nhiên và trái phép vào dữ liệu đó
- Thu hút nhân sự từ nhiều cấp độ của tổ chức trong các vấn đề liên quan đến bảo mật thông tin

ĐA NĂNG

Phần lớn các nghiên cứu ban đầu về bảo mật máy tính tập trung vào một hệ thống có tên là Dịch vụ Điện toán và Thông tin Đa kênh (MULTICS). Mặc dù hiện tại nó đã lỗi thời như ng MULTICS vẫn đáng chú ý vì đây là hệ điều hành đầu tiên tích hợp bảo mật vào các chức năng cốt lõi của nó. Đó là một máy tính lớn, chia sẻ thời gian

hệ điều hành được phát triển vào giữa những năm 1960 bởi một tập đoàn gồm General Electric (GE), Bell Labs và Viện Công nghệ Massachusetts (MIT).

Vào giữa năm 1969, không lâu sau khi tái cấu trúc dự án MULTICS, một số nhà phát triển của nó (Ken Thompson, Dennis Ritchie, Rudd Canada và Doug McElroy) đã tạo ra một hệ điều hành mới có tên là UNIX. Trong khi hệ thống MULTICS triển khai nhiều cấp độ bảo mật và mật khẩu, hệ thống UNIX thì không. Chức năng chính của nó, xử lý văn bản, không yêu cầu mức độ bảo mật giống như người tiền nhiệm của nó. Trên thực tế, mãi cho đến đầu những năm 1970, ngay cả thành phần bảo mật đơn giản nhất, chức năng mật khẩu, cũng trở thành một phần của UNIX.

Vào cuối những năm 1970, bộ vi xử lý đã mang đến máy tính cá nhân và một kỷ nguyên mới của máy tính. PC đã trở thành con ngựa thồ của điện toán hiện đại, do đó đưa nó ra khỏi trung tâm dữ liệu. Sự phi tập trung hóa các hệ thống xử lý dữ liệu này vào những năm 1980 đã tạo ra kết nối mạng - tức là sự kết nối giữa các máy tính cá nhân và máy tính lớn, cho phép toàn bộ cộng đồng máy tính làm cho tất cả các tài nguyên của họ hoạt động cùng nhau.

những năm 1990

Vào cuối thế kỷ 20, các mạng máy tính trở nên phổ biến hơn, cũng như nhu cầu kết nối các mạng này với nhau. Điều này đã tạo ra Internet, mạng toàn cầu đầu tiên của các mạng. Internet đã được cung cấp cho công chúng vào những năm 1990, trước đây là lĩnh vực của chính phủ, học viện và các chuyên gia tận tâm trong ngành. Internet mang lại khả năng kết nối cho hầu như tất cả các máy tính có thể kết nối với đường dây điện thoại hoặc mạng cục bộ (LAN) được kết nối Internet. Sau khi Internet được thươn mại hóa, công nghệ này đã trở nên phổ biến, tiếp cận hầu hết mọi nơi trên thế giới với phạm vi sử dụng ngày càng rộng.

Kể từ khi bắt đầu như một công cụ để chia sẻ thông tin của Bộ Quốc phòng, Internet đã trở thành một kết nối của hàng triệu mạng. Lúc đầu, các kết nối này dựa trên các tiêu chuẩn thực tế, bởi vì các tiêu chuẩn ngành về kết nối mạng không tồn tại vào thời điểm đó. Những tiêu chuẩn thực tế này đã làm rất ít để đảm bảo tính bảo mật của thông tin mặc dù các công nghệ tiên thân này được áp dụng rộng rãi và trở thành tiêu chuẩn của ngành, một số mức độ bảo mật đã được đưa ra. Tuy nhiên, việc triển khai Internet sớm coi bảo mật là ưu tiên thấp. Trên thực tế, nhiều vấn đề gây khó khăn cho e-mail trên Internet ngày nay là kết quả

về sự thiếu an toàn ban đầu này. Vào thời điểm đó, khi tất cả người dùng Internet và e-mail đều là các nhà khoa học máy tính (có lẽ là đáng tin cậy), việc xác thực máy chủ thư và mã hóa e-mail đương như không cần thiết. Các phương pháp điện toán ban đầu dựa vào bảo mật được tích hợp trong môi trường vật lý của trung tâm dữ liệu chứa máy tính. Khi các máy tính nối mạng trở thành kiểu máy tính thống trị, khả năng bảo mật vật lý cho một máy tính nối mạng đã mất đi và thông tin được lưu trữ nên dễ bị đe dọa hơn trước các mối đe dọa bảo mật.

2000 đến nay

Ngày nay, Internet đưa hàng triệu máy tính không an toàn liên lạc với nhau liên tục. Tính bảo mật của thông tin được lưu trữ của mỗi máy tính hiện phụ thuộc vào mức độ bảo mật của mọi máy tính khác mà nó được kết nối. Những năm gần đây, nhận thức ngày càng tăng về nhu cầu cải thiện an ninh thông tin, cũng như nhận thức rằng an ninh thông tin là quan trọng đối với quốc phòng. Mỗi đe dọa ngày càng tăng của các cuộc tấn công mạng đã khiến các chính phủ và công ty nhận thức rõ hơn về nhu cầu bảo vệ các hệ thống điều khiển do máy tính điều khiển của các tiện ích và cơ sở hạ tầng quan trọng khác. Ngoài ra còn có mối lo ngại ngày càng tăng về việc các quốc gia tham gia vào cuộc chiến thông tin và khả năng các hệ thống thông tin cá nhân và doanh nghiệp có thể trở thành thư ngỏ nếu chúng không được bảo vệ.

2.1. Trả lời các câu hỏi

1. Ai được coi là người sáng lập ra Internet? Ông đã phát triển những gì?
2. Việc tiếp cận các địa điểm quân sự nhạy cảm được kiểm soát như thế nào trong Thế giới Chiến tranh II?
3. Nghiên cứu nổi tiếng mang tên "Phân tích bảo vệ: Báo cáo cuối cùng" ra đời khi nào? được phát hành? Nó đã tập trung vào cái gì? Tại sao?
4. Sự khác biệt giữa hệ thống MULTICS và hệ thống UNIX là gì?
5. Internet trở thành kết nối của hàng triệu mạng từ bao giờ và tại sao?
6. Điều gì dẫn đến sự phức tạp hơn và tinh vi hơn về mặt công nghệ biến pháp bảo vệ an ninh máy tính trước?

7. Từ khi nào công nghệ trở nên phổ biến, đến gần như mọi ngõ ngách của toàn cầu với một mảng sử dụng ngày càng mở rộng?
8. Điều gì đã khiến các chính phủ và công ty nhận thức rõ hơn về nhu cầu bảo vệ các hệ thống điều khiển do máy tính điều khiển của các tiện ích và các cơ sở hạ tầng quan trọng?
- 2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa lỗi sai (F)
1. Tính bảo mật của thông tin được lưu trữ của mỗi máy tính hiện phụ thuộc vào mức độ bảo mật của mọi máy tính khác mà nó được kết nối.
 A. Đúng B. Sai C. NI
 2. Ken Thompson, Dennis Ritchie, Rudd Canada và Doug McElroy là những người phát minh ra Dịch vụ Điện toán và Thông tin Đa kênh.
 A. Đúng B. Sai C. NI
 3. "Phân tích Bảo vệ: Báo cáo Cuối cùng" là tài liệu được công bố rộng rãi đầu tiên xác định vai trò của quản lý và các vấn đề chính sách trong bảo mật máy tính.
 A. Đúng B. Sai C. NI
 4. Lập kế hoạch và phát triển ban đầu cho MULTICS bắt đầu vào năm 1964, tại Cambridge, Massachusetts. Ban đầu nó là một dự án hợp tác do MIT dẫn đầu.
 A. Đúng B. Sai C. NI
 5. Tổ chuyên trách do Cơ quan Dự án Nghiên cứu Tiên tiến thành lập để nghiên cứu quy trình bảo mật hệ thống thông tin mật.
 A. Đúng B. Sai C. NI
 6. Truy cập vào ARPANET được mở rộng vào năm 1981, khi Quỹ Khoa học Quốc gia tài trợ cho Mạng Khoa học Máy tính.
 A. Đúng B. Sai C. NI
- 2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau
1., mạng máy tính trở nên phổ biến hơn, cũng như nhu cầu để kết nối các mạng này với nhau.
 A. Vào cuối thế kỷ 20 C. Vào giữa những năm 1960.

- B. Cuối những năm 1970. D. Trong Chiến tranh Lạnh
2. Các mối đe dọa chính đối với an ninh là
A. phá hoại
B. trộm cắp vật chất của thiết bị
C. gián điệp chôngh lại các sản phẩm của hệ thống
D. Tất cả đều đúng
- 3..... chức năng chính, xử lý văn bản, không yêu cầu giống mức độ bảo mật như của người tiền nhiệm của nó.
A. ARPANET C. ĐA'
B. ARPA D. UNIX
4. Các cách tiếp cận điện toán ban đầu dựa trên
A. lý thuyết bảo mật thông tin và mật mã.
B. bảo mật được tích hợp vào môi trường vật lý của dữ liệu trung tâm chứa các máy tính.
C. mối đe dọa ngày càng tăng của các cuộc tấn công mạng.
D. mức độ bảo mật của mọi máy tính.
5. An ninh mạng được gọi là mảnh an ninh mạng.....phạm vi và tần suất vi phạm an ninh máy tính và sự bùng nổ về số lượng máy chủ và người dùng trên ARPANET.
A. Vì C. Do đó
B. Tuy nhiên D. Mặc dù
3. Nói
1. Thông tin chính nào trong từng thời kỳ của lịch sử thông tin an ninh bạn nhận được?
2. Trình bày sơ lược về lịch sử bảo mật thông tin.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi

1. Bảo mật là gì?
2. Bảo mật thông tin là gì?
3. Bạn biết những thành phần nào của bảo mật thông tin?
4. An toàn thông tin liên quan đến những lĩnh vực nào?

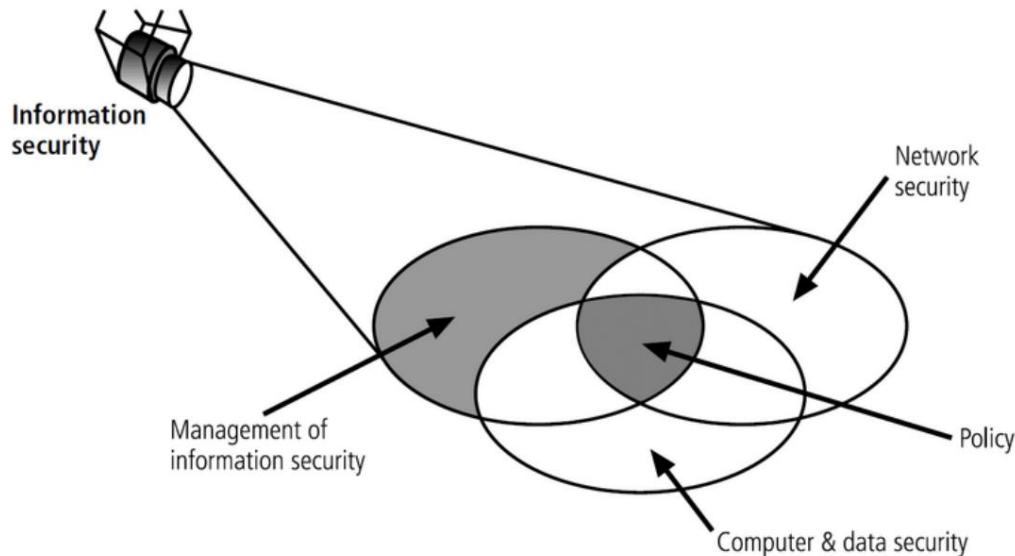
2. Đọc sơ lược về lịch sử mật mã và thực hiện các nhiệm vụ bên dưới

Bảo mật là gì?

Nói chung, an ninh là “chất lượng hoặc trạng thái an toàn để không bị nguy hiểm”. Nói cách khác, mục tiêu là bảo vệ chống lại kẻ thù khỏi những kẻ sẽ làm hại, dù cố ý hay không. Ví dụ, an ninh quốc gia là một hệ thống nhiều lớp nhằm bảo vệ chủ quyền của một quốc gia, tài sản, nguồn lực và người dân của quốc gia đó. Đạt được mức độ bảo mật thích hợp cho một tổ chức cũng đòi hỏi một hệ thống nhiều mặt. Một tổ chức thành công nên có sẵn nhiều lớp bảo mật sau đây để bảo vệ hoạt động của mình:

- Bảo mật vật lý, để bảo vệ các đồ vật, đồ vật hoặc khu vực khỏi bị truy cập trái phép và sử dụng sai mục đích
- An ninh nhân sự, để bảo vệ cá nhân hoặc nhóm người
được phép truy cập vào tổ chức và các hoạt động của nó
- Bảo mật hoạt động, để bảo vệ các chi tiết của một hoạt động cụ thể hoặc chuỗi hoạt động
- Bảo mật truyền thông, để bảo vệ phương tiện truyền thông,
công nghệ và nội dung
- An ninh mạng, để bảo vệ các thành phần mạng, kết nối và
nội dung
- Bảo mật thông tin, để bảo vệ tính bảo mật, tính toàn vẹn và
tính sẵn có của tài sản thông tin, cho dù trong lưu trữ, xử lý hoặc truyền
tải. Nó đạt được thông qua việc áp dụng chính sách, giáo dục, đào tạo và
nhận thức, và công nghệ.

Ủy ban về Hệ thống An ninh Quốc gia (CNSS) định nghĩa bảo mật thông tin là bảo vệ thông tin và các yếu tố quan trọng của nó, bao gồm các hệ thống và phần cứng sử dụng, lưu trữ và truyền thông tin đó. **Hình 1-3** cho thấy bảo mật thông tin bao gồm các lĩnh vực rộng lớn về quản lý bảo mật thông tin, bảo mật máy tính và dữ liệu cũng như bảo mật mạng. Mô hình bảo mật thông tin CNSS phát triển từ một khái niệm được phát triển bởi ngành công nghiệp bảo mật máy tính có tên là tam giác CIA. Tam giác CIA đã trở thành tiêu chuẩn công nghiệp cho bảo mật máy tính kể từ khi máy tính lớn được phát triển. Nó dựa trên ba đặc điểm của thông tin mang lại giá trị cho tổ chức: tính bảo mật, tính toàn vẹn và tính sẵn sàng. Tính bảo mật của ba đặc điểm thông tin này ngày nay vẫn quan trọng như trước đây, như mô hình tam giác CIA không còn giải quyết thỏa đáng môi trường thay đổi liên tục. Các mối đe dọa đối với tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin đã phát triển thành một tập hợp lớn các sự kiện, bao gồm thiệt hại vô tình hoặc cố ý, phá hủy, trộm cắp, sửa đổi ngoài ý muốn hoặc trái phép hoặc các hành vi lạm dụng khác từ các mối đe dọa của con người hoặc không phải con người. Mỗi trường mới với nhiều mối đe dọa liên tục phát triển này đã thúc đẩy sự phát triển của một mô hình mạnh mẽ hơn nhằm giải quyết sự phức tạp của môi trường bảo mật thông tin hiện tại.



Hình 1-3: Các thành phần của An toàn thông tin

Khái niệm và thuật ngữ bảo mật thông tin chính

- Truy cập: Khả năng sử dụng, thao tác, sửa đổi hoặc

ánh hư ờng đến chủ thẻ hoặc đối tư ợng khác. Người dùng đư ợc ủy quyền có quyền truy cập hợp pháp vào hệ thống, trong khi tin tặc có quyền truy cập bất hợp pháp vào hệ thống. Kiểm soát truy cập quy định khả năng này.

- Tài sản: Tài nguyên của tổ chức đang đư ợc bảo vệ. Một tài sản có thể logic, chẳng hạn như trang Web, thông tin hoặc dữ liệu; hoặc một tài sản có thể là vật chất, chẳng hạn như con người, hệ thống máy tính hoặc đối tư ợng hữu hình khác. Tài sản, đặc biệt là tài sản thông tin, là trọng tâm của các nỗ lực bảo mật; chúng là những gì mà những nỗ lực đó đang cố gắng bảo vệ.

- Tấn công: Một hành động cố ý hoặc vô ý có thể gây thiệt hại cho hoặc mặt khác làm tổn hại thông tin và/hoặc các hệ thống hỗ trợ thông tin đó. Các cuộc tấn công có thể chủ động hoặc bị động, cố ý hoặc vô ý, trực tiếp hoặc gián tiếp. Ai đó tình cờ đọc thông tin nhạy cảm không nhằm mục đích sử dụng của họ là một cuộc tấn công thụ động.

Một hacker cố gắng đột nhập vào một hệ thống thông tin là một cuộc tấn công có chủ đích. Sét đánh gây ra hỏa hoạn trong tòa nhà là một cuộc tấn công không có ý. Tấn công trực tiếp là việc hacker sử dụng máy tính cá nhân để đột nhập vào một hệ thống. Một cuộc tấn công gián tiếp là một tin tặc xâm phạm một hệ thống và sử dụng nó để tấn công các hệ thống khác, chẳng hạn như một phần của mạng botnet (tiếng lóng của mạng rô-bốt). Nhóm máy tính bị xâm nhập này, chạy phần mềm do kẻ tấn công lựa chọn, có thể hoạt động độc lập hoặc dư ới sự kiểm soát trực tiếp của kẻ tấn công để tấn công hệ thống và đánh cắp thông tin người dùng hoặc tiến hành các cuộc tấn công từ chối dịch vụ phân tán. Các cuộc tấn công trực tiếp bắt nguồn từ chính mối đe dọa. Các cuộc tấn công gián tiếp bắt nguồn từ một hệ thống hoặc tài nguyên bị xâm nhập đang gặp trực tiếp hoặc hoạt động dư ới sự kiểm soát của một mối đe dọa.

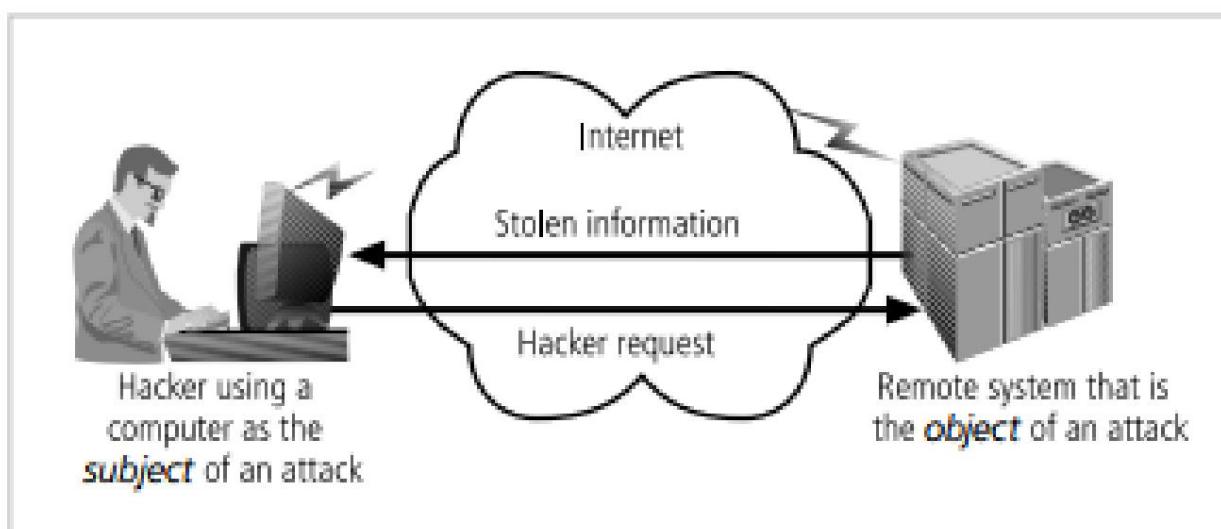
- Kiểm soát, bảo vệ hoặc biện pháp đối phó: Cơ chế bảo mật, chính sách hoặc quy trình có thể chống lại thành công các cuộc tấn công, giảm thiểu rủi ro, giải quyết các lỗ hổng và mặt khác cải thiện bảo mật trong một tổ chức.
- Khai thác: Một kỹ thuật đư ợc sử dụng để thỏa hiệp một hệ thống. Thuật ngữ này có thể là một động từ hoặc một danh từ. Các tác nhân đe dọa có thể cố gắng khai thác một hệ thống hoặc thông tin khác bằng cách sử dụng nó một cách bất hợp pháp vì lợi ích cá nhân của họ. Hoặc, khai thác có thể là một quy trình đư ợc ghi lại để tận dụng lỗ hổng bảo mật hoặc khả năng lộ diện, thư ờng là trong phần mềm, vốn có trong phần mềm hoặc do kẻ tấn công tạo ra. Khai thác tận dụng các công cụ phần mềm hiện có hoặc các thành phần phần mềm tùy chỉnh.

- Phơi nhiễm: Tình trạng hoặc trạng thái bị phơi nhiễm trong thông tin bảo mật, tiếp xúc tồn tại khi có lỗ hổng mà kẻ tấn công biết đến.
- Mất mát: Một trường hợp đơn lẻ của một tài sản thông tin bị thiệt hại hoặc sửa đổi hoặc tiết lộ ngoài ý muốn hoặc trái phép. Khi thông tin của một tổ chức bị đánh cắp, nó đã bị tổn thất.
- Hồ sơ bảo vệ hoặc tư thế bảo mật: Toàn bộ bộ điều khiển và các biện pháp bảo vệ, bao gồm chính sách, giáo dục, đào tạo và nâng cao nhận thức cũng như công nghệ mà tổ chức thực hiện (hoặc không thực hiện) để bảo vệ tài sản. Các thuật ngữ này đôi khi được sử dụng thay thế cho thuật ngữ chươn trình bảo mật, mặc dù chươn trình bảo mật thường bao gồm các khía cạnh quản lý về bảo mật, bao gồm lập kế hoạch, nhân sự và các chươn trình cấp dưới.

- Rủi ro: Khả năng xảy ra điều gì đó không mong muốn.

Các tổ chức phải giảm thiểu rủi ro để phù hợp với khẩu vị rủi ro của họ—số lượng và bản chất của rủi ro mà tổ chức sẵn sàng chấp nhận.

- Chủ thể và đối tượng : Một máy tính có thể là chủ thể của một tấn công—một thực thể tác nhân được sử dụng để tiến hành tấn công—hoặc đối tượng của một cuộc tấn công—thực thể mục tiêu, như trong [Hình 1-4](#). Một máy tính có thể vừa là đối tượng vừa là đối tượng của một cuộc tấn công, chẳng hạn như khi nó bị xâm phạm bởi một cuộc tấn công (đối tượng), và sau đó được sử dụng để tấn công các hệ thống khác (đối tượng).



[Hình 1-4. Máy tính là đối tượng và đối tượng của một cuộc tấn công](#)

• Đe dọa: Một loại đe dọa, nguy hiểm hoặc thực thể khác hiện một nguy hiểm đối với một tài sản. Các mối đe dọa luôn hiện hữu và có thể có mục đích hoặc vô hưng. Ví dụ: tin tặc có tình đe dọa các hệ thống thông tin không được bảo vệ, trong khi các cơ sở nghiêm trọng vô tình đe dọa các tòa nhà và nội dung của chúng.

• Tác nhân đe dọa: Trừ ờng hợp cụ thể hoặc một thành phần của mối đe dọa. Vì ví dụ, tất cả các tin tặc trên thế giới đều là mối đe dọa tập thể, trong khi Kevin Mitnick, người bị kết án vì xâm nhập vào hệ thống điện thoại, là một tác nhân đe dọa cụ thể. Tự ờng tự như vậy, sét đánh, mưa đá hoặc lốc xoáy là tác nhân đe dọa nằm trong mối đe dọa của các cơ sở nghiêm trọng.

• Lỗ hổng bảo mật: Điểm yếu hoặc lỗi trong hệ thống hoặc bảo vệ cơ chế mở nó để tấn công hoặc thiệt hại. Một số ví dụ về lỗ hổng bảo mật là lỗ hổng trong gói phần mềm, cổng hệ thống không được bảo vệ và cửa không khóa. Một số lỗ hổng nổi tiếng đã được kiểm tra, ghi lại và xuất bản; những người khác vẫn còn tiềm ẩn (hoặc chưa được khám phá).

2.1. Trả lời các câu hỏi

1. An toàn thông tin bao gồm những lĩnh vực nào?
2. Tại sao mô hình tam giác CIA không còn giải quyết thỏa đáng thay đổi môi trường?
3. Bảo mật là gì? Bảo mật thông tin là gì?
4. Thông tin có bao nhiêu đặc điểm cơ bản? Là gì họ?
5. Kể từ khi tam giác CIA trở thành tiêu chuẩn công nghiệp cho máy tính bảo vệ? Nó dựa trên cái gì?
6. Một tổ chức thành công nên có gì để bảo vệ hoạt động của mình?
7. Tấn công là gì? Những loại tấn công được đề cập trong đoạn văn?
8. Lỗ hổng là gì? Đưa ra một số ví dụ về lỗ hổng.

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa lỗi sai (F)

1. An ninh mạng là bảo vệ cá nhân hoặc nhóm cá nhân được phép truy cập vào tổ chức và các hoạt động của nó.

A. Đúng

B. Sai

C. NI

2. Các mối đe dọa an toàn thông tin có nhiều dạng khác nhau. Một số các mối đe dọa phổ biến nhất hiện nay là các cuộc tấn công phần mềm, đánh cắp trí tuệ trộm cắp tài sản và danh tính.

A. Đúng

B. Sai

C. NI

3. Mô hình tam giác CIA vẫn giải quyết thỏa đáng vấn đề liên tục thay đổi môi trường cho đến nay.

A. Đúng

B. Sai

C. NI

4. Bảo mật hoạt động là một quá trình xác định thông tin quan trọng để xác định xem các hành động thân thiện có thể được quan sát bởi trí thông minh của kẻ thù hay không.

A. Đúng

B. Sai

C. NI

5. Mô hình bảo mật thông tin CNSS phát triển từ một khái niệm được phát triển bởi ngành bảo mật máy tính được gọi là tam giác CIA.

A. Đúng

B. Sai

C. NI

6. Các tổ chức phải giảm thiểu rủi ro để phù hợp với khẩu vị rủi ro của họ - số lượng và bản chất của rủi ro mà tổ chức sẵn sàng chấp nhận.

A. Đúng

B. Sai

C. NI

7. Rủi ro là điểm yếu hoặc lỗi trong hệ thống hoặc cơ chế bảo vệ mà mở nó để tấn công hoặc thiệt hại.

A. Đúng

B. Sai

C. NI

8. Một tổ chức thành công nên có sẵn một lớp bảo mật để bảo vệ hoạt động của mình.

A. Đúng

B. Sai

C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu sau

1. là một phạm trù đối tượng, người hoặc các thực thể khác thể hiện một nguy hiểm đối với một tài sản.

Mối hiểm họa

C. Rủi ro

B. Thé trận an ninh

D. Tính dễ bị tồn thư ơng

2. là một hệ thống nhiều lớp bảo vệ chủ quyền của một nhà nước, tài sản, nguồn lực và con người.

A. An ninh nhân sự

C. An ninh mạng

B. An ninh quốc phòng

D. An ninh vật chất

3. Ai đó tình cờ đọc thông tin nhạy cảm không dành cho họ hoặc

công dụng của cô ấy là

A. cố ý tấn công

C. tấn công trực tiếp

B. một cuộc tấn công thụ động

D. chủ động tấn công

4. có thể là một quy trình được lập thành văn bản để tận dụng lợi thế của một

dễ bị tổn thương hoặc phơi nhiễm, thường là trong phần mềm, vốn có trong

phần mềm hoặc do kẻ tấn công tạo ra.

A. Hồ sơ bảo vệ

C. Khai thác

B. Một tác nhân đe dọa

D. Một tài sản

5. Người dùng được ủy quyền có hệ thống, trong khi tin tặc có

..... đến một hệ thống.

A. truy cập bất hợp pháp/ truy cập hợp pháp

C. hợp pháp/bất hợp pháp

B. truy cập hợp pháp/ truy cập bất hợp pháp

D. B & C đều đúng

6. các cuộc tấn công bắt nguồn từ chính mối đe dọa. cuộc tấn công bắt nguồn

từ một hệ thống hoặc tài nguyên bị xâm nhập đang bị trực tiếp hoặc đang hoạt động

duới sự kiểm soát của một mối đe dọa.

A. Trực tiếp/Gián tiếp

C. B & C đều đúng

B. Bị động/Chủ động

D. Gián tiếp/Bị động

7. Trong bảo mật thông tin, tồn tại khi một lỗ hổng được biết đến với một

kẻ tấn công có mặt.

A. bảo vệ

C. rủi ro

B. tiếp xúc

D. thế trận an ninh

8. Khi thông tin của một tổ chức bị đánh cắp, nó đã phải chịu một

A. thươ vong

C. thiệt hại

B. mất mát

D. Tất cả đều đúng

3. Nói 1. Bạn

biết những khái niệm hoặc thuật ngữ bảo mật thông tin quan trọng nào?

Đưa ra định nghĩa của họ theo cách của riêng bạn.

2. Trình bày các thành phần của an toàn thông tin.

ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi

1. Bạn biết bao nhiêu đặc điểm quan trọng của thông tin? Là gì họ?

2. Đặc điểm quan trọng nào của thông tin là quan trọng nhất? Tại sao?

2. Đọc mục tiêu mật mã và thực hiện các nhiệm vụ bên dưới

Đặc điểm quan trọng của thông tin

Tính khả dụng: Tính khả dụng cho phép người dùng được ủy quyền–ngườiօi hoặc hệ thống máy tính–truy cập thông tin mà không bị can thiệp hoặc cản trở và nhận thông tin đó ở định dạng được yêu cầu. Ví dụ, hãy xem xét các thư viện nghiên cứu yêu cầu nhận dạng truy օc khi vào. Thủ thư bảo vệ nội dung của thư viện để chúng chỉ có sẵn cho những ngườiօi bảo trợ được ủy quyền. Thủ thư phải chấp nhận nhận dạng của ngườiօi bảo trợ trước khi ngườiօi bảo trợ đó có quyền truy cập miễn phí vào các ngăn xếp sách. Sau khi những ngườiօi bảo trợ được ủy quyền có quyền truy cập vào nội dung của các ngăn xếp, họ mong muốn tìm thấy thông tin họ cần có sẵn ở định dạng có thể sử dụng được và ngôn ngữ quen thuộc, trong trường hợp này thư օng có nghĩa là đóng thành sách và viết bằng tiếng Anh.

Độ chính xác: Thông tin có độ chính xác khi nó không có sai sót hoặc lỗi và nó có giá trị mà ngườiօi dùng cuối mong đợi. Nếu thông tin đã bị sửa đổi một cách cố ý hoặc vô ý thì thông tin đó không còn chính xác nữa. Ví dụ, hãy xem xét một tài khoản séc. Bạn cho rằng thông tin có trong tài khoản séc của bạn là sự thể hiện chính xác về tình hình tài chính của bạn. Thông tin không chính xác trong tài khoản séc của bạn có thể do lỗi bên ngoài hoặc bên trong. Ví dụ, nếu một giao dịch viên ngân hàng cộng hoặc trừ quá nhiều từ tài khoản của bạn, thì giá trị của thông tin sẽ bị thay đổi. Hoặc, bạn có thể vô tình nhập sai số tiền vào sổ đăng ký tài khoản của mình. Dù bằng cách nào, số dư ngân hàng không chính xác có thể khiến bạn phạm sai lầm, chẳng hạn như trả lại séc.

Tính xác thực: Tính xác thực của thông tin là chất lư օng hoặc trạng thái của tính xác thực hoặc nguyên bản, chứ không phải là sự sao chép hoặc bịa đặt. Thông tin là xác thực khi nó ở cùng trạng thái mà nó được tạo ra, đặt, lưu trữ hoặc chuyển giao. Hãy xem xét một số giả định phổ biến về e-mail. Khi bạn nhận được e-mail, bạn cho rằng một cá nhân hoặc nhóm cụ thể đã tạo và

đã gửi e-mail-bạn cho rằng mình biết nguồn gốc của e-mail. Đây không phải là luôn luôn như vậy.

Giả mạo e-mail, hành động gửi một e-mail có trơ ờng bị sửa đổi, là một vấn đề đối với nhiều người ngày nay, vì thông thư ờng trơ ờng bị sửa đổi là địa chỉ của người gửi. Giả mạo địa chỉ của người gửi có thể đánh lừa người nhận e-mail nghĩ rằng thư là lưu lư ợng truy cập hợp pháp, do đó khiêm họ mở e-mail mà họ có thể không có. Giả mạo cũng có thể thay đổi dữ liệu được truyền qua mạng, như trong trơ ờng hợp giả mạo gói giao thức dữ liệu người dùng (UDP), có thể cho phép kẻ tấn công truy cập vào dữ liệu được lưu trữ trên máy tính

các hệ thống.

Bảo mật: Thông tin có tính bảo mật khi nó được bảo vệ khỏi bị tiết lộ hoặc tiếp xúc với các cá nhân hoặc hệ thống trái phép. Bảo mật đảm bảo rằng chỉ những người có quyền và đặc quyền truy cập thông tin mới có thể làm như vậy. Khi các cá nhân hoặc hệ thống trái phép có thể xem thông tin, tính bảo mật bị vi phạm. Để bảo vệ tính bảo mật của thông tin, bạn có thể sử dụng một số biện pháp, bao gồm các biện pháp sau:

- Phân loại thông tin
- Lưu trữ tài liệu an toàn
- Áp dụng các chính sách bảo mật chung
- Giáo dục người quản lý thông tin và người dùng cuối

Tính bảo mật, giống như hầu hết các đặc điểm của thông tin, phụ thuộc lẫn nhau với các đặc điểm khác và có liên quan chặt chẽ nhất với đặc điểm được gọi là quyền riêng tư.

Giá trị của tính bảo mật thông tin đặc biệt cao khi đó là thông tin cá nhân về nhân viên, khách hàng hoặc bệnh nhân. Các cá nhân giao dịch với một tổ chức mong muốn rằng thông tin cá nhân của họ sẽ được giữ bí mật, cho dù tổ chức đó là một cơ quan liên bang, chẳng hạn như Sở Thuế vụ hay một doanh nghiệp. Các vấn đề phát sinh khi các công ty tiết lộ thông tin bí mật.

Đôi khi việc tiết lộ này là cố ý, như cũng có những lúc việc tiết lộ thông tin bí mật xảy ra do nhầm lẫn-ví dụ: khi thông tin bí mật bị gửi nhầm qua email cho người bên ngoài tổ chức chứ không phải cho người bên trong tổ chức. Một số trơ ờng hợp vi phạm quyền riêng tư được vạch ra

trong Ngoại tuyến: Tiết lộ ngoài ý muốn.

Sự chính trực

Thông tin có tính toàn vẹn khi nó là toàn bộ, đầy đủ và không bị hỏng. Tính toàn vẹn của thông tin bị đe dọa khi thông tin bị phơi nhiễm, hư hỏng, phá hủy hoặc sự gián đoạn khác đối với trạng thái xác thực của nó.

Tham nhũng có thể xảy ra trong khi thông tin đang được lưu trữ hoặc truyền đi. Nhiều virus và sâu máy tính được thiết kế với mục đích rõ ràng là làm hỏng dữ liệu. Vì lý do này, một phương pháp quan trọng để phát hiện vi-rút hoặc sâu là tìm kiếm những thay đổi về tính toàn vẹn của tệp. Một phương pháp quan trọng khác để đảm bảo tính toàn vẹn của thông tin là băm tệp, trong đó một tệp được đọc bởi một thuật toán đặc biệt sử dụng giá trị của các bit trong tệp để tính toán một số lớn duy nhất được gọi là giá trị băm. Giá trị băm cho bất kỳ tổ hợp bit nào là duy nhất. Nếu một hệ thống máy tính thực hiện cùng một thuật toán băm trên một tệp và thu được một số khác với giá trị băm đã ghi cho tệp đó, thì tệp đó đã bị xâm phạm và tính toàn vẹn của thông tin sẽ bị mất. Tính toàn vẹn của thông tin là nền tảng của hệ thống thông tin, bởi vì thông tin sẽ không có giá trị hoặc giá trị sử dụng nếu người dùng không thể xác minh tính toàn vẹn của nó.

Tệp bị hỏng không nhất thiết là kết quả của các tác nhân bên ngoài, chẳng hạn như tin tặc.

Chẳng hạn, tiếng ồn trong phương tiện truyền dẫn cũng có thể khiến dữ liệu mất tính toàn vẹn. Truyền dữ liệu trên mạch với mức điện áp thấp có thể làm thay đổi và hỏng dữ liệu. Các bit dự phòng và các bit kiểm tra có thể bù đắp cho các lỗi để bảo vệ bên trong và bên ngoài đối với tính toàn vẹn của thông tin. Trong mỗi lần truyền, thuật toán, giá trị băm và mã sửa lỗi đảm bảo tính toàn vẹn của thông tin. Dữ liệu có tính toàn vẹn đã bị xâm phạm được truyền lại.

Tính thiết thực

Tiện ích của thông tin là chất lượng hoặc trạng thái có giá trị cho một mục đích hoặc mục đích nào đó.

Thông tin có giá trị khi nó có thể phục vụ một mục đích. Nếu thông tin có sẵn, nhưng không ở định dạng có ý nghĩa đối với người dùng cuối, thì thông tin đó không hữu ích. Ví dụ: đối với một công dân tư nhân, dữ liệu Điều tra dân số Hoa Kỳ có thể nhanh chóng trở nên quá tải và khó diễn giải; tuy nhiên, đối với một chính trị gia, dữ liệu Điều tra dân số Hoa Kỳ tiết lộ thông tin về cư dân trong một quận, chẳng hạn như chủng tộc, giới tính và tuổi tác của họ.

Thông tin này có thể giúp hình thành chiến lược tranh cử tiếp theo của một chính trị gia.

Chiếm hữu

Việc sở hữu thông tin là chất lượng hoặc trạng thái sở hữu hoặc kiểm soát.

Thông tin được cho là thuộc quyền sở hữu của một người nếu người đó có được nó, không phụ thuộc vào

định dạng hoặc các đặc điểm khác. Mặc dù vi phạm tính bảo mật luôn dẫn đến vi phạm quyền sở hữu, như việc vi phạm quyền sở hữu không phải lúc nào cũng dẫn đến vi phạm tính bảo mật.

2.1. Trả lời các câu hỏi

1. Thông tin xác thực khi nào?
2. Khi nào thông tin được coi là không chính xác?
3. Bảo mật thông tin khi nào?
4. Thông tin có bao nhiêu đặc điểm quan trọng? Họ là ai?
5. Tại sao tính toàn vẹn thông tin là nền tảng của hệ thống thông tin?
6. Khi nào tính toàn vẹn của thông tin bị đe dọa?
7. Bạn có thể sử dụng những gì để bảo vệ tính bảo mật của thông tin?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI).
Sửa lỗi sai (F).

1. Sau khi người bảo trợ đưa ra ủy quyền có quyền truy cập vào nội dung của ngăn xếp, họ mong muốn tìm thấy thông tin họ cần có sẵn ở định dạng có thể sử dụng đưa ra và ngôn ngữ quen thuộc.

- A. Đúng B. Sai C. NI

2. Khi các cá nhân hoặc hệ thống trái phép có thể xem thông tin, bảo mật bị vi phạm

- A. Đúng B. Sai C. NI

3. Giá trị xác thực của thông tin đặc biệt cao khi nó đưa ra thông tin cá nhân về nhân viên, khách hàng hoặc bệnh nhân.

- A. Đúng B. Sai C. NI

4. Tính bảo mật đảm bảo rằng chỉ những người có quyền và đặc quyền mới truy cập có thể làm như vậy.

- A. Đúng B. Sai C. NI

5. Nếu một hệ thống máy tính thực hiện thuật toán băm khác nhau trên một tệp và nhận được một số khác với giá trị băm đã ghi cho tệp, tệp đã bị xâm phạm và tính toàn vẹn của thông tin bị mất.

A. Đúng

B. Sai

C. NI

6. Trong kinh tế học, khái niệm tiện ích được sử dụng để mô hình giá trị hoặc giá trị, như ng việc sử dụng nó đã phát triển đáng kể theo thời gian.

A. Đúng

B. Sai

C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và các câu lệnh

1. Đặc điểm quan trọng nào của thông tin là chất lượng hoặc trạng thái hiện hữu

chính hãng hay bản gốc, chứ không phải là một bản sao hoặc chế tạo?

A. Tính xác thực

C. Độ chính xác

B. Bảo mật

D. Tiện ích

2. Tại sao ngày nay việc giả mạo E-mail là một vấn đề đối với nhiều người?

A. Bởi vì truờng đư ợc sửa đổi thư ờng là địa chỉ của người khởi tạo.

B. Vì truờng đư ợc sửa đổi thư ờng là địa chỉ của người khởi tạo.

C. A & B đúng

D. Bởi vì truờng đư ợc sửa đổi thư ờng là địa chỉ của người khởi tạo.

3. là chất lượng hoặc trạng thái có giá trị cho một số mục đích hoặc kết thúc.

A. chính trực

C. săn có

B. tiện ích của thông tin

D. A & B đúng

4. là chất lượng hoặc trạng thái sở hữu hoặc kiểm soát.

A. Tiện ích của thông tin

B. Sự săn có của thông tin

C. Bảo mật thông tin

D. Sở hữu thông tin

5. Thông tin không chính xác trong tài khoản séc của bạn có thể xuất phát từ bên ngoài hoặc nội bộ

A. truy cập

C. báo cáo

B. lỗi

D. truyền

6. Nếu giao dịch viên ngân hàng cộng hoặc trừ quá nhiều từ tài khoản của bạn,

A. Giá trị của hàm băm không thay đổi.

B. Sự sẵn có của thông tin là vô ích.

C. giá trị của thông tin bị thay đổi.

D. Tính bí mật của thông tin bị đánh cắp.

7. Bạn có thể sử dụngcác biện pháp để bảo vệ bí mật của thông tin.

A. phân loại thông tin, áp dụng các chính sách bảo mật chung

B. lưu trữ tài liệu an toàn

C. giáo dục người quản lý thông tin và người dùng cuối

D. Tất cả đều đúng

3. Nói

1. Trình bày các đặc điểm quan trọng của thông tin.

2. Chọn một trong những đặc điểm quan trọng của thông tin và trình bày nó.

ĐỌC VÀ NÓI 4

1. Thảo luận các câu hỏi

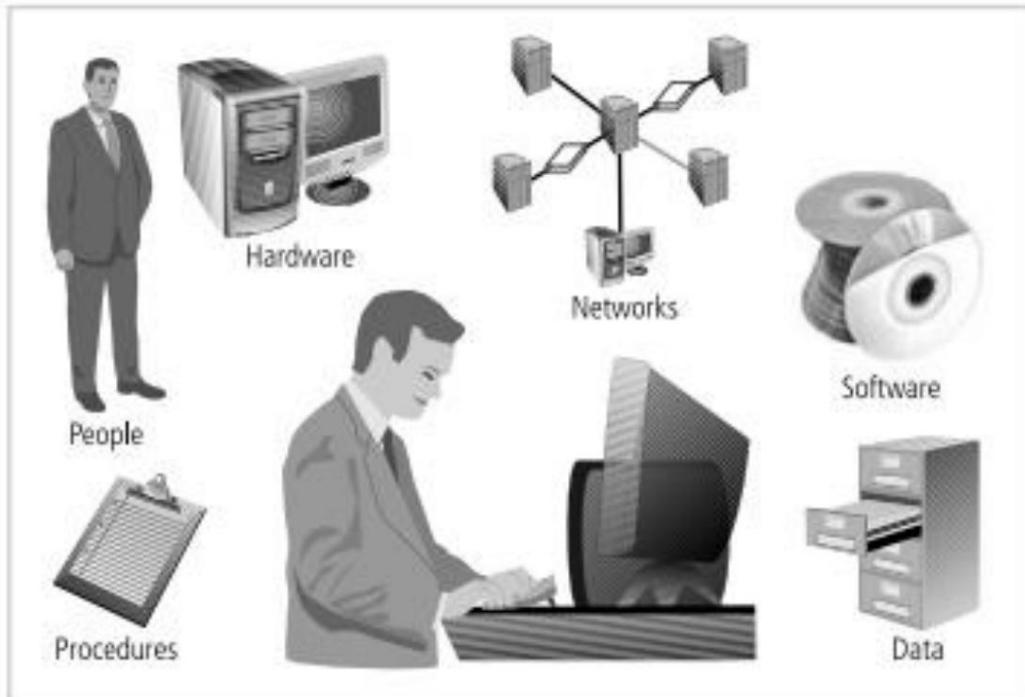
1. Bạn biết những thành phần nào của một hệ thống thông tin?
2. Thành phần nào quan trọng nhất và tại sao?
3. Phần mềm là gì? Bạn biết phần mềm nào?
4. Phàn cứng là gì? Liệt kê một số linh kiện phần cứng mà bạn biết.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Các thành phần của một hệ thống thông tin

Như trong **Hình 1-5**, một hệ thống thông tin (IS) không chỉ là phần cứng máy tính; nó là toàn bộ tập hợp phần mềm, phần cứng, dữ liệu, con người, quy trình và mạng giúp cho việc sử dụng các nguồn thông tin trong tổ chức trở nên khả thi.

Sáu thành phần quan trọng này cho phép thông tin được nhập, xử lý, xuất và lưu trữ. Mỗi thành phần IS này đều có điểm mạnh và điểm yếu riêng, cũng như các đặc điểm và cách sử dụng riêng. Mỗi thành phần của hệ thống thông tin cũng có những yêu cầu bảo mật riêng.



Hình 1-5. Các thành phần của một hệ thống thông tin

Phần mềm

Thành phần phần mềm của IS bao gồm các ứng dụng, hệ điều hành và các loại tiện ích lệnh. Phần mềm có lẽ là thành phần IS khó bảo mật nhất. Việc khai thác các lỗi trong lập trình phần mềm chiếm một phần đáng kể trong các cuộc tấn công vào thông tin. Ngành công nghệ thông tin đầy rẫy những báo cáo cảnh báo về lỗ hỏng, lỗi, điểm yếu hoặc các vấn đề cơ bản khác trong phần mềm. Trên thực tế, nhiều khía cạnh của cuộc sống hàng ngày bị ảnh hưởng bởi phần mềm lỗi, từ điện thoại thông minh gặp sự cố cho đến máy tính điều khiển ô tô bị lỗi dẫn đến thu hồi.

Phần mềm mang huyết mạch của thông tin thông qua một tổ chức.

Thật không may, các chương trình phần mềm thường được tạo ra dưới sự ràng buộc của quản lý dự án, hạn chế thời gian, chi phí và nhân lực. Bảo mật thông tin thường được thực hiện như một suy nghĩ sau, thay vì được phát triển như một thành phần không thể thiếu ngay từ đầu. Theo cách này, các chương trình phần mềm trở thành mục tiêu dễ dàng của các cuộc tấn công vô tình hoặc cố ý.

Phần cứng

Phần cứng là công nghệ vật lý chứa và thực thi phần mềm, lưu trữ và vận chuyển dữ liệu, đồng thời cung cấp các giao diện để nhập và xóa thông tin khỏi hệ thống. Các chính sách bảo mật vật lý coi phần cứng là tài sản vật chất và bảo vệ tài sản vật chất khỏi bị hư hại hoặc trộm cắp.

Việc áp dụng các công cụ bảo mật vật lý truyền thống, chẳng hạn như khóa và chìa khóa, hạn chế quyền truy cập và tương tác với các thành phần phần cứng của hệ thống thông tin. Việc bảo mật vị trí vật lý của máy tính và bản thân máy tính là rất quan trọng vì vi phạm bảo mật vật lý có thể dẫn đến mất thông tin.

Thật không may, hầu hết các hệ thống thông tin được xây dựng trên nền tảng phần cứng không thể đảm bảo bất kỳ mức độ bảo mật thông tin nào nếu có thể truy cập không hạn chế vào phần cứng.

Trước ngày 11 tháng 9 năm 2001, trộm cắp máy tính xách tay ở sân bay là phổ biến. Một nhóm gồm hai người đã làm việc để đánh cắp một chiếc máy tính khi chủ nhân của nó chuyển nó qua các thiết bị quét băng tải. Thủ phạm đầu tiên bุ ớc vào khu vực an ninh trước một mục tiêu không ngờ tới và nhanh chóng đi qua. Sau đó, thủ phạm thứ hai đợi phía sau mục tiêu cho đến khi mục tiêu đặt máy tính của mình lên máy quét hành lý.

Khi máy tính lướt qua, đặc vụ thứ hai vươn tay ra và bุ ớc vào máy dò kim loại với một bộ sưu tập đáng kể chìa khóa, tiền xu,

và những thứ tự ơ ng tự, do đó làm chậm quá trình phát hiện và cho phép thủ phạm đầu tiên chộp lấy máy tính và biến mất trong một lối đi đông đúc.

Dữ liệu

Dữ liệu được lưu trữ, xử lý và truyền bởi hệ thống máy tính phải được bảo vệ.

Dữ liệu thường là tài sản quý giá nhất mà một tổ chức sở hữu và nó là mục tiêu chính của các cuộc tấn công có chủ đích. Các hệ thống được phát triển trong những năm gần đây có khả năng sử dụng các hệ thống quản lý cơ sở dữ liệu. Khi được thực hiện đúng cách, điều này sẽ cải thiện tính bảo mật của dữ liệu và ứng dụng. Thật không may, nhiều dự án phát triển hệ thống không sử dụng đầy đủ các khả năng bảo mật của hệ thống quản lý cơ sở dữ liệu và trong một số trường hợp, cơ sở dữ liệu được triển khai theo cách kém an toàn hơn các hệ thống tệp truyền thống.

Con

người Mặc dù thường bị bỏ qua trong các câu nhắc về bảo mật máy tính, nhưng con người luôn là mối đe dọa đối với bảo mật thông tin. Truyền thuyết kể rằng vào khoảng năm 200 trước Công nguyên, một đội quân lớn đã đe dọa an ninh và sự ổn định của đế chế Trung Quốc. Những kẻ xâm lược hung dữ đến nỗi hoàng đế Trung Quốc đã chỉ huy xây dựng một bức tượng lớn để bảo vệ chống lại quân xâm lược Hun. Vào khoảng năm 1275 sau Công nguyên, Hốt Tất Liệt cuối cùng đã đạt được điều mà người Huns đã có gắng hàng nghìn năm. Ban đầu, quân đội của Khan cố gắng trèo qua, đào sâu và phá đường. Cuối cùng, Khan chỉ đơn giản là hối lộ người gác cổng và phần còn lại là lịch sử. Cho dù sự kiện này có thực sự xảy ra hay không, bài học của câu chuyện là con người có thể là mắt xích yếu nhất trong chương trình bảo mật thông tin của một tổ chức. Và trừ khi chính sách, giáo dục và đào tạo, nhận thức và công nghệ được sử dụng hợp lý để ngăn chặn mọi người vô tình hoặc cố ý làm hỏng hoặc mất thông tin, chúng sẽ vẫn là mắt xích yếu nhất.

thủ tục

Một thành phần khác thường bị bỏ qua của IS là các thủ tục. Các thủ tục là các hướng dẫn bằng văn bản để hoàn thành một nhiệm vụ cụ thể. Khi một người dùng trái phép có được các thủ tục của tổ chức, điều này gây ra mối đe dọa đối với tính toàn vẹn của thông tin. Ví dụ, một nhà tư vấn cho một ngân hàng đã học cách chuyển tiền bằng cách sử dụng các thủ tục sẵn có của trung tâm máy tính. Bằng cách lợi dụng điểm yếu bảo mật (thiếu xác thực), nhà tư vấn ngân hàng này đã ra lệnh chuyển hàng triệu đô la bằng chuyển khoản vào tài khoản của chính mình. Thủ tục an ninh lỏng lẻo khiến thất thoát hơn chục triệu USD trước tình hình

đã đư ợc sửa chữa. Hầu hết các tổ chức phân phối các thủ tục cho nhân viên hợp pháp của họ để họ có thể truy cập vào hệ thống thông tin, như ng nhiều công ty trong số này thư ờng không cung cấp giáo dục thích hợp về việc bảo vệ các thủ tục. Giáo dục nhân viên về các quy trình bảo vệ an toàn cũng quan trọng như bảo mật vật lý cho hệ thống thông tin. Xét cho cùng, các thủ tục là thông tin theo đúng nghĩa của chúng. Do đó, kiến thức về các thủ tục, cũng như tất cả các thông tin quan trọng, chỉ nên đư ợc phổ biến giữa các thành viên của tổ chức trên một cơ sở cần thiết.

Mạng

Thành phần IS tạo ra phần lớn nhu cầu tăng cư ờng bảo mật thông tin và máy tính là kết nối mạng. Khi các hệ thống thông tin đư ợc kết nối với nhau để tạo thành các mạng cục bộ (LAN) và các mạng LAN này đư ợc kết nối với các mạng khác như Internet, các thách thức bảo mật mới sẽ nhanh chóng xuất hiện. Công nghệ vật lý cho phép các chức năng mạng ngày càng trở nên dễ tiếp cận hơn đối với các tổ chức thuộc mọi quy mô. Việc áp dụng các công cụ bảo mật vật lý truyền thống, chẳng hạn như khóa và chìa khóa, để hạn chế quyền truy cập và tương tác với các thành phần phần cứng của hệ thống thông tin vẫn còn quan trọng; nhưng khi các hệ thống máy tính đư ợc nối mạng, cách tiếp cận này không còn đủ nữa. Các bước cung cấp bảo mật mạng là cần thiết, cũng như việc triển khai các hệ thống báo động và xâm nhập để chủ sở hữu hệ thống nhận thức đư ợc các thỏa hiệp đang diễn ra.

2.1. Trả lời các câu hỏi

1. Những công cụ bảo mật vật lý nào thư ờng đư ợc áp dụng để hạn chế quyền truy cập và tương tác với các thành phần phần cứng của một hệ thống thông tin?
2. Điều gì xảy ra khi một người dùng trái phép có đư ợc tài khoản của một tổ chức thủ tục?
3. Hệ thống thông tin là gì?
4. Tại sao dữ liệu là mục tiêu chính của các cuộc tấn công có chủ đích?
5. Thành phần nào của Hệ thống thông tin khó bảo mật nhất?
6. Điều gì trở nên phổ biến ở sân bay trước năm 2002? Cung cấp chi tiết.
7. Tại sao các chương trình phần mềm trở thành mục tiêu dễ dàng của các hành vi tình cờ hoặc tấn công có chủ ý?

8. Tại sao bảo mật vị trí vật lý của máy tính và máy tính
bản thân quan trọng?

9. Chỉ có phần mềm và phần cứng mới cho phép thông tin đư ợc nhập, xử lý,
đầu ra và đư ợc lưu trữ.? Nếu không, những thành phần nào cho phép nó làm như vậy?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI).
Sửa lỗi sai (F).

1. Phần cứng hệ thống thông tin là bộ phận của hệ thống thông tin mà bạn
có thể chạm vào - các thành phần vật lý của công nghệ.

- A. Đúng B. Sai C. NI

2. Ngành công nghệ thông tin đầy rẫy những báo cáo cảnh báo lỗ hổng,
lỗi, điểm yếu hoặc các vấn đề cơ bản khác trong phần mềm.

- A. Đúng B. Sai C. NI

3. Công nghệ vật lý hỗ trợ các chức năng mạng ngày càng ít đi
và ít tiếp cận hơn đối với các tổ chức thuộc mọi quy mô.

- A. Đúng B. Sai C. NI

4. Những kẻ xâm lư ợc rất hung dữ đến nỗi hoàng đế Trung Quốc đã chỉ huy
xây dựng một bức tường lớn để bảo vệ chống lại quân xâm lư ợc Hun.

- A. Đúng B. Sai C. NI

5. Bảo mật hệ thống thông tin về mặt vật lý không quan trọng bằng giáo dục
nhân viên về các thủ tục bảo vệ.

- A. Đúng B. Sai C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu sau

1. Nhiều dự án phát triển hệ thống không tận dụng hết
khả năng bảo mật của hệ thống quản lý, và trong một số trường hợp cơ sở dữ liệu là
..... theo những cách kém an toàn hơn so với các hệ thống tệp truyền thống.

- A. cơ sở dữ liệu/đã thực thi C. A & B đều đúng
B. cơ sở dữ liệu/đã triển khai D. dữ liệu/đã triển khai

2. Thành phần thư ờng bị bỏ qua của IS là Chúng đư ợc viết
hư ờng dẫn để hoàn thành một nhiệm vụ cụ thể.

- A. mạng C. phần mềm

B. thủ tục

D. cơ sở dữ liệu

3. Thành phần IS tạo ra phần lớn nhu cầu về máy tính gia tăng

và bảo mật thông tin là

Một phần mềm

C. phần cứng

B. mạng

D. dữ liệu

4. của IS bao gồm các ứng dụng, hệ điều hành và các loại tiện ích lệnh.

A. Thành phần phần mềm

C. Thành phần mạng

B. Thành phần phần cứng

D. A&C đều đúng

5. Các chính sách bảo mật vật chất xử lý như một tài sản vật chất và với việc bảo vệ tài sản vật chất khỏi bị hư hại hoặc trộm cắp.

Một phần mềm

C. phần mềm gián điệp

B. phần mềm quảng cáo

D. phần cứng

6. thư ờng đư ợc tạo dư ới sự ràng buộc của dự án quản lý, hạn chế thời gian, chi phí và nhân lực.

A. chương trình phần mềm

C. chương trình phần cứng

B. chương trình phần mềm gián điệp

D. chương trình phần mềm quảng cáo

7. Thật không may, hầu hết các hệ thống thông tin đư ợc xây dựng trên nền tảng phần cứng không thể đảm bảo bất kỳ mức độ bảo mật thông tin nào nếu quyền truy cập không hạn chế đến phần cứng là có thẻ.

A. thiết kế/đảm bảo

C. A & B đều đúng

B. thiết kế/đảm bảo

D. thực hiện/nhất định

8. Bằng cách lấy điểm yếu bảo mật, nhà tư vấn ngân hàng có thẻ yêu cầu hàng triệu đô la để đư ợc chuyển bằng điện vào tài khoản của chính mình.

A. lợi thế

C. vị trí

B. một tờ quảng cáo

D. cơ hội

9. Trên thực tế, nhiều trong cuộc sống hàng ngày bị ảnh hưởng bởi , từ điện thoại thông minh gặp sự cố với máy tính điều khiển ô tô bị lỗi dẫn đến thu hồi.

A. khía cạnh/phần mềm lỗi

C. A & B đều đúng

- B. khía cạnh/phần mềm lõi D. khía cạnh/phần cứng lõi
10. Kiến thức về các thủ tục, cũng như tất cả các thông tin quan trọng, nên đư ợc giữa các thành viên của tổ chức chỉ trên cơ sở cần biết.
- A. phô biến C. tổng quát
- B. phô biến D. tất cả đều đúng

3. Nói

1. Trình bày các thành phần của một hệ thống thông tin.
2. Chọn một trong các thành phần của hệ thống thông tin và trình bày thành thông tin chi tiết.
3. Thành phần nào của hệ thống thông tin bạn nghĩ nhiều nhất quan trọng và tại sao?

4. Lắng nghe

1. <https://www.youtube.com/watch?v=eUxUUarTRW4>
2. <https://www.youtube.com/watch?v=432IHWNMqJE>
3. <https://www.youtube.com/watch?v=8caqok3ah8o>
4. <https://www.youtube.com/watch?v=XlcolUHMnh0>

VIẾT VÀ NÓI

1. Viết khoảng 400 từ về một trong những chủ đề sau theo cách của riêng bạn từ ngữ

- Sơ lược về lịch sử bảo mật thông tin
- Đặc điểm quan trọng của thông tin
- Các thành phần của một hệ thống thông tin

2. Trình bày các nội dung sau:

- Sơ lược về lịch sử an toàn thông tin
- Đặc điểm quan trọng của thông tin
- Các thành phần của một hệ thống thông tin

ĐỌC THÊM

Vòng đời phát triển hệ thống

Bảo mật thông tin phải được quản lý theo cách tự.org tự như bất kỳ hệ thống chính nào khác được triển khai trong một tổ chức. Một cách tiếp cận để triển khai hệ thống bảo mật thông tin trong một tổ chức có ít hoặc không có bảo mật chính thức là sử dụng một biến thể của vòng đời phát triển hệ thống (SDLC): vòng đời phát triển hệ thống bảo mật (SecSDLC). Để hiểu vòng đời phát triển hệ thống bảo mật, trước tiên bạn phải hiểu những điều cơ bản của phương pháp mà nó dựa vào.

Phương pháp và giai đoạn

Vòng đời phát triển hệ thống (SDLC) là một phương pháp thiết kế và triển khai hệ thống thông tin. Một phương pháp luận là một cách tiếp cận chính thức để giải quyết một vấn đề bằng một chuỗi các thủ tục có cấu trúc. Sử dụng một phương pháp đảm bảo một quy trình chặt chẽ với mục tiêu được xác định rõ ràng và tăng khả năng thành công. Khi một phương pháp đã được áp dụng, các mốc quan trọng được thiết lập và một nhóm các cá nhân được chọn chịu trách nhiệm giải trình cho việc hoàn thành các mục tiêu của dự án.

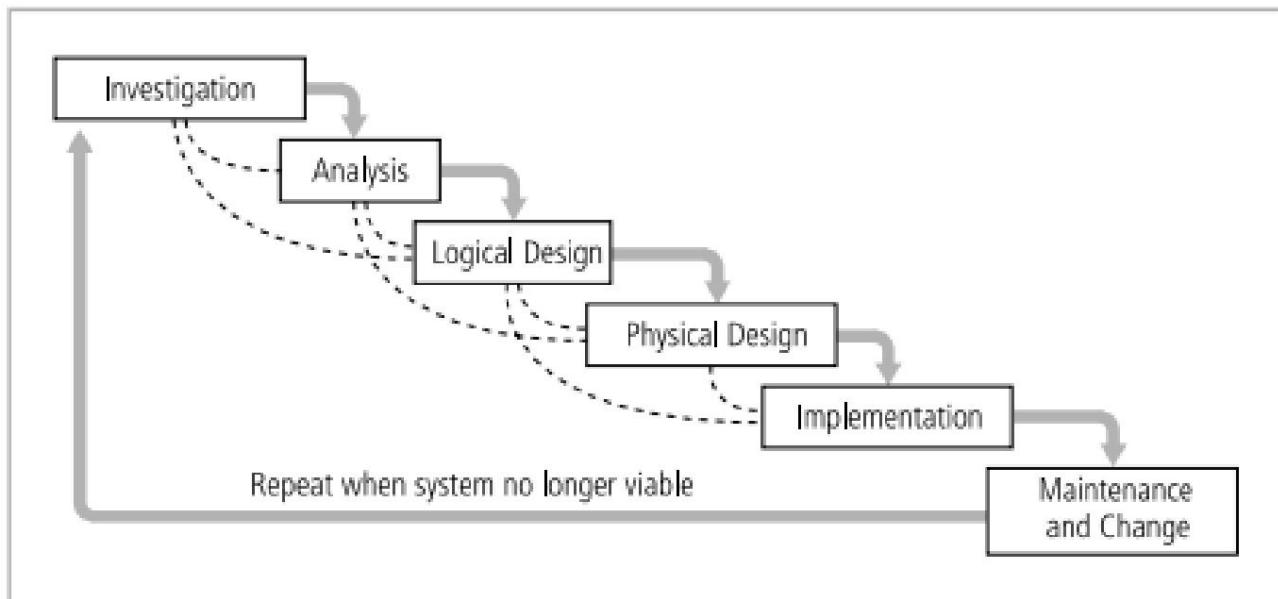
SDLC truyền thống bao gồm sáu giai đoạn chung. Nếu bạn đã tham gia khóa học thiết kế và phân tích hệ thống, bạn có thể đã tiếp xúc với một mô hình bao gồm một số giai đoạn khác nhau. Các mô hình SDLC có từ ba đến mươi hai giai đoạn, tất cả đều được ánh xạ thành sáu giai đoạn được trình bày ở đây. Mô hình thác nước trong [Hình 1-6](#). minh họa rằng mỗi giai đoạn bắt đầu với kết quả và thông tin thu được từ giai đoạn trước.

Vào cuối mỗi giai đoạn, sẽ có một đánh giá có cấu trúc hoặc kiểm tra thực tế, trong đó nhóm xác định xem dự án có nên được tiếp tục, dừng lại, thuê ngoài, hoãn lại hoặc quay trở lại giai đoạn trước đó hay không tùy thuộc vào việc dự án có được tiến hành như mong đợi hay không. nhu cầu chuyên môn bổ sung, kiến thức tổ chức, hoặc các nguồn lực khác.

Sau khi hệ thống được triển khai, nó sẽ được duy trì (và sửa đổi) trong suốt thời gian hoạt động còn lại của nó. Bất kỳ việc triển khai hệ thống thông tin nào cũng có thể có nhiều lần lặp lại khi chu kỳ được lặp lại theo thời gian. Chỉ bằng cách kiểm tra và đổi mới liên tục, bất kỳ hệ thống nào, đặc biệt là hệ thống thông tin

chương trình bảo mật, hoạt động như mong đợi trong môi trường thay đổi liên tục mà nó được đặt vào.

Các phần sau mô tả từng giai đoạn của SDLC truyền thống.



Hình 1-6. Phư ơng pháp thác nư ớc SDLC

Cuộc điều tra

Giai đoạn đầu tiên, điều tra, là quan trọng nhất. Hệ thống đang được phát triển để giải quyết vấn đề gì? Giai đoạn điều tra bắt đầu bằng việc kiểm tra sự kiện hoặc kế hoạch bắt đầu quá trình. Trong giai đoạn điều tra, các mục tiêu, hạn chế và phạm vi của dự án được chỉ định. Một phân tích lợi ích chi phí sơ bộ đánh giá những lợi ích cảm nhận được và mức chi phí thích hợp cho những lợi ích đó. Khi kết thúc giai đoạn này và ở mọi giai đoạn tiếp theo, phân tích khả thi đánh giá tính khả thi về kinh tế, kỹ thuật và hành vi của quy trình và đảm bảo rằng việc triển khai xứng đáng với thời gian và chi phí của tổ chức.

có gắng.

Phân tích

Giai đoạn phân tích bắt đầu với thông tin thu được trong giai đoạn điều tra. Giai đoạn này chủ yếu bao gồm các đánh giá về tổ chức, các hệ thống hiện tại và khả năng hỗ trợ các hệ thống được đề xuất của tổ chức. Các nhà phân tích bắt đầu bằng việc xác định xem hệ thống mới sẽ làm gì và nó sẽ tương tác với

các hệ thống hiện có. Giai đoạn này kết thúc với tài liệu về các phát hiện và bản cập nhật của phân tích khả thi.

thiết kế hợp lý

Trong giai đoạn thiết kế logic, thông tin thu được từ giai đoạn phân tích được sử dụng để bắt đầu tạo giải pháp hệ thống cho một vấn đề kinh doanh. Trong bất kỳ giải pháp hệ thống nào, điều bắt buộc là yêu tố đầu tiên và thúc đẩy là nhu cầu kinh doanh. Dựa trên nhu cầu kinh doanh, các ứng dụng được chọn để cung cấp các dịch vụ cần thiết, sau đó hỗ trợ dữ liệu và cấu trúc có khả năng cung cấp đầu vào cần thiết được chọn. Cuối cùng, dựa trên tất cả những điều trên, các công nghệ cụ thể để thực hiện giải pháp vật lý được vạch ra. Do đó, thiết kế hợp lý là kế hoạch chi tiết cho giải pháp mong muốn. Thiết kế hợp lý độc lập với việc triển khai, nghĩa là Ban biên tập đã cho rằng mọi nội dung bị chặn không ảnh hưởng nghiêm trọng đến trải nghiệm học tập tổng thể. Cengage Learning bảo lưu quyền xóa nội dung bổ sung bất cứ lúc nào nếu các hạn chế về quyền tiếp theo yêu cầu điều đó. rằng nó không chứa tham chiếu đến các công nghệ, nhà cung cấp hoặc sản phẩm cụ thể. Thay vào đó, nó đề cập đến cách hệ thống được đề xuất sẽ giải quyết vấn đề hiện tại. Trong giai đoạn này, các nhà phân tích tạo ra một số giải pháp thay thế, mỗi giải pháp có điểm mạnh và điểm yếu tương ứng, chi phí và lợi ích, cho phép so sánh chung các lựa chọn có sẵn. Vào cuối giai đoạn này, một phân tích khả thi khác được thực hiện.

Thiết kế vật lí

Trong giai đoạn thiết kế vật lí, các công nghệ cụ thể được chọn để hỗ trợ các giải pháp thay thế được xác định và đánh giá trong thiết kế logic. Các thành phần đã chọn được đánh giá dựa trên quyết định tự sản xuất hoặc mua (tự phát triển các thành phần hoặc mua chúng từ nhà cung cấp). Thiết kế cuối cùng tích hợp các thành phần và công nghệ khác nhau. Sau một phân tích khả thi khác, toàn bộ giải pháp được trình bày cho ban quản lý tổ chức phê duyệt.

Triển khai Trong

giai đoạn triển khai, mọi phần mềm cần thiết đều được tạo ra. Các thành phần được đặt hàng, nhận và kiểm tra. Sau đó, người dùng được đào tạo và tạo tài liệu hỗ trợ. Khi tất cả các thành phần được kiểm tra riêng lẻ, chúng sẽ được cài đặt và kiểm tra như một hệ thống. Một lần nữa, một phân tích khả thi được chuẩn bị, và

các nhà tài trợ sau đó đư ợc giới thiệu hệ thống để đánh giá hiệu suất và kiểm tra chấp nhận.

Bảo trì và Thay đổi

Giai đoạn bảo trì và thay đổi là giai đoạn dài nhất và tốn kém nhất của quy trình. Giai đoạn này bao gồm các nhiệm vụ cần thiết để hỗ trợ và sửa đổi hệ thống trong phần còn lại của vòng đời hữu ích của nó. Mặc dù sự phát triển chính thức có thể kết thúc trong giai đoạn này, vòng đời của dự án vẫn tiếp tục cho đến khi xác định đư ợc rằng quá trình nên bắt đầu lại từ giai đoạn điều tra. Tại các điểm định kỳ, hệ thống đư ợc kiểm tra tính tuân thủ và tính khả thi của việc tiếp tục so với việc ngừng đư ợc đánh giá. Nâng cấp, cập nhật và vá lỗi đư ợc quản lý. Khi nhu cầu của tổ chức thay đổi, các hệ thống hỗ trợ tổ chức cũng phải thay đổi. Điều bắt buộc là những người quản lý các hệ thống, cũng như những người hỗ trợ chúng, phải liên tục theo dõi hiệu quả của các hệ thống liên quan đến môi trường của tổ chức. Khi một hệ thống hiện tại không còn có thể hỗ trợ sứ mệnh phát triển của tổ chức, dự án sẽ bị chấm dứt và một dự án mới đư ợc triển khai.

Bảo vệ SDLC

Mỗi giai đoạn của SDLC phải bao gồm việc xem xét tính bảo mật của hệ thống đư ợc lắp ráp cũng như thông tin mà nó sử dụng. Cho dù hệ thống là tùy chỉnh và đư ợc xây dựng từ đầu, đư ợc mua và sau đó đư ợc tùy chỉnh hoặc là phần mềm thương mại có sẵn (COTS), tổ chức triển khai chịu trách nhiệm đảm bảo hệ thống đư ợc sử dụng an toàn. Điều này có nghĩa là mỗi lần triển khai hệ thống đều an toàn và không có nguy cơ ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn có của tài sản thông tin của tổ chức.

BÀI 2: NHU CẦU AN NINH

ĐỌC VÀ NÓI 1

1. Thảo luận các câu hỏi

1. Mối đe dọa là gì?
2. Bạn biết những mối đe dọa nào trong khu vực thông tin?
3. Bạn phải làm gì để tránh những mối đe dọa đó?
4. Mối đe dọa khác với rủi ro hay rủi ro giống nhau? sự khác biệt của họ là gì?
Điểm giống nhau của chúng là gì?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Đe dọa (1)

Thỏa hiệp về sở hữu trí tuệ

Nhiều tổ chức tạo ra hoặc hỗ trợ phát triển tài sản trí tuệ (IP) như một phần trong hoạt động kinh doanh của họ. Sở hữu trí tuệ được định nghĩa là "quyền sở hữu ý tư ởng và quyền kiểm soát đối với sự thể hiện hữu hình hoặc ảo của những ý tư ởng đó. Việc sử dụng tài sản trí tuệ của người khác có thể hoặc không liên quan đến việc thanh toán tiền bản quyền hoặc sự cho phép, như ng phải luôn bao gồm tín dụng thích hợp cho nguồn."

Sở hữu trí tuệ có thể là bí mật thương mại, bản quyền, thương hiệu và bằng sáng chế. Việc chiếm đoạt trái phép IP tạo thành nguy cơ đe dọa an toàn thông tin.

Nhân viên có thể có đặc quyền truy cập vào các loại IP khác nhau và có thể được yêu cầu sử dụng IP để tiến hành công việc hàng ngày.

Các tổ chức thường mua hoặc thuê IP của các tổ chức khác và phải tuân thủ thỏa thuận mua hoặc cấp phép để sử dụng hợp lý và có trách nhiệm. Vi phạm sở hữu trí tuệ phổ biến nhất là sử dụng trái phép hoặc sao chép tài sản trí tuệ dựa trên phần mềm, thường được gọi là vi phạm bản quyền phần mềm. Nhiều cá nhân và tổ chức không mua phần mềm theo yêu cầu của thỏa thuận cấp phép của chủ sở hữu. Bởi vì hầu hết phần mềm được cấp phép cho một người mua cụ thể, nên việc sử dụng phần mềm này bị hạn chế đối với một người dùng hoặc người dùng được chỉ định trong một tổ chức. Nếu người dùng sao chép chương trình sang máy tính khác mà không đảm bảo giấy phép khác hoặc chuyển như ợng giấy phép, người đó đã vi phạm bản quyền.

Tấn công phần mềm có chủ ý

Các cuộc tấn công phần mềm có chủ ý xảy ra khi một cá nhân hoặc một nhóm thiết kế và triển khai phần mềm để tấn công một hệ thống. Hầu hết phần mềm này được gọi là mã độc hoặc phần mềm độc hại hoặc đôi khi là phần mềm độc hại. Các thành phần hoặc chương trình phần mềm này được thiết kế để làm hỏng, phá hủy hoặc từ chối dịch vụ đối với các hệ thống đích.

Một số trường hợp phổ biến hơn của mã độc hại là vi-rút và sâu máy tính, ngựa thành Troy, bom logic và cửa sau.

Vi-rút: Vi-rút máy tính bao gồm các đoạn mã thực hiện các hành động độc hại. Mã này hoạt động rất giống một mầm bệnh vi rút tấn công động vật và thực vật, sử dụng bộ máy sao chép của chính tế bào để truyền cuộc tấn công ra ngoài mục tiêu ban đầu. Mã này tự gắn vào một chương trình hiện có và kiểm soát quyền truy cập của chương trình đó vào máy tính được nhắm mục tiêu. Sau đó, chương trình mục tiêu do vi-rút kiểm soát sẽ thực hiện kế hoạch của vi-rút bằng cách sao chép chính nó vào các hệ thống được nhắm mục tiêu bổ sung.

Một trong những phương pháp phổ biến nhất của vi-rút lây truyền là qua tệp đính kèm e-mail các tập tin. Hầu hết các tổ chức chặn các tệp đính kèm e-mail thuộc một số loại nhất định và cũng lọc tất cả e-mail để tìm vi-rút đã biết. Trước đây, vi-rút là những sinh vật di chuyển chậm chuyển tải trọng vi-rút thông qua chuyển động cồng kềnh của đĩa mềm từ hệ thống này sang hệ thống khác. Giờ đây, các máy tính được kết nối mạng và các chương trình e-mail chứng tỏ là mảnh đất mỡ cho vi-rút máy tính trừ khi có các biện pháp kiểm soát thích hợp.

Trong số các loại vi-rút hệ thống thông tin phổ biến nhất là vi-rút macro, được nhúng trong mã macro thực thi tự động được sử dụng bởi các trình xử lý văn bản, trang tính và ứng dụng cơ sở dữ liệu và vi-rút khởi động, lây nhiễm các tệp hệ điều hành chính nằm trong máy tính. giày cao cỏ.

Sâu: Được đặt tên theo con Sán dây trong tiểu thuyết The Shockwave Rider của John Brunner, sâu là một chương trình độc hại tự sao chép liên tục mà không yêu cầu môi trường chương trình khác. Sâu có thể tiếp tục tự sao chép cho đến khi chúng lấp đầy hoàn toàn các tài nguyên có sẵn, chẳng hạn như bộ nhớ, dung lượng ổ cứng và băng thông mạng.

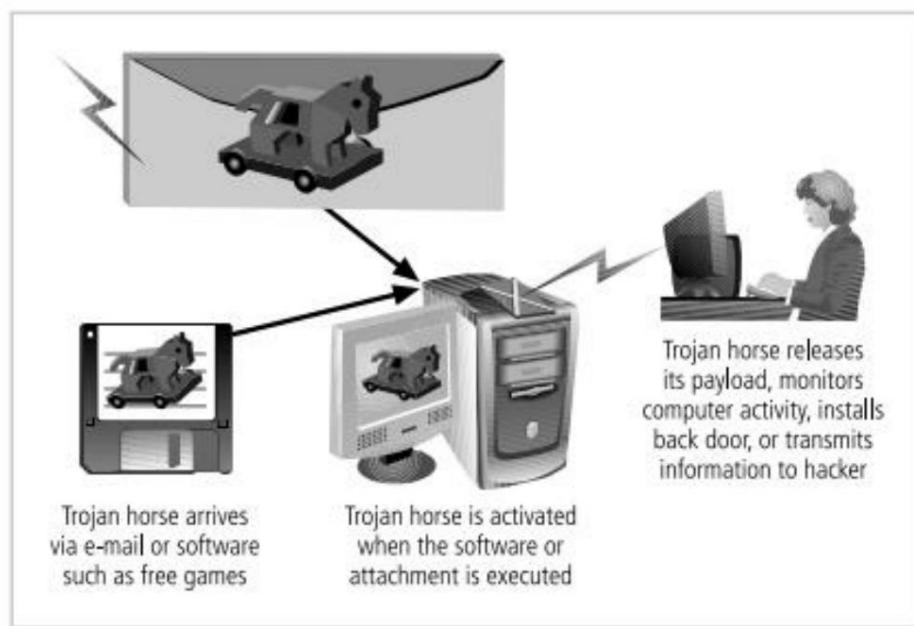
Hành vi phức tạp của sâu có thể bắt đầu có hoặc không có người dùng tải xuống hoặc thực thi tệp. Khi sâu đã lây nhiễm vào máy tính, nó có thể tự phân phối lại tới tất cả các địa chỉ email được tìm thấy trên hệ thống bị lây nhiễm.

Hơn nữa, một con sâu có thể gửi các bản sao của chính nó lên tất cả các máy chủ Web mà hệ thống bị nhiễm có thể tiếp cận, để những người dùng sau đó truy cập các trang web đó trở thành

bị lây nhiễm. Sâu cũng lợi dụng các chia sẻ mở được tìm thấy trên mạng có đặt hệ thống bị nhiễm, đặt các bản sao đang hoạt động của mã sâu lên máy chủ để người dùng của những chia sẻ đó có khả năng bị nhiễm.

Trojan Horses: Trojan horse ([xem Hình 2-1](#)) là các chương trình phần mềm che giấu bản chất thực sự của chúng và chỉ tiết lộ hành vi được thiết kế của chúng khi được kích hoạt.

Trojan thường được ngụy trang dưới dạng các phần mềm hữu ích, thư vị hoặc cần thiết, chẳng hạn như các tệp readme.exe thường được bao gồm trong các gói phần mềm chia sẻ hoặc phần mềm miễn phí. Thật không may, giống như tên gọi của chúng trong truyền thuyết Hy Lạp, một khi ngựa thành Troy được đưa vào hệ thống, chúng sẽ được kích hoạt và có thể tàn phá người dùng cả tin.



[Hình 2-1. Tấn công ngựa thành Troia](#)

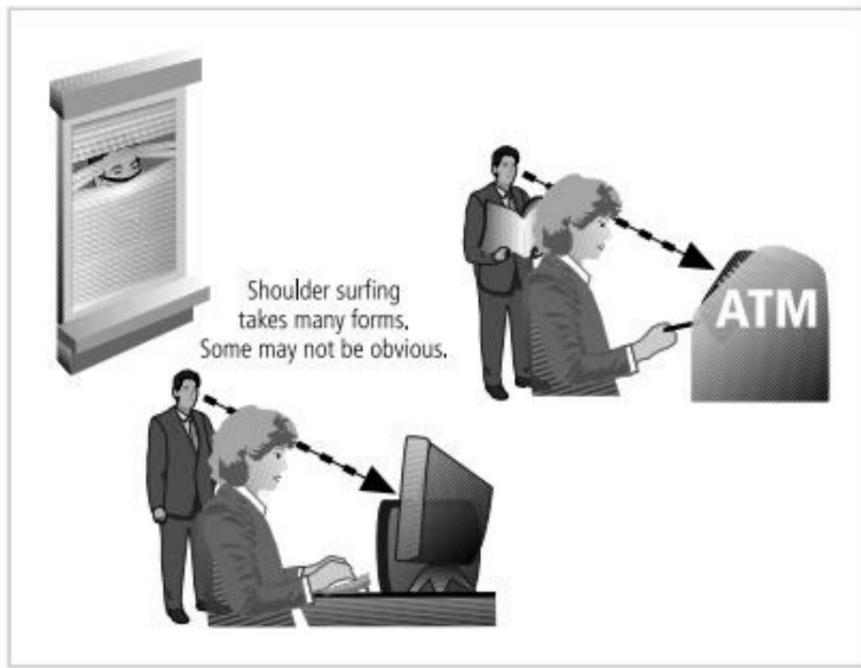
Cửa sau hoặc Cửa bẩy: Vi-rút hoặc sâu có thể có tải trọng cài đặt thành phần cửa sau hoặc cửa bẩy trong hệ thống, cho phép kẻ tấn công truy cập vào hệ thống theo ý muốn với các đặc quyền đặc biệt. Ví dụ về các loại tải trọng này bao gồm Subeven và Back Orifice

Các mối đe dọa đa hình: Một trong những thách thức lớn nhất để chống lại virus và sâu máy tính là sự xuất hiện của các mối đe dọa đa hình. Mối đe dọa đa hình là mối đe dọa theo thời gian thay đổi cách nó xuất hiện đối với các chương trình phần mềm chống vi-rút, khiến nó không thể phát hiện được bằng các kỹ thuật tìm kiếm chữ ký được cấu hình sẵn. Những vi-rút và sâu này thực sự phát triển, thay đổi kích thước của chúng và các đặc điểm tệp bên ngoài khác để tránh bị các chương trình phần mềm chống vi-rút phát hiện.

Trò lừa bịp về vi-rút và sâu máy tính: Cũng khó chịu như vi-rút và sâu máy tính, có lẽ người ta sẽ dành nhiều thời gian và tiền bạc hơn để giải quyết các trò lừa bịp về vi-rút. Những người có ý tốt có thể phá vỡ sự hài hòa và dòng chảy của một tổ chức khi họ gửi e-mail nhóm cảnh báo về những vi-rút đư ợc cho là nguy hiểm không tồn tại. Khi mọi người không tuân theo quy trình báo cáo vi-rút, mạng sẽ trở nên quá tải và lãng phí nhiều thời gian và năng lượng khi người dùng chuyển tiếp thông báo cảnh báo tới mọi người mà họ biết, đăng thông báo lên bảng thông báo và cố gắng cập nhật phần mềm bảo vệ chống vi-rút của họ.

Gián điệp hoặc xâm phạm

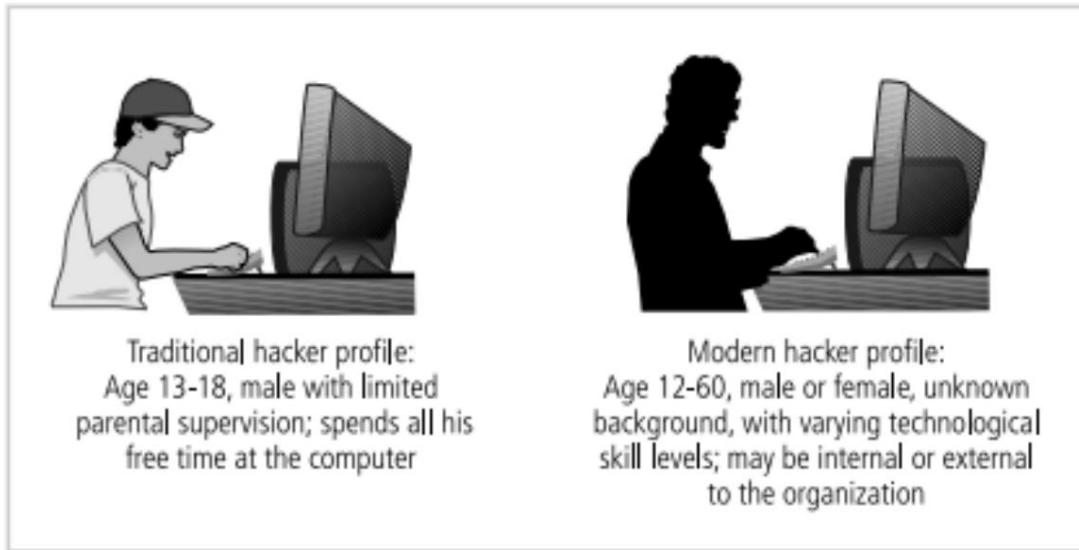
Gián điệp hoặc xâm phạm là một danh mục phổ biến và nổi tiếng của các hoạt động điện tử và con người có thể vi phạm tính bảo mật của thông tin. Khi một cá nhân trái phép giành đư ợc quyền truy cập vào thông tin mà một tổ chức đang cố gắng bảo vệ, hành động đó đư ợc phân loại là gián điệp hoặc xâm phạm. Kẻ tấn công có thể sử dụng nhiều phương pháp khác nhau để truy cập thông tin đư ợc lưu trữ trong hệ thống thông tin. Một số kỹ thuật thu thập thông tin khá hợp pháp, chẳng hạn như sử dụng trình duyệt Web để thực hiện nghiên cứu thị trường. Những kỹ thuật hợp pháp này đư ợc gọi chung là trí thông minh cạnh tranh. Khi những người thu thập thông tin sử dụng các kỹ thuật vươn qua người օng của những gì hợp pháp hoặc đạo đức, họ đang tiến hành hoạt động gián điệp công nghiệp. Nhiều quốc gia đư ợc coi là đồng minh của Hoa Kỳ tham gia vào hoạt động gián điệp công nghiệp chống lại các tổ chức của Mỹ. Khi các chính phủ nước ngoài tham gia, các hoạt động này đư ợc coi là gián điệp và là mối đe dọa đối với an ninh quốc gia. Một số hình thức gián điệp là công nghệ tương đối thấp. Một ví dụ, đư ợc gọi là lừa ảo vai đư ợc minh họa trong [Hình 2-2](#).



Hình 2-2. lư ợt vai

Hành vi xâm phạm có thể dẫn đến các hành động thực hoặc ảo trái phép cho phép người thu thập thông tin vào cơ sở hoặc hệ thống mà họ không được phép vào. Kiểm soát đôi khi đánh dấu ranh giới của lãnh thổ ảo của một tổ chức. Những ranh giới này đưa ra thông báo cho những kẻ xâm phạm rằng họ đang xâm phạm không gian mạng của tổ chức. Các nguyên tắc xác thực và ủy quyền hợp lý có thể giúp các tổ chức bảo vệ hệ thống và thông tin có giá trị. Các phương pháp và công nghệ kiểm soát này sử dụng nhiều lớp hoặc nhiều yếu tố để bảo vệ chống truy cập trái phép.

Thủ phạm cốt điểm của hoạt động gián điệp hoặc xâm phạm là tin tặc. Tin tặc là "những người sử dụng và tạo phần mềm máy tính để truy cập thông tin một cách bất hợp pháp." Tin tặc thường được tôn vinh trong các tài khoản hư cấu là những người lén lút điều khiển mề cung mạng máy tính, hệ thống và dữ liệu để tìm thông tin giải quyết bí ẩn hoặc tiết kiệm thời gian. Truyền hình và phim ảnh tràn ngập hình ảnh các hacker như những anh hùng hoặc nữ anh hùng. Tuy nhiên, cuộc sống thực sự của hacker còn tràn tục hơn nhiều ([xem Hình 2-3](#)). Trong thế giới thực, tin tặc thường dành nhiều giờ để kiểm tra các loại và cấu trúc của hệ thống để nhắm mục tiêu và sử dụng kỹ năng, mưu mẹo hoặc gian lận để cố gắng vượt qua các biện pháp kiểm soát được đặt xung quanh thông tin là tài sản của người khác.



Hình 2-3. Hồ sơ tin tặc

Nhìn chung có hai cấp độ kỹ năng giữa các tin tặc. Đầu tiên là chuyên gia tin tặc, hoặc tin tặc ưu tú, người phát triển các tập lệnh phần mềm và khai thác chương trình được sử dụng bởi những người thuộc loại thứ hai, tin tặc mới làm quen hoặc không có kỹ năng. Tin tặc lão luyện thường là người thành thạo một số ngôn ngữ lập trình, giao thức mạng và hệ điều hành, đồng thời cũng thể hiện sự thành thạo về môi trường kỹ thuật của hệ thống được nhắm mục tiêu đã chọn. Khi một hacker chuyên nghiệp chọn một hệ thống mục tiêu, khả năng anh ta hoặc cô ta sẽ xâm nhập thành công vào hệ thống là rất cao. May mắn thay cho nhiều tổ chức được bảo vệ kém trên thế giới, về cơ bản có ít tin tặc chuyên nghiệp hơn so với tin tặc mới vào nghề.

2.1. Trả lời các câu hỏi

1. Tại sao không có cá nhân, tổ chức nào mua phần mềm bắt buộc bởi các thỏa thuận cấp phép của chủ sở hữu?
2. Các chương trình phần mềm mã độc nào thuê đúng bản chất và tiết lộ hành vi được thiết kế của họ chỉ khi được kích hoạt?
3. Tại sao các thành phần phần mềm hoặc chương trình của mã độc được thiết kế?
4. Những loại tấn công phần mềm nào được đề cập trong văn bản?
5. IP là viết tắt của từ gì? Nó là gì?
6. Ai được coi là hacker lão luyện?

7. Hacker là ai? Các cấp độ kỹ năng nào được phân chia giữa các tin tặc?

8. Một trong những phương thức lây truyền virus phổ biến nhất là gì?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI).

Sửa lỗi sai (F).

1. Bí mật thư riêng mại, bản quyền, thư hiệu và bằng sáng chế thư ờng được xem xét

Sở hữu trí tuệ.

A. Đúng

B. Sai

C. NI

2. Trú ớc đây, virus dễ dàng chuyển tải trọng virus từ hệ thống này sang hệ thống khác
hệ thống vì không có chương trình e-mail.

A. Đúng

B. Sai

C. NI

3. Giun không thể tiếp tục tự nhân lên cho đến khi chúng
lấp đầy hoàn toàn các tài nguyên có sẵn, chẳng hạn như bộ nhớ, dung lượng ổ cứng và
bằng thông mạng.

A. Đúng

B. Sai

C. NI

4. Trú ớc khi Trojan horse có thể lây nhiễm vào máy, người dùng phải tải xuống
phía máy chủ của ứng dụng độc hại.

A. Đúng

B. Sai

C. NI

5. Khi một tổ chức đặt máy chủ Web của mình dưới sự chăm sóc của dịch vụ lưu trữ Web
nhà cung cấp, nhà cung cấp đó chịu trách nhiệm đối với tất cả các dịch vụ Internet và
cho phần cứng và phần mềm hệ điều hành được sử dụng để vận hành Web

Địa điểm.

A. Đúng

B. Sai

C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và
các câu lệnh

1. Vi phạm IP phổ biến nhất là gì?

A. việc sử dụng trái phép hoặc sao chép trí tuệ dựa trên phần mềm
tài sản

B. việc sử dụng bất hợp pháp tài sản trí tuệ dựa trên phần mềm

C. A & B đều đúng

D. việc sử dụng bất hợp pháp tài sản trí tuệ dựa trên phần mềm

2..... là một danh mục nổi tiếng và rộng rãi về điện tử và con người các hoạt động có thể vi phạm tính bảo mật của thông tin.

A. Con ngựa thành Troy

C. Gián điệp hoặc xâm phạm

B. Một mối đe dọa đa hình

D. Sâu

3. Vi-rút hoặc sâu có thể có tải trọngcửa sau hoặc cửa bẫy thành phần trong một hệ thống, cho phép kẻ tấn công truy cập vào hệ thống theo ý muốn với đặc quyền.

A. thay đổi

C. cài đặt

B. đặt

D. thay thế

4.....là một cái mà theo thời gian sẽ thay đổi cách nó xuất hiện đối với phần mềm chống vi-rút các chương trình, làm cho nó không thể bị phát hiện bởi các kỹ thuật tìm kiếm cấu hình sẵn chữ ký.

A. Con ngựa thành Troy

C. Vi-rút

B. Một mối đe dọa đa hình

D. Sâu

5. Sâu cũng tận dụng các chia sẻ mở được tìm thấy trên mạng trong đó có một hệ thống bị lây nhiễm, đặt các bản sao đang hoạt động của mã sâu vào máy chủ người dùng của những chia sẻ đó có khả năng trở thành bị lây nhiễm.

A. để

C. sao cho

B. theo thứ tự mà

D. B & C đều đúng

6. Chương trình nào sau đây là chương trình độc hại tự sao chép liên tục, mà không yêu cầu một môi trường chương trình khác?

A. Cửa đen

C. Vi-rút

B. Con sâu

D. Trò lừa bịp

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?

2. Chọn một trong các mối đe dọa trong văn bản và trình bày.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi

1. Bạn biết những thảm họa thiên nhiên nào?
2. Thiên tai có được coi là mối đe dọa trong an toàn thông tin không? Đưa ra cho một ví dụ để hỗ trợ ý tư tưởng của bạn.
3. Trộm cắp là gì? Bạn thuộc loại trộm cắp nào trong bảo mật thông tin biết rõ?
4. Mối đe dọa nào nguy hiểm nhất trong an toàn thông tin? Tại sao?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Đe dọa (2)

Lực lượng tự nhiên

Các lực lượng tự nhiên, bất khả kháng hoặc thiên tai có thể gây ra một số mối đe dọa nguy hiểm nhất, bởi vì chúng thường xảy ra với rất ít cảnh báo và nằm ngoài tầm kiểm soát của con người. Những mối đe dọa này, bao gồm các sự kiện như hỏa hoạn, lũ lụt, động đất và sét cũng như núi lửa phun trào và sự phá hoại của côn trùng, có thể làm gián đoạn không chỉ cuộc sống của các cá nhân mà còn cả việc lưu trữ, truyền tải và sử dụng thông tin. Một số mối đe dọa phổ biến hơn trong nhóm này là hỏa hoạn, lũ lụt, động đất, sét, lở đất hoặc lở đất, lốc xoáy, cuồng phong, Sóng thần, phóng tĩnh điện (ESD) và ô nhiễm bụi.

Lỗi hoặc Thất bại của Con người

Danh mục này bao gồm các hành vi được thực hiện mà không có ý định hoặc mục đích xấu bởi con người dùng được ủy quyền. Khi mọi người sử dụng hệ thống thông tin, sai lầm xảy ra. Thiếu kinh nghiệm, đào tạo không đúng cách và các giả định không chính xác chỉ là một vài điều có thể gây ra những rủi ro này. Bất kể nguyên nhân là gì, ngay cả những sai lầm vô hại cũng có thể gây ra thiệt hại lớn.

Một trong những mối đe dọa lớn nhất đối với an ninh thông tin của một tổ chức là chính nhân viên của tổ chức đó. Nhân viên là tác nhân đe dọa gần nhất với dữ liệu của tổ chức. Vì nhân viên sử dụng dữ liệu trong các hoạt động hàng ngày để tiến hành công việc kinh doanh của tổ chức nên những sai lầm của họ là mối đe dọa nghiêm trọng đối với

tính bảo mật, tính toàn vẹn và tính sẵn có của dữ liệu-thật chí, như **Hình 2-4** gợi ý, liên quan đến các mối đe dọa từ bên ngoài.

Điều này là do những sai lầm của nhân viên có thể dễ dàng dẫn đến những điều sau: tiết lộ dữ liệu đư ợc phân loại, nhập dữ liệu sai, vô tình xóa hoặc sửa đổi dữ liệu, lưu trữ dữ liệu ở những khu vực không đư ợc bảo vệ và không bảo vệ đư ợc thông tin. Để thông tin đã phân loại ở những nơi không đư ợc bảo vệ, chẳng hạn như trên máy tính để bàn, trên trang Web hoặc thậm chí trong thùng rác, đều là mối đe dọa đối với việc bảo vệ thông tin cũng như cá nhân tìm cách khai thác thông tin, bởi vì một người sự bất cẩn có thể tạo ra lỗ hổng và do đó là cơ hội cho kẻ tấn công.

Nhiều sai sót hoặc sai sót do con người gây ra có thể đư ợc ngăn chặn bằng các hoạt động đào tạo và nâng cao nhận thức liên tục, cũng như bằng các biện pháp kiểm soát, từ các quy trình đơn giản, chẳng hạn như yêu cầu người dùng nhập một lệnh quan trọng hai lần, đến các quy trình phức tạp hơn, chẳng hạn như xác minh các lệnh bằng một bên thứ hai. Một ví dụ về cái sau là hiệu suất của các hành động khôi phục khóa trong các hệ thống PKI. Nhiều ứng dụng quân sự đư ợc tích hợp sẵn các biện pháp kiểm soát mạnh mẽ, phê duyệt kép. Một số hệ thống có khả năng mất dữ liệu hoặc ngừng hoạt động hệ thống cao sử dụng các hệ thống chuyên gia để giám sát hành động của con người và yêu cầu xác nhận các thông tin đầu vào quan trọng.



Hình 2-4. Hành động lỗi hoặc thất bại của con người

Thông tin tống tiền xảy ra khi kẻ tấn công hoặc người trong cuộc đánh cắp thông tin từ một hệ thống máy tính và yêu cầu bồi thường cho việc trả lại hoặc cho một thỏa thuận không tiết lộ nó. Tống tiền là phổ biến trong hành vi trộm cắp số thẻ tín dụng. Ví dụ: nhà bán lẻ dựa trên web CD Universe là nạn nhân của một vụ đánh cắp tệp dữ liệu chứa thông tin thẻ tín dụng của khách hàng. Thủ phạm là một hacker người Nga tên là Maxus, kẻ đã hack nhà cung cấp trực tuyến và đánh cắp hàng trăm nghìn số thẻ tín dụng. Khi công ty từ chối trả khoản tiền tống tiền 100.000 đô la, anh ta đã đăng số thẻ lên một trang web, cung cấp chúng cho cộng đồng tội phạm.

Trang web của anh ấy trở nên nổi tiếng đến mức anh ấy phải hạn chế quyền truy cập.

trộm cắp

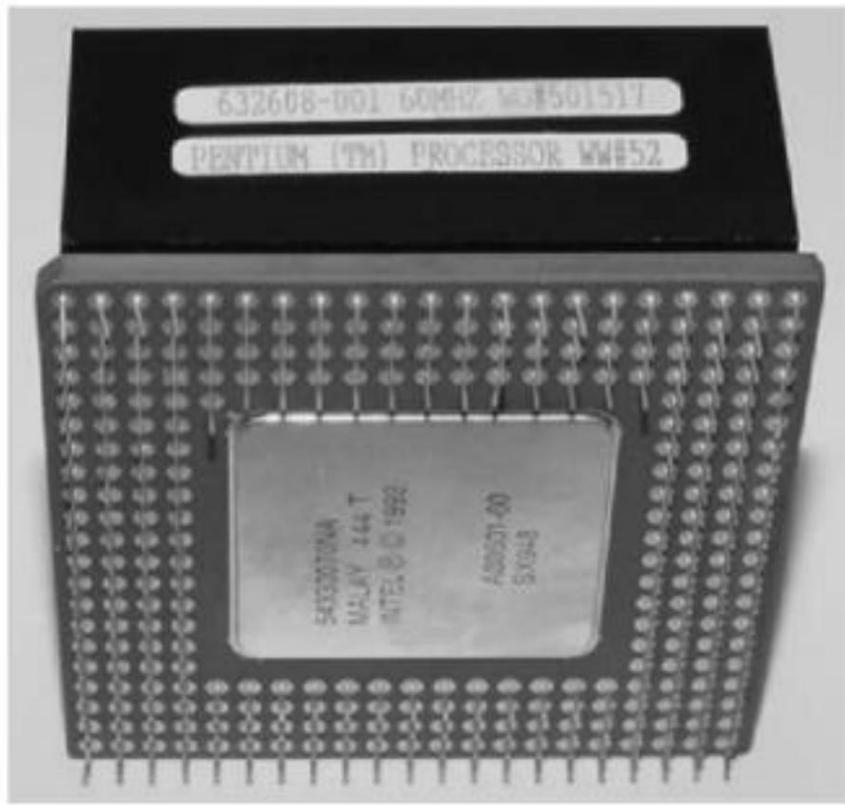
Mỗi đe dọa trộm cắp–việc chiếm đoạt bất hợp pháp tài sản của người khác, có thể là tài sản vật chất, điện tử hoặc trí tuệ–là điều thường xuyên xảy ra. Giá trị của thông tin bị giảm đi khi nó bị sao chép mà chủ sở hữu không hề hay biết. Hành vi trộm cắp vật lý có thể được kiểm soát khá dễ dàng bằng nhiều biện pháp khác nhau, từ khóa cửa đến nhân viên an ninh được đào tạo và lắp đặt hệ thống báo động. Tuy nhiên, trộm cắp điện tử là một vấn đề phức tạp hơn để quản lý và kiểm soát. Khi ai đó đánh cắp một vật thể, sự mất mát dễ dàng được phát hiện; nếu nó có bất kỳ tầm quan trọng nào, thì sự vắng mặt của nó được ghi nhận. Khi thông tin điện tử bị đánh cắp, tội phạm không phải lúc nào cũng rõ ràng. Nếu kẻ trộm thông minh và che giấu dấu vết của chúng cẩn thận, không ai có thể

bao giờ biết về tội ác cho đến khi quá muộn.

Lỗi hoặc lỗi phần cứng kỹ thuật

Lỗi hoặc lỗi phần cứng kỹ thuật xảy ra khi nhà sản xuất phân phối thiết bị có lỗi hỏng đã biết hoặc chưa biết. Những khuyết điểm này có thể khiến hệ thống hoạt động ngoài các thông số dự kiến, dẫn đến dịch vụ không đáng tin cậy hoặc thiếu tính khả dụng. Một số lỗi là thiết bị đầu cuối–nghĩa là chúng dẫn đến việc thiết bị bị mất không thể khôi phục được. Một số lỗi không liên tục, tức là chúng chỉ biểu hiện theo định kỳ, dẫn đến các lỗi không dễ lặp lại và do đó, thiết bị đôi khi có thể ngừng hoạt động hoặc hoạt động theo những cách không mong muốn.

Một trong những lỗi phần cứng nổi tiếng nhất là chip Intel Pentium II ([xem Hình 2-5](#), có một lỗi dẫn đến lỗi tính toán trong một số điều kiện nhất định).
trừ ờng hợp.



Hình 2-5. Chip Pentium II

Lỗi phần mềm kỹ thuật hoặc lỗi

Một lượng lớn mã máy tính được viết, sửa lỗi, xuất bản và bán trước khi tất cả các lỗi của chúng được phát hiện và giải quyết. Đôi khi, sự kết hợp của một số phần mềm và phần cứng cho thấy các lỗi mới. Những lỗi này bao gồm từ lỗi đến các điều kiện lỗi chưa được kiểm tra. Đôi khi những lỗi này không phải là lỗi, mà là những lỗi tắt có mục đích do các lập trình viên để lại vì những lý do lành tính hoặc ác tính. Nói chung, các lỗi tắt truy cập vào các chương trình bỏ qua kiểm tra bảo mật được gọi là cửa bẫy và có thể gây ra các vi phạm bảo mật nghiêm trọng. Các lỗi phần mềm phổ biến đến mức toàn bộ các trang Web được dành riêng để ghi lại chúng. Trong số những thử thách được sử dụng nhất là Bugtraq, được tìm thấy tại www.securityfocus.com, cung cấp thông tin cập nhật từng phút về các lỗi hỏng bảo mật mới nhất, cũng như một kho lưu trữ rất kỹ lưỡng các lỗi trong quá khứ.

Ngoài các mối đe dọa được đề cập ở trên, chính sách hoặc kế hoạch của tổ chức còn thiêu, không đầy đủ hoặc không đầy đủ; kiểm soát bị thiếu, không đầy đủ hoặc không đầy đủ; phá hoại hoặc phá hoại; và sự lạc hậu về công nghệ phải được xem xét.

2.1. Trả lời các câu hỏi

1. Tại sao sai lầm của nhân viên là mối đe dọa nghiêm trọng đối với bảo mật, toàn vẹn và sẵn có của dữ liệu?
2. Những mối đe dọa nào đư ợc đề cập trong văn bản? Cái nào là mối đe dọa lớn nhất đối với một tổ chức?
3. Làm thế nào để kiểm soát hành vi trộm cắp?
4. Tại sao trộm cắp điện tử là một vấn đề phức tạp hơn để quản lý và kiểm soát?
5. Maxus là ai? Anh ấy đã làm gì? Cung cấp chi tiết cho hành động của mình.
6. Có thể ngăn ngừa lỗi hoặc sai sót của con người không? Làm thế nào nó có thể đư ợc bảo vệ?
7. Thiên tai có đư ợc coi là mối đe dọa trong an toàn thông tin không? Gi^t chung gây ra những tác hại gì?
8. Nhân viên thư ờng mắc lỗi nào khi sử dụng thông tin hệ thống?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa lỗi sai (F).

1. Kinh nghiệm, đào tạo phù hợp và những giả định không chính xác chỉ là một số ít những thứ có thể gây ra những bất hạnh này.
A. Đúng B. Sai C. NI
2. Có thể ngăn ngừa nhiều sai sót hoặc thất bại của con người bằng cách đào tạo và liên tục các hoạt động nhận thức, mà còn với các biện pháp kiểm soát, từ các thủ tục đơn giản.
A. Đúng B. Sai C. NI
3. Một trong những lỗi phần cứng nổi tiếng nhất là của Intel Pentium II chip, có lỗi dẫn đến lỗi tính toán theo một số trữ ờng hợp.
A. Đúng B. Sai C. NI
4. Số lư ợng lớn mã máy tính đư ợc viết, sửa lỗi, xuất bản và đư ợc bán trước khi tất cả các lỗi của chúng đư ợc phát hiện và giải quyết.
A. Đúng B. Sai C. NI
5. Lỗi hoặc lỗi phần cứng kỹ thuật luôn là một trong những lỗi phổ biến nhất chủ đe nguy hiểm trong bảo mật thông tin.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất để hoàn thành các câu hỏi và câu sau

1. xảy ra khi kẻ tấn công hoặc người trong cuộc đáng tin cậy đánh cắp thông tin từ một hệ thống máy tính và yêu cầu bồi thư ờng cho sự trở lại của nó hoặc cho một thỏa thuận không tiết lộ nó.

A. Tống tiền thông tin

C. Lỗi kỹ thuật

B. Lỗi Con Người

D. B & D đúng

2. xảy ra khi nhà sản xuất phân phối thiết bị có lỗ hỏng đã biết hoặc chưa biết.

A. Lỗi phần cứng kỹ thuật

C. Trộm Cắp

B. kiểm soát không đầy đủ

D. Lỗi kỹ thuật

3. Mối đe dọa nào nguy hiểm nhất đối với thông tin của tổ chức
Bảo vệ?

A. Tống tiền thông tin

C. Phá hoại

B. Nhân viên của chính tổ chức.

D. Thiếu điều khiển

4. Giá trị của thông tin là khi nó được sao chép mà không có sự xác nhận của chủ sở hữu.
kiến thức.

A. giảm đi

C. A & B đúng

B. giảm đi

D. thu nhỏ

5. Số lượng lớn được viết, sửa lỗi, xuất bản và bán
trước khi tất cả các lỗi của chúng được phát hiện và giải quyết.

Một phần mềm

C. mã máy tính

B. phần cứng

D. ngôn ngữ máy tính

6. có thể đưa ra một số mối đe dọa nguy hiểm nhất, bởi vì chúng
thường xảy ra với rất ít cảnh báo và nằm ngoài tầm kiểm soát của con người.

A. Trưởng hợp bất khả kháng

C. Lực lượng tự nhiên

B. Công vụ của Đức Chúa Trời

D. Tất cả đều đúng

3. Phát biểu

1. Qua văn bản em rút ra được những nội dung chính nào?
2. Chọn hai trong số các mối đe dọa trong văn bản và trình bày nó.

ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi

1. Tân công là gì?
2. Bạn biết những tấn công nào trong bảo mật thông tin? Cái nào là nguy hiểm nhất?
3. DDoS có nghĩa là gì? Nó là gì?
4. Bạn nghĩ rằng mật khẩu của mình có thể bị tấn công? Nếu có, làm thế nào bạn có thể mật khẩu bị tấn công?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Tấn công (1)

Tấn công là hành động lợi dụng lỗ hổng để xâm nhập hệ thống được kiểm soát. Nó được thực hiện bởi một tác nhân đe dọa gây thiệt hại hoặc đánh cắp thông tin hoặc tài sản vật chất của một tổ chức. Lỗ hổng bảo mật là một điểm yếu được xác định trong một hệ thống được kiểm soát, trong đó các biện pháp kiểm soát không có hoặc không còn hiệu quả. Không giống như các mối đe dọa luôn hiện hữu, các cuộc tấn công chỉ tồn tại khi một hành động cụ thể có thể gây ra tổn thất. Ví dụ, nguy cơ thiệt hại do giông bão xuất hiện trong suốt mùa hè ở nhiều nơi, như một cuộc tấn công và nguy cơ tổn thất liên quan chỉ tồn tại trong thời gian xảy ra giông bão thực sự. Các phần sau đây thảo luận về từng loại tấn công chính được sử dụng để chống lại các hệ thống được kiểm soát.

Mã độc

Cuộc tấn công bằng mã độc hại bao gồm việc thực thi vi-rút, sâu máy tính, ngựa thành Troy và các tập lệnh Web đang hoạt động với mục đích phá hủy hoặc đánh cắp thông tin. Cuộc tấn công bằng mã độc tiên tiến nhất là sâu đa hình hoặc đa vector.

Các chương trình tấn công này sử dụng tối đa sáu vectơ tấn công đã biết để khai thác nhiều lỗ hổng trong các thiết bị hệ thống thông tin thường thấy. Có lẽ minh họa tốt nhất cho một cuộc tấn công như vậy vẫn là sự bùng nổ của Nimda vào tháng 9 năm 2001, sử dụng năm trong số sáu vectơ để tự lây lan với tốc độ đáng kinh ngạc. TruSecure Corporation, một nguồn tin công nghiệp về thông kê và giải pháp bảo mật thông tin, báo cáo rằng Nimda đã lan rộng khắp không gian địa chỉ Internet của 14 quốc gia trong vòng chưa đầy 25 phút.

Các dạng phần mềm độc hại khác bao gồm các ứng dụng phần mềm bí mật—các bot thư ờng là công nghệ đư ợc sử dụng để triển khai Trojan Horse, bom logic, cửa sau; phần mềm gián điệp là “bất kỳ công nghệ nào hỗ trợ thu thập thông tin về một người hoặc tổ chức mà họ không biết và nó đư ợc đặt trên máy tính để bí mật thu thập thông tin về người dùng và báo cáo thông tin đó”; và phần mềm quảng cáo —là “bất kỳ chương trình phần mềm nào dành cho mục đích tiếp thị, chẳng hạn như chương trình đư ợc sử dụng để phân phối và hiển thị các biểu ngữ quảng cáo hoặc cửa sổ bật lên trên màn hình của người dùng hoặc theo dõi hoạt động mua hàng hoặc sử dụng trực tuyến của người dùng”. Mỗi thành phần mã ẩn này có thể đư ợc

đư ợc sử dụng để thu thập thông tin từ hoặc về người dùng mà sau đó có thể đư ợc sử dụng trong một kỹ thuật xã hội hoặc tấn công đánh cắp danh tính.

trò lừa bịp

Một cuộc tấn công xảo quyệt hơn vào hệ thống máy tính là truyền một trò lừa bịp vi-rút có đính kèm vi-rút thực. Khi cuộc tấn công đư ợc che giấu trong một thông báo có vẻ hợp pháp, những người dùng không nghi ngờ sẽ dễ dàng phân phối nó hơn. Mặc dù những người dùng này đang cố gắng làm điều đúng đắn để tránh bị lây nhiễm, như cuối cùng họ lại gửi cuộc tấn công đến đồng nghiệp và bạn bè của họ và lây nhiễm cho nhiều người dùng trên đường đi.

cửa sau

Sử dụng cơ chế truy cập đã biết hoặc chưa biết trước đó và mới đư ợc phát hiện, kẻ tấn công có thể giành quyền truy cập vào hệ thống hoặc tài nguyên mạng thông qua cửa sau.

Đôi khi những mục nhập này bị bỏ lại bởi các nhà thiết kế hệ thống hoặc nhân viên bảo trì, và do đó đư ợc gọi là cửa bẫy. Một cửa bẫy rất khó bị phát hiện, bởi vì thư ờng thì người lập trình đặt nó vào vị trí cũng làm cho quyền truy cập đư ợc miễn trừ khỏi các tính năng ghi nhật ký kiểm tra thông thư ờng của hệ thống.

Crack mật khẩu

Cố gắng tính người ợc mật khẩu thư ờng đư ợc gọi là bẻ khóa. Một cuộc tấn công bẻ khóa là một thành phần của nhiều cuộc tấn công từ điển (sẽ đư ợc đề cập ngay sau đây). Nó đư ợc sử dụng khi có thể lấy đư ợc một bản sao của tệp dữ liệu Trình quản lý tài khoản bảo mật (SAM), tệp này chứa biểu diễn băm của mật khẩu người dùng. Mật khẩu có thể đư ợc băm bằng cùng một thuật toán và đư ợc so sánh với kết quả đư ợc băm. Nếu chúng giống nhau, mật khẩu đã bị bẻ khóa.

Lực lượng vũ phu

Việc áp dụng tài nguyên máy tính và mạng để thử mọi kết hợp mật khẩu có thể đư ợc gọi là tấn công vũ phu. Vì cuộc tấn công vũ phu thư ờng đư ợc sử dụng để lấy mật khẩu của các tài khoản thư ờng đư ợc sử dụng nên đôi khi nó đư ợc gọi là cuộc tấn công mật khẩu. Nếu kẻ tấn công có thể thu hẹp phạm vi tài khoản mục tiêu, thì chúng có thể dành nhiều thời gian và tài nguyên hơn cho các tài khoản này. Đó là một lý do để luôn thay đổi tên và mật khẩu tài khoản quản trị viên mặc định của nhà sản xuất. Các cuộc tấn công bằng mật khẩu hiếm khi thành công đối với các hệ thống đã áp dụng các biện pháp bảo mật đư ợc khuyến nghị của nhà sản xuất. Các biện pháp kiểm soát giới hạn số lần thử truy cập không thành công đư ợc phép trên mỗi đơn vị thời gian đã trôi qua rất hiệu quả trừ ớc các cuộc tấn công vũ phu.

Từ điển

Tấn công từ điển là một biến thể của tấn công vũ phu thu hẹp phạm vi bằng cách chọn các tài khoản mục tiêu cụ thể và sử dụng danh sách các mật khẩu thư ờng đư ợc sử dụng (từ điển) thay vì kết hợp ngẫu nhiên. Các tổ chức có thể sử dụng các từ điển tương tự để không cho phép mật khẩu trong quá trình đặt lại và do đó bảo vệ chống lại các mật khẩu dễ đoán. Ngoài ra, các quy tắc yêu cầu số và/hoặc ký tự đặc biệt trong mật khẩu làm cho cuộc tấn công từ điển kém hiệu quả hơn.

Từ chối dịch vụ (DoS) và phân tán

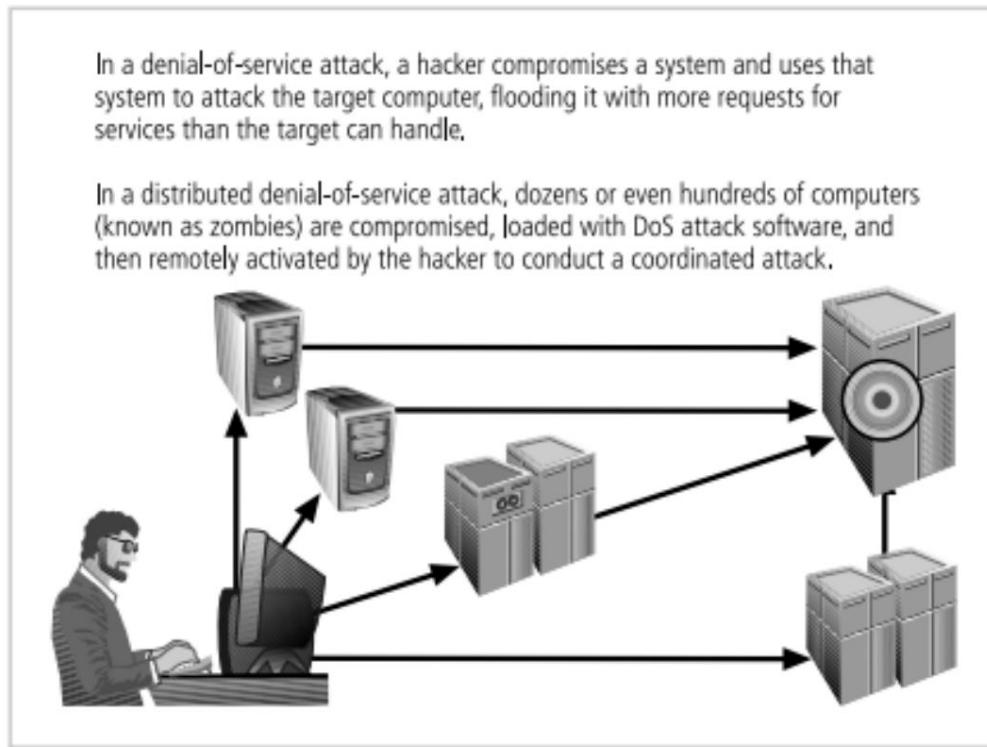
Từ chối dịch vụ (DDoS)

Trong một cuộc tấn công từ chối dịch vụ (DoS), kẻ tấn công gửi một số lượng lớn các yêu cầu kết nối hoặc thông tin tới một mục tiêu ([xem Hình 2-6](#)). Vì vậy, nhiều yêu cầu đư ợc thực hiện khiến hệ thống đích trở nên quá tải và không thể đáp ứng các yêu cầu dịch vụ hợp pháp. Hệ thống có thể gặp sự cố hoặc đơn giản là không thể thực hiện các chức năng thông thường. Tấn công từ chối dịch vụ phân tán (DDoS) là một cuộc tấn công trong đó một luồng yêu cầu phối hợp đư ợc khởi chạy nhằm vào mục tiêu từ nhiều địa điểm cùng một lúc. Hầu hết các cuộc tấn công DDoS đều diễn ra trư ớc một giai đoạn chuẩn bị, trong đó nhiều hệ thống, có thể là hàng nghìn, bị xâm phạm. Các máy bị xâm nhập bị biến thành zombie, các máy bị kẻ tấn công điều khiển từ xa (thư ờng bằng một lệnh đư ợc truyền) để tham gia vào cuộc tấn công. Các cuộc tấn công DDoS là khó chống lại nhất và hiện tại không có biện pháp kiểm soát nào mà bất kỳ tổ chức đơn lẻ nào cũng có thể áp dụng. Tuy nhiên, có một số nỗ lực hợp tác để kích hoạt hệ thống phòng thủ DDoS giữa các nhóm nhà cung cấp dịch vụ; trong số đó là Lộ trình đồng thuận để đánh bại các cuộc tấn công từ chối dịch vụ phân tán. Để sử

Trong ví dụ phổ biến, DDoS được coi là vũ khí hủy diệt hàng loạt trên Internet. Cuộc tấn công sâu MyDoom vào đầu năm 2004 được dự định là một cuộc tấn công DDoS nhằm vào www.sco.com (trang web của nhà cung cấp hệ điều hành UNIX) kéo dài từ ngày 1 tháng 2 năm 2004 cho đến ngày 12 tháng 2 năm 2004. Cuộc tấn công được cho là đã được hoàn trả cho sự thù địch được nhận thấy của Tập đoàn SCO đối với cộng đồng Linux nguồn mở.

Bất kỳ hệ thống nào được kết nối với Internet và cung cấp các dịch vụ mạng dựa trên TCP (chẳng hạn như máy chủ Web, máy chủ FTP hoặc máy chủ thư) đều dễ bị tấn công DoS.

Các cuộc tấn công DoS cũng có thể được khởi chạy nhằm vào các bộ định tuyến hoặc các hệ thống máy chủ mạng khác nếu các máy chủ này bật (hoặc bật) các dịch vụ TCP khác (ví dụ: tiếng vang).



Hình 2-6. Sự từ chối của dịch vụ tấn công

2.1. Trả lời các câu hỏi

1. Tấn công crack là gì? Khi nào nó được sử dụng?
2. Từ chối dịch vụ phân tán là gì?
3. Tại sao đôi khi tấn công vét cạn được gọi là tấn công mật khẩu?
4. Cuộc tấn công nào bao gồm việc thực thi virus, sâu máy tính, ngựa thành Troy và các tập lệnh Web đang hoạt động với mục đích phá hủy hoặc đánh cắp thông tin.

5. Tại sao cửa sổ khó bị phát hiện?
 6. Tại sao luôn có tên tài khoản quản trị viên mặc định của nhà sản xuất và mật khẩu đã thay đổi?
 7. Tại sao có nhiều yêu cầu khiền hệ thống mục tiêu trở nên quá tải và không thể đáp ứng các yêu cầu dịch vụ hợp pháp trong một cuộc tấn công DoS?
 8. Lỗi hỏng là gì?
- 2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI).
Sửa lỗi sai (F).
1. Rất nhiều hệ thống và người dùng gửi thông tin trên mạng cục bộ rõ ràng văn bản để những kẻ đánh hơi gây thêm rủi ro cho mạng.

A. Đúng	B. Sai	C. NI
---------	--------	-------
 2. Hoàn toàn không thể chống lại các cuộc tấn công DDoS vì chúng quá nguy hiểm.

A. Đúng	B. Sai	C. NI
---------	--------	-------
 3. Từ điển tự ngự có thể được sử dụng để cho phép mật khẩu trong quá trình thiết lập lại xử lý và do đó bảo vệ chống lại các mật khẩu dễ đoán của các tổ chức.

A. Đúng	B. Sai	C. NI
---------	--------	-------
 4. Nhiều quốc gia bị ảnh hưởng bởi mã độc có tên Nimda thời gian ngắn.

A. Đúng	B. Sai	C. NI
---------	--------	-------
 5. Một mật khẩu có thể được băm bằng cùng một thuật toán và được so sánh với kết quả băm.

A. Đúng	B. Sai	C. NI
---------	--------	-------

- 2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và các câu lệnh
1. Cuộc tấn công nào sau đây là một biến thể của cuộc tấn công vũ phu?

Một cuốn từ điển	B. Bẻ khóa mật khẩu
C. Cửa sau	D. Chơi khăm
 2. là bất kỳ công nghệ nào hỗ trợ thu thập thông tin về một người hoặc tổ chức mà họ không biết và nó được đặt trên một

máy tính để bí mật thu thập thông tin về người dùng và báo cáo.

A. Phần mềm quảng cáo

B. Từ chối dịch vụ

C. Từ điển

D. Phần mềm gián điệp

3. các cuộc tấn công là khó chống lại nhất, và có

hiện tại không có biện pháp kiểm soát nào mà bất kỳ tổ chức đơn lẻ nào cũng có thể áp dụng.

A. Bẻ khóa mật khẩu

C. DDoS

B. Từ điển

D. Cửa sau

4. thuộc loại mã độc tấn công tinh vi.

A. Đa hình

C. vector đa hướng

B. Con sâu

D. Tất cả đều đúng

5. Cuộc tấn công nào được coi là vũ khí hủy diệt hàng loạt trên Internet nhằm

sử dụng một ẩn dụ phổ biến?

A. DDoS

C. Cửa Sau

B. Cư ỡng bức

D. Crack mật khẩu

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?

2. Chọn ba trong số các cuộc tấn công trong văn bản và trình bày nó.

ĐỌC VÀ NÓI 4

1. Thảo luận các câu hỏi

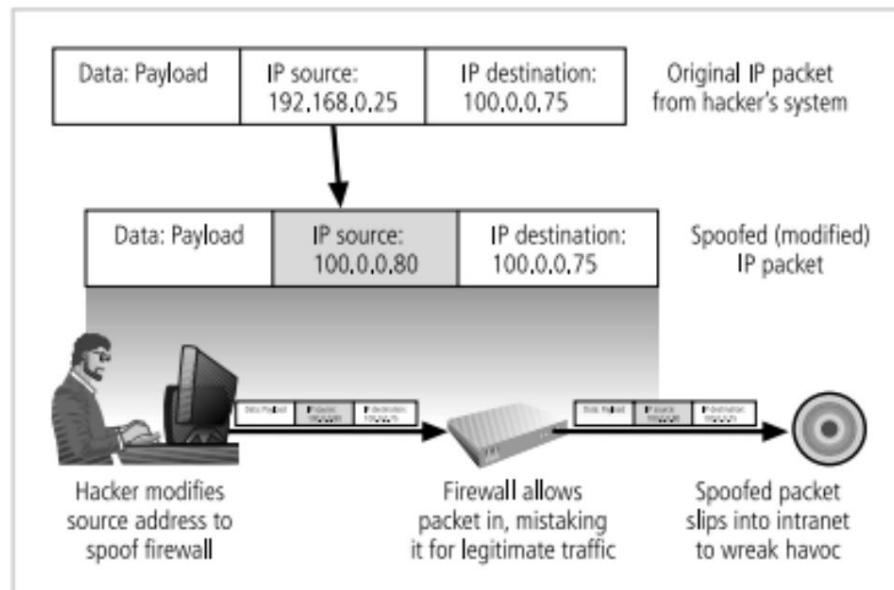
1. Bạn đã bao giờ nghe đến man-in-the-middle chưa? Nếu có, nó có ý nghĩa gì trong bạn ngôn ngữ?
2. Bạn biết gì về man-in-the-middle?
3. Bạn đã bao giờ nghe nói về kỹ thuật xã hội chưa? Nếu có, cho một số thông tin về nó.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Tấn công (2)

giả mạo

Giả mạo là một kỹ thuật được sử dụng để giành quyền truy cập trái phép vào máy tính, trong đó kẻ xâm nhập gửi thư có địa chỉ IP nguồn đã được giả mạo để cho biết rằng thư đến từ một máy chủ đáng tin cậy. Để tham gia giả mạo IP, tin tức sử dụng nhiều kỹ thuật khác nhau để lấy địa chỉ IP đáng tin cậy, sau đó sửa đổi tiêu đề gói để chèn các địa chỉ giả mạo này. Các bộ định tuyến và sắp xếp tư ờng lừa mới hơn có thể cung cấp khả năng bảo vệ chống giả mạo IP (xem Hình 2-7).

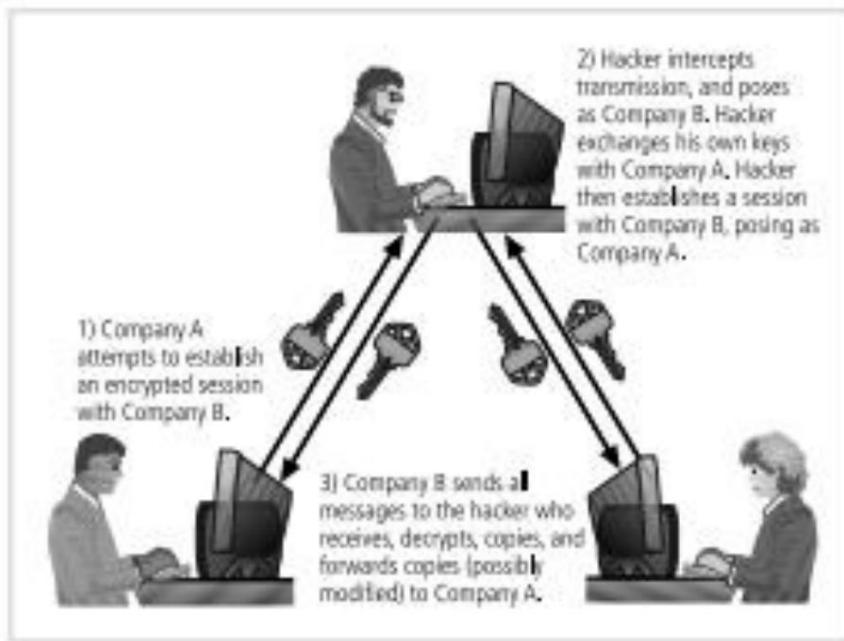


Hình 2-7. Giả mạo IP

Ngư ời trung gian

Trong cuộc tấn công chiêm quyền điều khiển TCP hoặc man-in-the-middle nổi tiếng, kẻ tấn công giám sát (hoặc đánh hơi) các gói từ mạng, sửa đổi chúng và chèn chúng trở lại mạng. Kiểu tấn công này sử dụng giả mạo IP để cho phép kẻ tấn công mạo danh một thực thể khác trên mạng. Nó cho phép kẻ tấn công nghe trộm cũng như thay đổi, xóa, định tuyến lại, thêm, giả mạo hoặc chuyển hướng dữ liệu.³⁹ Một biến thể của tấn công chiêm quyền điều khiển TCP, liên quan đến việc chặn một trao đổi khóa mã hóa, cho phép tin tặc hành động như một ngư ời vô hình -in-the-middle-tức là kẻ nghe lén-trên các liên lạc đư ợc mã hóa.

Hình 2-8 minh họa các cuộc tấn công này bằng cách chỉ ra cách tin tặc sử dụng khóa mã hóa công khai và riêng tư để chặn tin nhắn.



Hình 2-8. Ngư ời trung gian

Thư rác

Thư rác là e-mail thư rác mại không đư ợc yêu cầu. Mặc dù nhiều ngư ời coi thư rác là một môi phiền toái nhỏ hơn là một cuộc tấn công, như ng nó đã đư ợc sử dụng như một phư ơng tiện để tăng cư ờng các cuộc tấn công mã độc. Vào tháng 3 năm 2002, đã có báo cáo về mã độc đư ợc nhúng trong các tệp MP3 đư ợc đư a vào dưới dạng tệp đính kèm thư rác. Tuy nhiên, hậu quả đáng kể nhất của thư rác là sự lãng phí tài nguyên máy tính và con ngư ời. Nhiều tổ chức cố gắng đối phó với cơ n lũ thư rác bằng cách sử dụng các công nghệ lọc e-mail. Các tổ chức khác chỉ cần yêu cầu ngư ời dùng hệ thống thư xóa các thư không mong muốn.

Đánh bom thư

Một hình thức tấn công e-mail khác cũng là DoS được gọi là bom thư, trong đó kẻ tấn công định tuyên một lượng lớn e-mail đến mục tiêu. Điều này có thể được thực hiện bằng kỹ thuật xã hội (sẽ được thảo luận ngay sau đây) hoặc bằng cách khai thác các lỗi kỹ thuật khác nhau trong Giao thức vận chuyển thư đơn giản (SMTP). Mục tiêu của cuộc tấn công nhận được một khôi lượng lớn e-mail không được yêu cầu. Bằng cách gửi các e-mail lớn với thông tin tiêu đề giả mạo, kẻ tấn công có thể lợi dụng các hệ thống e-mail được cấu hình kém trên Internet và lừa chúng gửi nhiều e-mail đến một địa chỉ do kẻ tấn công chọn. Nếu nhiều hệ thống như vậy bị lừa tham gia vào sự kiện, địa chỉ e-mail mục tiêu sẽ bị chôn vùi dưới hàng ngàn hoặc

thậm chí hàng triệu e-mail không mong muốn.

người đánh hơi

Một trình thám thính là một chương trình hoặc thiết bị có thể theo dõi dữ liệu truyền qua mạng. Sniffer có thể được sử dụng cho cả chức năng quản lý mạng hợp pháp và đánh cắp thông tin. Các trình nghe lén trái phép có thể cực kỳ nguy hiểm đối với an ninh của mạng vì chúng hầu như không thể bị phát hiện và có thể được chèn vào hầu hết mọi nơi. Điều này khiến chúng trở thành vũ khí yêu thích trong kho vũ khí của tin tặc. Các trình nghe lén thường hoạt động trên các mạng TCP/IP, nơi mà đôi khi chúng được gọi là các trình nghe lén gói tin. Những kẻ đánh hơi tạo thêm rủi ro cho mạng vì nhiều hệ thống và người dùng gửi thông tin trên các mạng cục bộ ở dạng văn bản rõ ràng. Một chương trình nghe trộm hiển thị tất cả dữ liệu đi qua, bao gồm mật khẩu, dữ liệu bên trong tệp-chẳng hạn như tài liệu soạn thảo văn bản và màn hình chứa đầy dữ liệu nhạy cảm từ các ứng dụng.

Kỹ thuật xã hội

Trong bối cảnh bảo mật thông tin, kỹ thuật xã hội là quá trình sử dụng các kỹ năng xã hội để thuyết phục mọi người tiết lộ thông tin đăng nhập hoặc thông tin có giá trị khác cho kẻ tấn công. Có một số kỹ thuật lừa đảo xã hội, thường liên quan đến thủ phạm giả làm người có cấp bậc tổ chức cao hơn nạn nhân. Để chuẩn bị cho sự trình bày sai lệch này, thủ phạm có thể đã sử dụng các chiến thuật kỹ thuật xã hội chống lại những người khác trong tổ chức để thu thập thông tin đường như không liên quan, khi được sử dụng cùng nhau, sẽ làm cho sự trình bày sai lệch trở nên đáng tin cậy hơn. Chẳng hạn, bất kỳ ai cũng có thể kiểm tra trang Web của một công ty, hoặc thậm chí gọi đến tổng đài chính để lấy tên của CIO; kẻ tấn công sau đó có thể lấy được nhiều thông tin hơn bằng cách gọi cho những người khác trong công ty và khẳng định

thảm quyền (sai) của mình bằng cách đe dọa đến tên của CIO. Các cuộc tấn công kỹ thuật xã hội có thể liên quan đến các cá nhân giả làm nhân viên mới hoặc nhân viên hiện tại yêu cầu hỗ trợ để tránh bị sa thải. Đôi khi những kẻ tấn công đe dọa, phỉnh phờ hoặc cầu xin làm lung lay mục tiêu.

Có nhiều cuộc tấn công khác liên quan đến kỹ thuật xã hội. Một trong số đó là Phishing - nỗ lực lấy thông tin cá nhân hoặc thông tin tài chính từ một cá nhân, thường bằng cách giả làm một thực thể hợp pháp. Một biến thể là lừa đảo trực tiếp, một nhãn áp dụng cho bất kỳ cuộc tấn công lừa đảo có mục tiêu cao nào. Trong khi các cuộc tấn công lừa đảo thông thường nhằm vào càng nhiều người nhận càng tốt, thì một kẻ lừa đảo nhỏ sẽ gửi một tin nhắn có vẻ như là từ chủ lao động, đồng nghiệp hoặc đối tác hợp pháp khác đến một nhóm nhỏ hoặc thậm chí một người cụ thể. Cuộc tấn công này đôi khi được sử dụng để nhắm mục tiêu đến những người sử dụng một sản phẩm hoặc trang Web nhất định. Các cuộc tấn công lừa đảo sử dụng ba kỹ thuật chính, thường kết hợp với nhau: thao túng URL, giả mạo trang web và lừa đảo qua điện thoại.

Pharming

Pharming là "việc chuyển hướng lưu lượng truy cập Web hợp pháp (ví dụ: yêu cầu trình duyệt) đến một trang web bất hợp pháp nhằm mục đích lấy thông tin cá nhân. Pharming thường sử dụng Trojan, sâu máy tính hoặc các công nghệ vi rút khác để tấn công thanh địa chỉ của trình duyệt Internet để URL hợp lệ do người dùng nhập được sửa đổi thành URL của trang Web bất hợp pháp. Pharming cũng có thể khai thác Hệ thống tên miền (DNS) bằng cách khiến nó chuyển đổi tên máy chủ hợp pháp thành địa chỉ IP của trang web không hợp lệ; hình thức pharming này còn được gọi là ngộ độc bộ đệm DNS.

Thời gian tấn công

Một cuộc tấn công theo thời gian khám phá nội dung của bộ đệm của trình duyệt Web và lưu trữ một cookie độc hại trên hệ thống của khách hàng. Cookie (là một lưu lượng nhỏ dữ liệu được trình duyệt Web lưu trữ trên hệ thống cục bộ, theo hướng của máy chủ Web) có thể cho phép nhà thiết kế thu thập thông tin về cách truy cập các trang web được bảo vệ bằng mật khẩu. Một cuộc tấn công khác cùng tên liên quan đến việc đánh chặn các yếu tố mật mã để xác định các khóa và thuật toán mã hóa.

2.1. Trả lời các câu hỏi

1. Lừa đảo là gì? Biến thể của nó là gì?
2. Được phẩm cũng có thể khai thác Hệ thống tên miền như thế nào?

3. Đôi khi những kẻ tấn công làm gì để gây ảnh hưởng đến mục tiêu cho kỹ thuật xã hội?

4. Trong cuộc tấn công nào kẻ tấn công giám sát các gói từ mạng, sửa đổi chúng và đưa chúng trở lại mạng?

5. Tại sao được phẩm thư ờng sử dụng Trojan, sâu hoặc các công nghệ vi rút khác để tấn công thanh địa chỉ của trình duyệt Internet?

6. Hacker dùng gì để giả mạo IP?

7. Trong cuộc tấn công nào thì cookie có thể cho phép người thiết kế thu thập thông tin về cách truy cập các trang web được bảo vệ bằng mật khẩu?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa lỗi sai (F).

1. Lừa đảo là một kỹ thuật lấy thông tin cá nhân một cách gian lận.

- A. Đúng B. Sai C. NI

2. Trước một vài cuộc tấn công là giai đoạn chuẩn bị trong đó nhiều hệ thống, có lẽ hàng ngàn, bị xâm phạm.

- A. Đúng B. Sai C. NI

3. Sniffer gây thêm rủi ro cho mạng vì nhiều hệ thống và người dùng gửi thông tin trên các mạng cục bộ ở dạng văn bản rõ ràng.

- A. Đúng B. Sai C. NI

4. Tấn công được phẩm và thời gian thuộc về các cuộc tấn công kỹ thuật xã hội.

- A. Đúng B. Sai C. NI

5. Một trong những kỹ thuật mà kẻ tấn công giả mạo sử dụng để lừa trái phép truy cập vào máy tính là giả mạo một địa chỉ IP nguồn.

- A. Đúng B. Sai C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và các câu lệnh

1. Gửi e-mail dung lượng lớn với thông tin tiêu đề giả mạo, có thể tận dụng các hệ thống e-mail được cấu hình kém trên Internet và lừa họ gửi nhiều e-mail đến một địa chỉ do kẻ tấn công chọn.

- A. kẻ tấn công

người dùng C.

- B. ban tổ chức

D. lập trình viên

2.....khám phá nội dung của bộ nhớ cache của trình duyệt Web và

một cookie độc hại trên hệ thống của khách hàng.

C. Pha chẽ/sử dụng

C. Một cuộc tấn công thời gian/lưu trữ

D. Thư rác/chứa

D. Không có câu nào đúng

3.....có thể được sử dụng cho cả chức năng quản lý mạng hợp pháp và

vì ăn cắp thông tin.

A. Phần mềm gián điệp

C. Cú ống bức

B. Đánh hơi

D. Từ điển

4. Nhiều tổ chức có gắng đối phó với cơ n lũ thư rác bằng cách sử dụng e-
công nghệ lọc thư .

A. đối phó với

C. theo kịp với

B. có được trên tốt

D. đưa vào với

5. Những cuộc tấn công nào có thể được thực hiện bằng cách khai thác các lỗi kỹ thuật khác nhau trong
Giao thức vận chuyển thư đơn giản.

A. Ngư ời trung gian

C. Đánh bom thư

B. Lừa đảo

D. Dư ợc phảm

6.....là một nỗ lực để có được thông tin cá nhân hoặc tài chính từ một
cá nhân, thư ờng bằng cách giả làm một thực thể hợp pháp.

Một cuốn từ điển

C. đánh hơi

B. Lừa đảo

D. Chơi khăm

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về
họ?

2. Chọn ba cuộc tấn công trong văn bản và trình bày chúng.

4. Lắng nghe

1. https://www.youtube.com/watch?v=MIzKq8_Q0ro
2. <https://www.youtube.com/watch?v=jIDmqDhs17k>
3. <https://www.youtube.com/watch?v=n8mbzU0X2nQ>
4. <https://www.youtube.com/watch?v=-Z3pp14oUiA>
5. <https://www.youtube.com/watch?v=M2kExUGSDEo>
6. <https://www.youtube.com/watch?v=yAnthlVHxbk>

VIẾT VÀ NÓI

1. Viết khoảng 400 từ về một trong những nội dung sau bằng văn bản của bạn từ ngữ.
 - Các mối đe dọa trong bảo mật thông tin.
 - Tấn công vào an toàn thông tin
2. Trình bày các cuộc tấn công trong an toàn thông tin.
3. Trình bày các nguy cơ trong bảo mật thông tin.

ĐỌC THÊM

Tấn công mạng

Trong máy tính và mạng máy tính, một cuộc tấn công là bất kỳ nỗ lực nào nhằm phá hủy, thay đổi, vô hiệu hóa, phá hủy, đánh cắp hoặc giành quyền truy cập trái phép hoặc sử dụng trái phép một tài sản. Tấn công mạng là bất kỳ loại thủ đoạn tấn công nào nhắm vào hệ thống thông tin máy tính, cơ sở hạ tầng, mạng máy tính hoặc thiết bị máy tính cá nhân. Kẻ tấn công là một người hoặc quá trình cố gắng truy cập dữ liệu, chức năng hoặc các khu vực hạn chế khác của hệ thống mà không được phép, có khả năng với mục đích xấu. Tùy thuộc vào ngữ cảnh, các cuộc tấn công mạng có thể là một phần của phần mềm mạng hoặc khủng bố mạng. Một cuộc tấn công mạng có thể được thực hiện bởi các quốc gia có chủ quyền, cá nhân, nhóm, xã hội hoặc tổ chức và nó có thể bắt nguồn từ một nguồn ẩn danh.

Một cuộc tấn công mạng có thể đánh cắp, thay đổi hoặc phá hủy một mục tiêu cụ thể bằng cách xâm nhập vào một hệ thống dễ bị tấn công. Các cuộc tấn công mạng có thể bao gồm từ cài đặt phần mềm gián điệp trên máy tính cá nhân đến cố gắng phá hủy cơ sở hạ tầng của toàn bộ quốc gia. Các chuyên gia pháp lý đang tìm cách hạn chế việc sử dụng thuật ngữ này đối với các sự cố gây thiệt hại vật chất, phân biệt thuật ngữ này với các vi phạm dữ liệu thường xuyên hơn và các hoạt động hack rộng hơn. Tấn công mạng ngày càng tinh vi và nguy hiểm

Các loại tấn công mạng

Một cuộc tấn công có thể chủ động hoặc thụ động.

- Một "cuộc tấn công tích cực" cố gắng thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến hoạt động.

Tấn công từ chối dịch vụ

Giả mạo

Tấn công đe dọa hỗn hợp

Mạng (Man-in-the-middle, Man-in-the-browser, ARP
ngộ độc, Ping lũ, Ping chết chóc, và Xì trum tấn công)

Máy chủ (Tràn bộ đệm, Tràn heap, Tràn ngăn xếp, Tấn công chuỗi
định dạng)

- Một "cuộc tấn công thụ động" cố gắng tìm hiểu hoặc sử dụng thông tin từ hệ thống như ng không ảnh hưởng đến tài nguyên hệ thống.

Giám sát máy tính và mạng

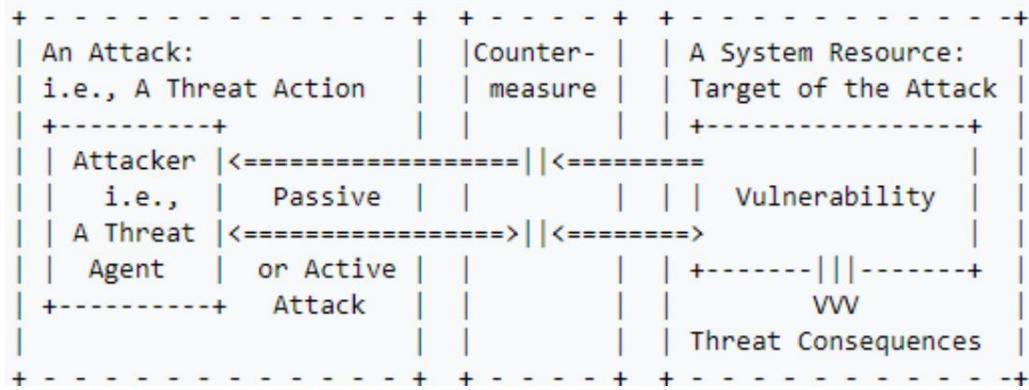
Mạng (Nghe lén, Khai thác sợi quang, Quét cổng và Quét khi không hoạt động)

Máy chủ (Ghi nhật ký gõ phím, Quét dữ liệu, Cửa hậu

Một cuộc tấn công có thể được thực hiện bởi người trong cuộc hoặc từ bên ngoài tổ chức;

- Một "cuộc tấn công bên trong" là một cuộc tấn công được khởi xướng bởi một thực thể bên trong bảo mật vành đai ("người trong cuộc"), tức là, một thực thể được phép truy cập tài nguyên hệ thống như sử dụng chúng theo cách không được những người đã cấp phép chấp thuận.
- Một "cuộc tấn công bên ngoài" được bắt đầu từ bên ngoài vành đai, bởi một người dùng trái phép hoặc bất hợp pháp của hệ thống ("người ngoài"). Trên Internet, những kẻ tấn công bên ngoài tiềm ẩn bao gồm từ những kẻ chơi khăm nghiệp dư đến tội phạm có tổ chức, những kẻ khủng bố quốc tế và các chính phủ thù địch.

Thuật ngữ "tấn công" liên quan đến một số thuật ngữ bảo mật cơ bản khác như trong sơ đồ sau:



Một tài nguyên (cả vật lý hoặc logic), được gọi là tài sản, có thể có một hoặc nhiều lỗ hổng mà tác nhân đe dọa có thể khai thác trong hành động đe dọa. Do đó, tính bảo mật, tính toàn vẹn hoặc tính sẵn có của tài nguyên có thể bị tổn hại.

Có khả năng, thiệt hại có thể mở rộng đến các nguồn lực ngoài ban đầu được xác định là dễ bị tổn thương, bao gồm các nguồn lực bổ sung của tổ chức và các nguồn lực của các bên liên quan khác (khách hàng, nhà cung cấp).

BÀI 3: TƯ ỜNG LỬA

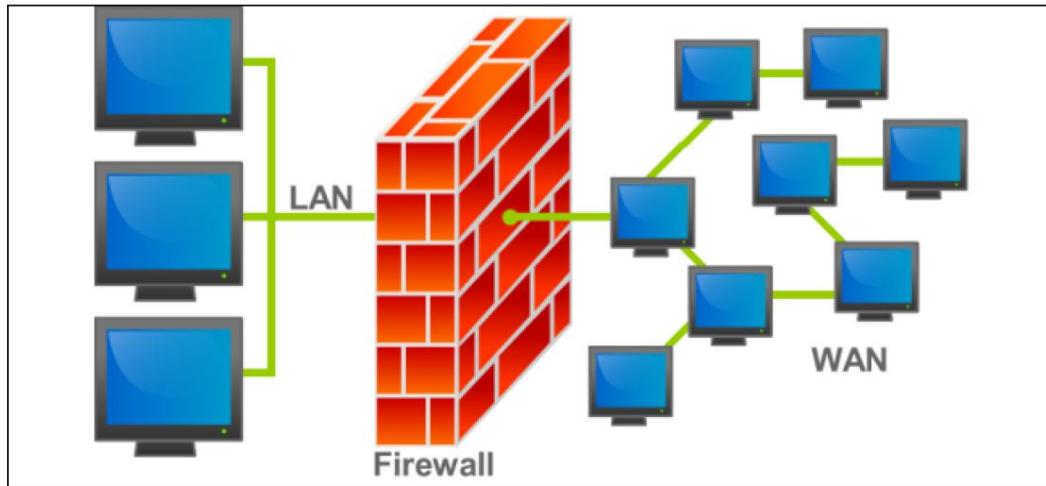
ĐỌC VÀ NÓI 1

1. Thảo luận các câu hỏi

1. Tư ờng lửa trong tin học là gì?
2. Có phải thuật ngữ "tư ờng lửa" chỉ được sử dụng trong tin học?
3. Ưu điểm của tư ờng lửa là gì?
4. Bạn biết bao nhiêu loại tư ờng lửa? Họ là ai?
5. Tư ờng lửa luôn có ưu điểm? Nếu không, nhược điểm của nó là gì?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Tư ờng lửa và lịch sử của nó



Hình 3-1. tư ờng lửa

Trong xây dựng thư ờng mại và dân cư, tư ờng lửa là những bức tư ờng bê tông hoặc gạch xây chạy từ tầng hầm qua mái nhà, để ngăn lửa lan từ phần này sang phần khác của tòa nhà. Trong máy bay và ô tô, tư ờng lửa là một hàng rào kim loại cách nhiệt giúp giữ cho các bộ phận chuyển động nóng và nguy hiểm của động cơ tách biệt với phần bên trong dễ cháy nổ i hành khách ngồi. Tư ờng lửa trong chương trình bảo mật thông tin tư ờng tự như tư ờng lửa của tòa nhà ở chỗ nó ngăn các loại thông tin cụ thể di chuyển giữa thế giới bên ngoài, được gọi là mạng không đáng tin cậy (ví dụ: Internet) và thế giới bên trong, được gọi là mạng đáng tin cậy . mạng. Tư ờng lửa có thể là một hệ thống máy tính riêng biệt, một

dịch vụ phần mềm chạy trên bộ định tuyến hoặc máy chủ hiện có hoặc một mạng riêng có chứa một số thiết bị hỗ trợ. Trong điện toán, tư ờng lửa là một hệ thống an ninh mạng giám sát và kiểm soát lưu lượng mạng vào và ra dựa trên các quy tắc bảo mật định trước. Tư ờng lửa thường thiết lập một rào cản giữa mạng nội bộ đáng tin cậy và mạng bên ngoài không đáng tin cậy, chẳng hạn như Internet. Tư ờng lửa có thể được phân loại theo chế độ xử lý, thời kỳ phát triển hoặc cấu trúc.

Thuật ngữ tư ờng lửa ban đầu được gọi là một bức tư ờng nhằm hạn chế đám cháy trong một dãy các tòa nhà liền kề. Các cách sử dụng sau này đề cập đến các cấu trúc tự nhiên, chẳng hạn như tấm kim loại ngăn cách khoang động cơ của phuơng tiện hoặc máy bay với khoang hành khách. Thuật ngữ này được áp dụng vào cuối những năm 1980 cho công nghệ mạng xuất hiện khi Internet còn khá mới về khả năng sử dụng và kết nối toàn cầu của nó. Tiền thân của tư ờng lửa để bảo mật mạng là các bộ định tuyến được sử dụng vào cuối những năm 1980, vì chúng tách biệt các mạng với nhau, do đó ngăn chặn sự lây lan của các sự cố từ mạng này sang mạng khác.

Trước khi nó được sử dụng trong điện toán thực tế, thuật ngữ này đã xuất hiện trong bộ phim hack máy tính WarGames năm 1983 và có thể truyền cảm hứng cho việc sử dụng nó sau này.

Thế hệ đầu tiên: bộ lọc gói

Loại tư ờng lửa mạng được báo cáo đầu tiên được gọi là bộ lọc gói. Bộ lọc gói hoạt động bằng cách kiểm tra các gói được truyền giữa các máy tính. Khi một gói không khớp với bộ quy tắc lọc của bộ lọc gói, bộ lọc gói sẽ loại bỏ (âm thầm loại bỏ) gói hoặc từ chối gói (loại bỏ nó và tạo thông báo Giao thức thông báo điều khiển Internet cho người gửi) nếu không nó được phép đi qua.

Các gói có thể được lọc theo địa chỉ mạng nguồn và đích, giao thức, số cổng nguồn và đích. Phần lớn giao tiếp Internet trong thế kỷ 20 và đầu thế kỷ 21 đã sử dụng Giao thức điều khiển truyền tải (TCP) hoặc Giao thức gói dữ liệu người dùng (UDP) kết hợp với các cổng nối tiếng, cho phép tư ờng lửa của thời đại đó phân biệt và do đó kiểm soát các loại cụ thể của (chẳng hạn như duyệt web, in từ xa, truyền email, truyền tệp), trừ khi các máy ở mỗi bên của bộ lọc gói sử dụng cùng một cổng không chuẩn.

Bài báo đầu tiên được xuất bản về công nghệ tư ờng lửa là vào năm 1987, khi các kỹ sư từ Tập đoàn Thiết bị Kỹ thuật số (DEC) phát triển các hệ thống lọc được gọi là

tư ờng lửa lọc gói. Tại AT&T Bell Labs, Bill Cheswick và Steve Bellovin tiếp tục nghiên cứu về lọc gói và phát triển một mô hình hoạt động cho công ty của riêng họ dựa trên khung trục thế hệ đầu tiên ban đầu của họ.

Thế hệ thứ hai: bộ lọc trạng thái

Từ năm 1989-1990, ba đồng nghiệp từ Phòng thí nghiệm AT&T Bell, Dave Presotto, Janardan Sharma và Kshitij Nigam, đã phát triển thế hệ tư ờng lửa thứ hai, gọi chúng là cổng cấp mạch.

Tư ờng lửa thế hệ thứ hai thực hiện công việc của thế hệ tiền nhiệm đầu tiên như ng cũng duy trì kiến thức về các cuộc hội thoại cụ thể giữa các điểm cuối bằng cách ghi nhớ số cổng mà hai địa chỉ IP đang sử dụng ở lớp 4 (lớp vận chuyển) của mô hình OSI cho cuộc hội thoại của chúng, cho phép kiểm tra trao đổi tổng thể giữa các nút.

Loại tư ờng lửa này có khả năng dễ bị tấn công từ chối dịch vụ bắn phá tư ờng lửa bằng các kết nối giả nhằm cố gắng áp đảo tư ờng lửa bằng cách lắp đầy bộ nhớ trạng thái kết nối của nó.

Thế hệ thứ ba: lớp ứng dụng

Marcus Ranum, Wei Xu và Peter Churchyard đã phát hành một tư ờng lửa ứng dụng có tên là Bộ công cụ tư ờng lửa (FWTK) vào tháng 10 năm 1993. Điều này trở thành nền tảng cho tư ờng lửa Gauntlet tại Trusted Information Systems.

Lợi ích chính của lọc lớp ứng dụng là nó có thể hiểu một số ứng dụng và giao thức nhất định (chẳng hạn như Giao thức truyền tệp (FTP), Hệ thống tên miền (DNS) hoặc Giao thức truyền siêu văn bản (HTTP)). Điều này rất hữu ích vì nó có thể phát hiện xem một ứng dụng hoặc dịch vụ không mong muốn có đang cố vươn ra tư ờng lửa bằng giao thức không được phép trên một cổng được phép hay không hoặc phát hiện xem một giao thức có đang bị lạm dụng theo bất kỳ cách nào không

Kể từ năm 2012, cái gọi là tư ờng lửa thế hệ tiếp theo (NGFW) là một cuộc kiểm tra rộng hơn hoặc sâu hơn ở lớp ứng dụng. Ví dụ: chức năng kiểm tra gói sâu hiện có của tư ờng lửa hiện đại có thể được mở rộng để bao gồm:

- Hệ thống ngăn chặn xâm nhập (IPS) •

Tích hợp quản lý danh tính người dùng (bằng cách liên kết ID người dùng với IP hoặc MAC địa chỉ cho "danh tiếng")

- Tư ờng lửa ứng dụng web (WAF). Các cuộc tấn công WAF có thể được thực hiện trong công cụ "WAF Fingerprinting sử dụng các kênh bên thời gian"

2.1. Trả lời các câu hỏi

1. Tư ờng lửa trong tin học là gì?
2. Thuật ngữ tư ờng lửa bắt nguồn từ đâu?
3. Tư ờng lửa trong chương trình bảo mật thông tin giống hay khác từ tư ờng lửa của tòa nhà? Điểm tư ờng đồng hoặc khác biệt của chúng là gì?
4. Các chức năng của bộ lọc trạng thái là gì?
5. Tư ờng lửa có thể được phân loại như thế nào?
6. Tiềm thân của tư ờng lửa để bảo mật mạng là gì?
7. Lợi ích quan trọng nhất của lọc lớp ứng dụng là gì?
8. Lợi ích của tư ờng lửa trên máy bay và ô tô là gì?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI).

Sửa cái sai

1. Bộ lọc gói hoạt động bằng cách kiểm tra các gói được truyền giữa máy vi tính.
A. Đúng B. Sai C. NI
2. Bộ công cụ tư ờng lửa được phát minh bởi Marcus Ranum, Wei Xu và Peter Niles.
A. Đúng B. Sai C. NI
3. Các cổng cấp mạch là thẻ hệ thống tư ờng lửa đầu tiên
A. Đúng B. Sai C. NI
4. Tư ờng lửa được xây dựng giữa hoặc xuyên qua các tòa nhà, công trình hoặc hệ thống điện trạm biến áp, hoặc trong một chiếc máy bay hoặc phư ơng tiện.
A. Đúng B. Sai C. NI
5. Tư ờng lửa có thể được sử dụng để chia nhỏ tòa nhà thành các khu vực cháy riêng biệt và được xây dựng phù hợp với quy chuẩn xây dựng hiện hành tại địa phư ơng.
A. Đúng B. Sai C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1..... thư ờng đư ợc thiết lập giữa mạng nội bộ đáng tin cậy và
mạng bên ngoài không đáng tin cậy trong

A. bảng điều khiển/máy tính B. một bức tư ờng/xây dựng

C. một lá chắn/máy tính D. A&C đều đúng

2. Tư ờng lửa đư ợc áp dụng khi nào và nó đư ợc áp dụng để làm gì?

- A. Năm 1987/ công nghệ tư ờng lửa
- B. vào cuối những năm 1980/ công nghệ mạng
- C. Đầu thế kỷ 21/địa chỉ IP
- D. Tháng 10 năm 1993/ Hệ thống thông tin

3. Lợi ích của tư ờng lửa..... là ngăn đám cháy lan rộng

từ phần này sang phần khác của tòa nhà.

- A. Trong xây dựng thư ờng mại và dân cư
- B. trong một chương trình bảo mật thông tin
- C. Trong tin học
- C. A&C đều đúng

4. WarGames là gì và nó ra đời khi nào?

- A. Tư ờng lửa thế hệ thứ ba/năm 2012
- B. Bộ lọc gói/vào đầu thế kỷ 21
- C. Một bộ phim hack máy tính/năm 1983
- D. bộ lọc trạng thái/ từ 1989-1990

5. Điều gì đã trở thành cơ sở cho tư ờng lửa Gauntlet tại Trusted Information Systems?

- A. Giao thức truyền tải siêu văn bản
- B. Bộ công cụ tư ờng lửa
- C. Giao thức gói dữ liệu ngẫu nhiên
- D. tầng vận chuyển

3. Nói

- 1. Bạn nhận đư ợc thông tin chính nào từ văn bản?
- 2. Trình bày tư ờng lửa và lịch sử của nó.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi

1. Từ "thiết bị" nghĩa là gì?
2. SOHO là viết tắt của từ gì? Nó có nghĩa là gì?
3. Tư ờng lửa được phân loại như thế nào?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Tư ờng lửa được phân loại theo cấu trúc

Tư ờng lửa cũng có thể được phân loại theo cấu trúc được sử dụng để triển khai chúng. Hầu hết các tư ờng lửa cấp thư ơng mại là các thiết bị chuyên dụng. Cụ thể, chúng là các đơn vị độc lập chạy trên các nền tảng điện toán được tùy chỉnh hoàn toàn, cung cấp cả kết nối mạng vật lý và lập trình phần mềm cần thiết để thực hiện chức năng của chúng, bao gồm cả chức năng lọc gói tĩnh, proxy ứng dụng, v.v.) có thể là gì. Một số thiết bị tư ờng lửa sử dụng các hệ thống phần cứng độc quyền, đôi khi được tùy chỉnh cao, được phát triển riêng dưới dạng thiết bị tư ờng lửa.

Các hệ thống tư ờng lửa thư ơng mại khác thực sự là các hệ thống máy tính có mục đích chung chạy sẵn phần mềm ứng dụng tùy chỉnh trên các hệ điều hành tiêu chuẩn như Windows hoặc Linux/Unix hoặc trên các biển thẻ chuyên dụng của các hệ điều hành này. Hầu hết các tư ờng lửa cấp văn phòng hoặc khu dân cư nhỏ đều là các thiết bị chuyên dụng được đơn giản hóa chạy trên các thiết bị máy tính hoặc phần mềm ứng dụng được cài đặt trực tiếp trên máy tính của người dùng.

Thiết bị tư ờng lửa cấp thư ơng mại

Các thiết bị tư ờng lửa là sự kết hợp độc lập, khép kín của phần cứng và phần mềm máy tính. Các thiết bị này thường có nhiều tính năng của một máy tính đa năng với việc bổ sung các hướng dẫn dựa trên phần mềm giúp tăng độ tin cậy và hiệu suất của chúng, đồng thời giảm thiểu khả năng chúng bị xâm phạm. Hệ điều hành phần mềm tùy chỉnh điều khiển thiết bị có thể được nâng cấp định kỳ như ng chỉ có thể được sửa đổi thông qua kết nối vật lý trực tiếp hoặc sau khi chạy các giao thức xác thực và ủy quyền mở rộng.

Các bộ quy tắc tư ờng lửa được lưu trữ trong bộ nhớ cố định và do đó nhân viên kỹ thuật có thể thay đổi chúng khi cần thiết như ng luôn sẵn sàng mỗi khi thiết bị hoạt động.
khởi động lại.

Các thiết bị này có thể được sản xuất từ các hệ thống máy tính đa năng đã được rút gọn và/hoặc được thiết kế để chạy một phiên bản tùy chỉnh của hệ điều hành đa năng. Các hệ điều hành biến thể này được điều chỉnh để đáp ứng loại hoạt động tương ứng lửa được tích hợp trong phần mềm ứng dụng cung cấp chức năng tương ứng lửa.

Hệ thống tương ứng lửa cấp thươn mại

Hệ thống tương ứng lửa cấp thươn mại bao gồm phần mềm ứng dụng được cấu hình cho ứng dụng tương ứng lửa và chạy trên máy tính đa năng.

Các tổ chức có thể cài đặt phần mềm tương ứng lửa trên hệ thống máy tính có mục đích chung hiện có hoặc họ có thể mua phần cứng đã được định cấu hình theo các thông số kỹ thuật mang lại hiệu suất tương ứng lửa tối ưu. Các hệ thống này khai thác thực tế rằng tương ứng lửa về cơ bản là các gói phần mềm ứng dụng sử dụng các kết nối mạng có mục đích chung để di chuyển dữ liệu từ mạng này sang mạng khác.

Thiết bị tương ứng lửa cho văn phòng nhỏ/văn phòng tại nhà (SOHO)

Khi ngày càng có nhiều doanh nghiệp nhỏ và khu dân cư có kết nối Internet nhanh với các đường dây thuê bao kỹ thuật số (DSL) hoặc kết nối modem cáp, chúng ngày càng trở nên dễ bị tấn công hơn. Điều mà nhiều doanh nghiệp nhỏ và người dùng làm việc tại nhà không nhận ra rằng, không giống như các kết nối quay số, các dịch vụ tốc độ cao này luôn được bật; do đó, các máy tính được kết nối với chúng có nhiều khả năng hiển thị trong quá trình quét do kẻ tấn công thực hiện hơn là những máy tính chỉ được kết nối trong suốt thời gian của phiên quay số. Một trong những phương pháp hiệu quả nhất để cải thiện bảo mật máy tính trong cài đặt SOHO là bằng SOHO hoặc tương ứng lửa cấp khu dân cư. Các thiết bị này, còn được gọi là cổng băng thông rộng hoặc bộ định tuyến modem DSL/cáp, kết nối mạng cục bộ của người dùng hoặc hệ thống máy tính cụ thể với thiết bị Kết nối Internet-trong trường hợp này là modem cáp hoặc bộ định tuyến DSL do nhà cung cấp dịch vụ Internet (ISP) cung cấp. Tương ứng lửa SOHO hoạt động đầu tiên như một tương ứng lửa có trạng thái để cho phép truy cập từ trong ra ngoài và có thể được

được định cấu hình để cho phép chuyển tiếp cổng TCP/IP hạn chế và/hoặc khả năng mạng con được sàng lọc. (Xem Hình 3-2)



Hình 3-2. Thiết bị tư ờng lứa SOHO

Phần mềm tư ờng lứa cấp khu dân cư

Một phư ơng pháp khác để bảo vệ ngư ời dùng dân cư là cài đặt tư ờng lứa phần mềm trực tiếp trên hệ thống của ngư ời dùng. Nhiều ngư ời đã triển khai các tư ờng lứa dựa trên phần mềm cấp độ dân dụng này (một số trong số đó cũng cung cấp khả năng chống vi-rút hoặc phát hiện xâm nhập), như ng thật không may, chúng có thể không được bảo vệ đầy đủ như họ nghĩ.

Phần mềm so với phần cứng: Cuộc tranh luận về tư ờng lứa SOHO

Vậy loại tư ờng lứa nào mà ngư ời dùng dân cư nên triển khai? Nhiều ngư ời dùng thè với tư ờng lứa phần mềm của họ. Kinh nghiệm cá nhân sẽ tạo ra nhiều quan điểm khác nhau.

Hãy tự hỏi mình câu hỏi này: Bạn muốn phòng thủ ở đâu trước kẻ tấn công? Tùy chọn phần mềm cho phép tin tặc bên trong máy tính của bạn chống lại một phần mềm (phần mềm miễn phí, trong nhiều trường hợp) có thể không được cài đặt, định cấu hình, vá lỗi, nâng cấp hoặc thiết kế đúng cách. Nếu phần mềm có một lỗ hổng đã biết, kẻ tấn công có thể bỏ qua nó và sau đó có quyền truy cập không hạn chế vào hệ thống của bạn. Với tư ờng lứa phần cứng, ngay cả khi kẻ tấn công làm hỏng hệ thống tư ờng lứa, máy tính và thông tin của bạn vẫn an toàn sau kết nối hiện đã bị vô hiệu hóa. Việc sử dụng không có địa chỉ có thể định tuyến của tư ờng lứa phần cứng giúp mở rộng khả năng bảo vệ, khiến kẻ tấn công gần như không thể lấy được thông tin của bạn. Một cựu sinh viên của một trong những tác giả

đã trả lời cuộc tranh luận này bằng cách cài đặt tư ờng lửa phần cứng, sau đó truy cập phòng trò chuyện của hacker. Anh ta thách nhóm xâm nhập vào hệ thống của anh ta. Vài ngày sau, anh ta nhận được một e-mail từ một hacker tuyên bố đã truy cập vào hệ thống của anh ta. Tin tức đã đính kèm một hình ảnh màn hình hiển thị dấu nhắc C:\ mà anh ta khẳng định là từ hệ thống của sinh viên. Sau khi thực hiện một số nghiên cứu, sinh viên phát hiện ra rằng tư ờng lửa có một hình ảnh được lưu trữ trong phần sụn được thiết kế để đánh lạc hướng những kẻ tấn công. Đó là hình ảnh của một cửa sổ lệnh với dấu nhắc DOS. Giải pháp phần cứng (NAT) đã vượt qua thử thách.

2.1. Trả lời các câu hỏi

1. Hệ thống tư ờng lửa cấp thư ơng mại bao gồm những gì?
2. Tại sao bộ quy tắc tư ờng lửa có thể bị thay đổi bởi nhân viên kỹ thuật khi cần thiết?
3. Hầu hết các tư ờng lửa cấp văn phòng hoặc khu dân cư nhỏ là gì?
4. Một trong những phương pháp hiệu quả nhất để cải thiện bảo mật máy tính trong cài đặt SOHO là gì?
5. Phương pháp nào được sử dụng để bảo vệ người dùng dân cư?
6. Windows hay Linux/Unix là gì?
7. Tại sao ngày càng có nhiều doanh nghiệp nhỏ và khu dân cư dễ bị tấn công hơn?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Cổng băng thông rộng hoặc bộ định tuyến modem DSL/cáp là Cấp thư ơng mại Thiết bị tư ờng lửa.
 A. Đúng B. Sai C. NI
2. Nếu người dùng dân cư cài đặt tư ờng lửa phần mềm trực tiếp trên hệ thống của họ, máy tính của họ hoàn toàn được bảo vệ.
 A. Đúng B. Sai C. NI
3. Tư ờng lửa cũng có thể được phân loại theo cấu trúc được sử dụng để triển khai chúng. Hầu hết các tư ờng lửa cấp thư ơng mại là các thiết bị chuyên dụng.
 A. Đúng B. Sai C. NI
4. Tất cả các thiết bị tư ờng lửa có thể được cấu hình trong một số kết nối mạng

kiến trúc.

A. Đúng

B. Sai

C. NI

5. Việc sử dụng không có địa chỉ có thể định tuyến của tư ờng lửa phần cứng sẽ mở rộng hơn nữa bảo vệ, khiến kẻ tấn công hakk như không thể tiếp cận đư ợc thông tin.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu sau

1. là các tổ hợp máy tính độc lập, khép kín phần cứng và phần mềm.

A. Thiết bị tư ờng lửa

B. Kiến trúc tư ờng lửa

C. Hệ thống tư ờng lửa

D. Phần mềm tư ờng lửa

2. Tổ chức có thể cài đặt vào mục đích chung hiện có hệ thống máy tính.

A. phần cứng tư ờng lửa

B. kiến trúc tư ờng lửa

C. phần mềm tư ờng lửa

D. thiết bị tư ờng lửa

3. Từ "họ" trong đoạn 4 đề cập đến điều nào sau đây? _____

A. đường dây thuê bao kỹ thuật số

B. Kết nối Internet

C. kết nối modem cáp

D. doanh nghiệp và nhà ở

4. Điều nào sau đây giúp máy tính của bạn vẫn an toàn dù làm cách nào những kẻ tấn công khó quản lý?

A. Một chương trình phần mềm diệt virus

B. Mật khẩu mạnh

C. Tư ờng lửa phần cứng

D. SOHO

5. Tư ờng lửa SOHO hoạt động đầu tiên như một tư ờng lửa có trạng thái để cho phép truy cập.

A. từ trong ra ngoài

B. từ ngoài vào trong

C. A & B đều đúng

D. Không có câu nào đúng

3. Nói

1. Qua văn bản em rút ra đư ợc những nội dung chính nào?

2. Chọn một trong các nội dung trong văn bản và trình bày.

ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi

1. Từ “kiến trúc” nghĩa là gì? nghĩa là? Liệt kê một số từ đi với nó?
2. Bạn biết gì về kiến trúc tư ờng lửa trong tin học?
2. NIC là viết tắt của từ gì? Nó có nghĩa là gì?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Kiến trúc tư ờng lửa

Tất cả các thiết bị tư ờng lửa có thể được cấu hình trong một số kiến trúc kết nối mạng. Những cách tiếp cận này đôi khi loại trừ lẫn nhau và đôi khi có thể được kết hợp. Cấu hình hoạt động tốt nhất cho một tổ chức cụ thể phụ thuộc vào ba yếu tố: mục tiêu của mạng, khả năng phát triển và triển khai kiến trúc của tổ chức và ngân sách sẵn có cho chức năng.

Mặc dù có hàng trăm biến thể tồn tại theo nghĩa đen, nhưng có bốn triển khai kiến trúc phổ biến: Bộ định tuyến lọc gói, tư ờng lửa máy chủ được sàng lọc, tư ờng lửa hai nhà và tư ờng lửa mạng con được sàng lọc.

Bộ định tuyến lọc gói

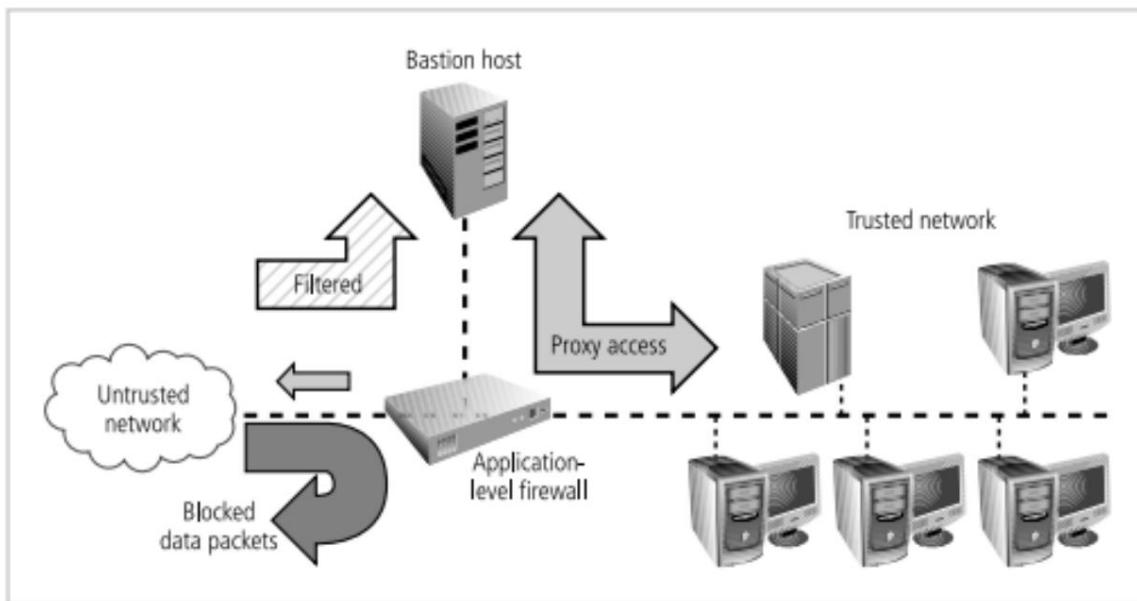
Hầu hết các tổ chức có kết nối Internet đều có một số dạng bộ định tuyến ở ranh giới giữa mạng nội bộ của tổ chức và nhà cung cấp dịch vụ bên ngoài. Nhiều bộ định tuyến trong số này có thể được cấu hình để từ chối các gói mà tổ chức không muốn cho phép vào mạng. Đây là một cách đơn giản như ng hiệu quả để giảm rủi ro của tổ chức khỏi sự tấn công từ bên ngoài. Những hạn chế đối với loại hệ thống này bao gồm thiếu kiểm toán và xác thực mạnh.

Screened Host Firewalls ([xem Hình 3-3](#))

Tư ờng lửa máy chủ được sàng lọc kết hợp bộ định tuyến lọc gói với tư ờng lửa chuyên dụng, riêng biệt, chẳng hạn như máy chủ proxy ứng dụng. Cách tiếp cận này cho phép bộ định tuyến sàng lọc trước các gói để giảm thiểu lưu lượng mạng và tải trên proxy nội bộ. Proxy ứng dụng kiểm tra một giao thức lớp ứng dụng, chẳng hạn như HTTP và thực hiện các dịch vụ proxy. Máy chủ riêng biệt này thường được gọi là máy chủ pháo đài; nó có thể là một mục tiêu phong phú cho các cuộc tấn công từ bên ngoài và cần được bảo mật rất kỹ lưỡng. Mặc dù máy chủ pháo đài/proxy ứng dụng thực sự

chỉ chứa các bản sao đư ợc lưu u trong bộ nhớ cache của các tài liệu Web nội bộ, nó vẫn có thể là một mục tiêu đầy hứa hẹn, bởi vì sự xâm nhập của máy chủ pháo đài có thể tiết lộ cấu hình của các mạng nội bộ và có thể cung cấp cho kẻ tấn công thông tin nội bộ.

Vì máy chủ pháo đài đóng vai trò là người bảo vệ duy nhất trên mạng chu vi, nó thường đư ợc gọi là máy chủ hiến tế. Để thuận lợi, cấu hình này yêu cầu cuộc tấn công bên ngoài phải thỏa hiệp hai hệ thống riêng biệt trước khi cuộc tấn công có thể truy cập dữ liệu nội bộ. Bằng cách này, máy chủ pháo đài bảo vệ dữ liệu đầy đủ hơn so với chỉ một mình bộ định tuyến.



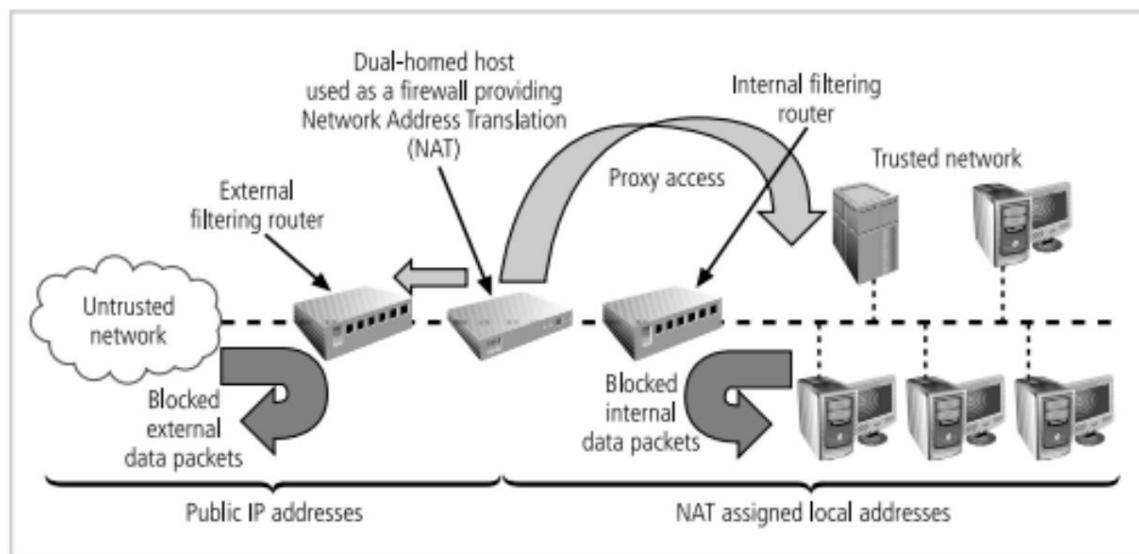
Hình 3-3. Tư ờng lúa máy chủ đư ợc sàng lọc

Tư ờng lúa Dual-Homed Host ([xem Hình 3-4](#))

Bước tiếp theo trong sự phức tạp của kiến trúc tư ờng lúa là máy chủ kép. Khi sử dụng phương pháp kiến trúc này, máy chủ pháo đài chứa hai NIC (thẻ giao diện mạng) chứ không phải một như trong cấu hình máy chủ pháo đài. Một NIC đư ợc kết nối với mạng bên ngoài và một NIC đư ợc kết nối với mạng nội bộ, cung cấp thêm một lớp bảo vệ. Với hai NIC, tất cả lưu lượng phải đi qua tư ờng lúa để di chuyển giữa các mạng bên trong và bên ngoài. Việc triển khai kiến trúc này thư ờng sử dụng NAT.

NAT là một phương pháp ánh xạ các địa chỉ IP thực, hợp lệ, bên ngoài tới các dải đặc biệt không có địa chỉ IP bên trong có thể định tuyến, do đó tạo ra một rào cản khác đối với sự xâm nhập từ những kẻ tấn công bên ngoài. Các địa chỉ nội bộ đư ợc sử dụng bởi NAT bao gồm ba phạm vi khác nhau. Lợi dụng điều này, NAT ngăn chặn các cuộc tấn công từ bên ngoài

tiếp cận các máy nội bộ có địa chỉ trong phạm vi được chỉ định. Nếu máy chủ NAT là một máy chủ pháo đài nhiều nhà, nó sẽ chuyển đổi giữa các địa chỉ IP thực, bên ngoài được các cơ quan đặt tên mạng công cộng gán cho tổ chức và các địa chỉ IP không thể định tuyến được gán nội bộ. NAT dịch bằng cách tự động gán địa chỉ cho các liên lạc nội bộ và theo dõi các cuộc hội thoại với các phiên để xác định thư đến nào là phản hồi cho lưu lư ợng gửi đi nào. Hình 6-13 cho thấy cấu hình điển hình của tư ờng lửa máy chủ hai nhà sử dụng quyền truy cập NAT và proxy để bảo vệ mạng nội bộ. Một lợi ích khác của máy chủ hai nhà là khả năng dịch giữa nhiều giao thức khác nhau ở các lớp liên kết dữ liệu tư ờng ứng của chúng, bao gồm Ethernet, vòng mã thông báo, Giao diện dữ liệu phân tán sợi quang (FDDI) và chế độ truyền không đồng bộ (ATM). Một khía cạnh khác, nếu máy chủ nhà kép này bị xâm phạm, nó có thể vô hiệu hóa kết nối với mạng bên ngoài và khi lưu lư ợng truy cập tăng lên, nó có thể trở nên quá tải. Tuy nhiên, so với các giải pháp phức tạp hơn, kiến trúc này cung cấp khả năng bảo vệ tổng thể mạnh mẽ với chi phí tối thiểu



Hình 3-4. Tư ờng lửa máy chủ kép

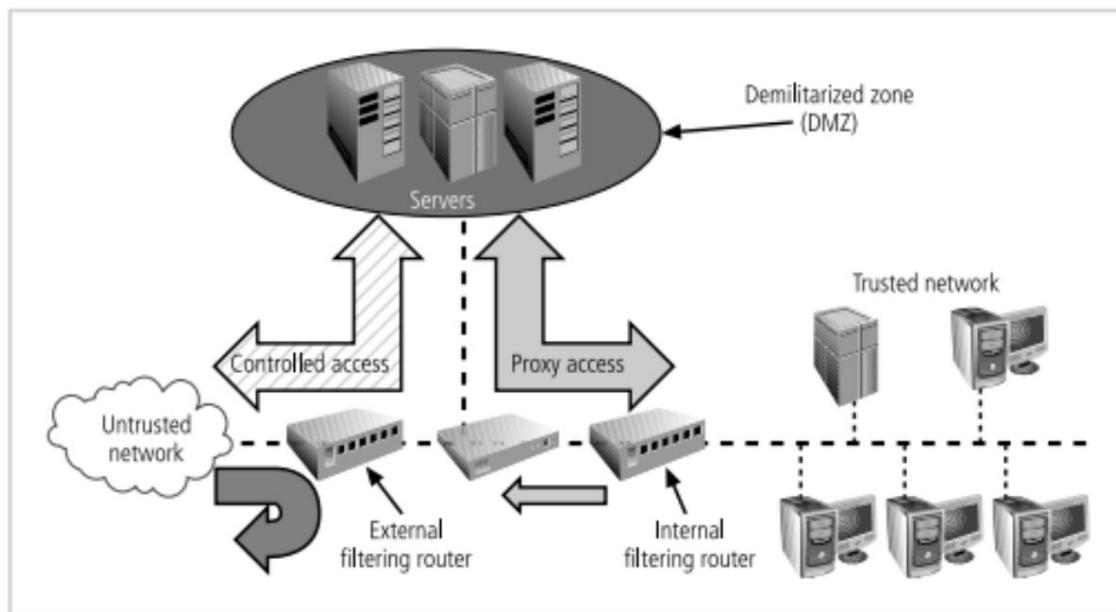
Tư ờng lửa mạng con đư ợc sàng lọc (với DMZ) ([xem Hình 3-5](#))

Kiến trúc chủ yếu đư ợc sử dụng ngày nay là tư ờng lửa mạng con đư ợc sàng lọc. Kiến trúc của tư ờng lửa mạng con đư ợc sàng lọc cung cấp DMZ. DMZ có thể là một cổng chuyên dụng trên thiết bị tư ờng lửa liên kết với một máy chủ pháo đài duy nhất hoặc nó có thể đư ợc kết nối với một mạng con đư ợc sàng lọc, như trong Hình 6-14. Cho đến gần đây, các máy chủ

cung cấp dịch vụ thông qua một mạng không đáng tin cậy thư ờng đư ợc đặt trong DMZ. Ví dụ về những điều này bao gồm máy chủ Web, máy chủ giao thức truyền tệp (FTP) và máy chủ cơ sở dữ liệu nhất định. Các chiến lược gần đây hơn sử dụng máy chủ proxy đã cung cấp nhiều giải pháp an toàn hơn.

Một sự sắp xếp phổ biến tìm thấy thư ờng lửa mạng con bao gồm hai hoặc nhiều máy chủ pháo đài bên trong phía sau bộ định tuyến lọc gói, với mỗi máy chủ bảo vệ mạng đáng tin cậy. Có nhiều biến thể của kiến trúc mạng con đư ợc sàng lọc. Mô hình chung đầu tiên bao gồm hai bộ định tuyến lọc, với một hoặc nhiều máy chủ pháo đài hai nhà ở giữa chúng. Trong mô hình chung thứ hai, các kết nối đư ợc định tuyến như sau:

- Các kết nối từ bên ngoài hoặc mạng không đáng tin cậy đư ợc định tuyến thông qua bộ định tuyến lọc bên ngoài.
- Các kết nối từ bên ngoài hoặc mạng không đáng tin cậy đư ợc định tuyến vào-và sau đó out of-một thư ờng lửa định tuyến đến phân đoạn mạng riêng biệt đư ợc gọi là DMZ.
- Các kết nối vào mạng nội bộ đáng tin cậy chỉ đư ợc phép từ DMZ máy chủ lưu trữ pháo đài.



Hình 3-5. Thư ờng lửa mạng con đư ợc sàng lọc (với DMZ)

Máy chủ SOCKS

Đáng đư ợc quan tâm đặc biệt ngắn gọn là triển khai thư ờng lửa SOCKS.

SOCKS là giao thức xử lý lưu trữ lư ợng TCP thông qua máy chủ proxy. Vớ

system là một máy chủ proxy cấp mẠch đỘc quyỀn đặt các tÁC nhÂN phÍA mÁy khÁch SOCKS đặc biỆt trÊn mŐi mÁy trÂm. CÁCH tiẾp cẬn chUNG là đặt các yÊu cÂU lỌc trÊn mÁy trÂm riĘng lĚ hƠn là trÊn mỘt đIỂM phÒng thỦ duy nhẤt (vÀ do đÓ là đIỂM thÂt bÃI). ĐIỀU nÀy giải phÓng bỘ đINH tuyỀn đÂu vÀO khÓi các trÁCh nhIỆm lỌc, nhÚ ng nÓ yÊu cÂU mŐi mÁy trÂm phẢi đUR ợc quÂn lÝ nhÚ mỘt thiẾt bÌ bAO vẸ và phÂt hiỆn tƯ Ờng lÚa. MỘt hỆ thÔng SOCKS có thỂ yÊu cÂU các tÀI ngUYÊN hÕ trØ và quÂn lÝ ngoÀi nhÚNG tÀI ngUYÊN cUA tƯ Ờng lÚa trUYỀN thÔng vÌ nÓ đOÌ hÓi phẢi cÂU hÌnh và quÂn lÝ hÀng trÃM mÁy khÁch riĘng lĚ, trÁi ngUER ợc vÓi mỘt thiẾt bÌ hoẶC bỘ thiẾt bÌ nhỎ.

2.1. Trả lời các câu hỏi

1. NhÚNG triỀn khAI kiÉn trÚc phÔ biĒn nÀo đUR ợc đÈ cÂp trONG vĂn bÂn?
2. TẠI sao hÀu hÊt cÁC tÖZ chÜrc cÓ kÉt nÓi Internet đEUV cÓ mÔt sÔ dÂng bØ dINH tuyỀn Ở ranh giÓi giÚa mÄng nÓi bØ cUA tÖZ chÜrc vÀ nhÀ cUNG cÂp dÎch vU bÊn ngoÀi?
3. CÁCH tiẾp cÂn nÀo cho phEP bØ dINH tuyỀn sÀng lỌc trU ỚC cÁC gÓi đÈ gIÂM thiỀu lUu lU ợng mÄng vÀ tÂi trÊn proxy nÓi bØ?
4. Giao thÚc xÙ lÝ lUu lU ợng TCP thÔng qua mÁy chÙ proxy lÀ gÌ?
5. CÓ nhIỀU biĒn thË cUA kiÉn trÚc mÄng con đUR ợc sÀng lỌc khÔng? MÔ hÌnh chUNG đÂU tIEN bAO gÖM nhÚNG gÌ?
6. Bastion host chÙA bAO nhIỀU NIC? HØ lÀ ai?
7. TAI sao NAT cÓ thË ngÄn chÄn cÁC cuOC tÄn cÔng tÙ bÊn ngoÀi vÀO bÊn trONG mÁy cÓ dIa chÌ trONG phÂm vi đUR ợc chÌ dINH?
8. TAI sao phAO dÀI thu Ờng đUR ợc gOI lÀ vÂt hiËn tÉ?

2.2. Quyết định xEM nhÚNG cÂU sau đÂY lÀ đÚng (T), sai (F) hay khÔng cÓ thÔng tin (NI)

1. CÓ ba ƯU dIËM cUA NAT đUR ợc đÈ cÂp trONG vĂn bÂn.

A. ĐÚng	B. Sai	C. NI
---------	--------	-------
2. MỘt phU Ơ ng phÂp ánh xÂy cÁC dIa chÌ IP thUc, hÓp lÊ, bÊn ngoÀi thÀnh cÁCs dAI dÄc biËt khÔng cÓ dIa chÌ IP nÓi bØ cÓ thË dINH tuyỀn lÀ NAT.

A. ĐÚng	B. Sai	C. NI
---------	--------	-------

3. Proxy ứng dụng kiểm tra một giao thức lớp ứng dụng, chẳng hạn như

HTTP và thực hiện các dịch vụ proxy.

A. Đúng

B. Sai

C. NI

4. Có một số dạng bộ định tuyến ở ranh giới giữa các bộ định tuyến của tổ chức

mạng nội bộ và nhà cung cấp dịch vụ bên ngoài luôn có lợi cho

tổ chức có kết nối Internet.

A. Đúng

B. Sai

C. NI

5. Kiến trúc tư ờng lửa chịu trách nhiệm về các tiêu chuẩn và khuôn khổ

liên kết với kiến trúc của các mạng con

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu sau

1. kết hợp bộ định tuyến lọc gói với một bộ định tuyến chuyên dụng, riêng biệt.

tư ờng lửa, chẳng hạn như máy chủ proxy ứng dụng.

B. Tư ờng lửa máy chủ đư ợc sàng lọc

B. Hệ thống tư ờng lửa

C. Tư ờng lửa máy chủ nhà kép

D. Tư ờng lửa mạng con màn hình

2. Tất cả các thiết bị tư ờng lửa có thể đư ợc cấu hình trong kết nối mạng

kiến trúc.

A. một loạt các

B. chỉ một vài

C. nhiều loại

D. A&C đều đúng

3. Kiến trúc chiếm ưu thế đư ợc sử dụng ngày nay là tư ờng lửa.

A. máy chủ màn hình

B. máy chủ nhà kép

C. mạng con đư ợc sàng lọc

D. C&B đều đúng

4. Cấu hình hoạt động tốt nhất cho một tổ chức cụ thể phụ thuộc vào

.....

A. khả năng của tổ chức để phát triển và triển khai kiến trúc

B. mục tiêu của mạng

C. ngân sách có sẵn cho chức năng

D. Tất cả đều đúng

5. Lợi ích của là khả năng chuyển đổi giữa nhiều giao thức khác nhau tại các lớp liên kết dữ liệu tư ơng ứng của chúng.

A. máy chủ hai nhà

B. máy chủ màn hình

C. Máy chủ SOCKS

D. tư ờng lửa mạng con màn hình

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?
2. Chọn một trong các nội dung trong văn bản và trình bày.

ĐỌC VÀ NÓI 4

1. Thảo luận câu hỏi 1.

- Em đã học những loại tư ờng lửa nào?
2. Cụm từ “chế độ xử lý tư ờng lửa” nghĩa là gì?
 3. Bạn biết những chế độ xử lý tư ờng lửa nào? Cung cấp một số thông tin để hỗ trợ câu trả lời của bạn.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

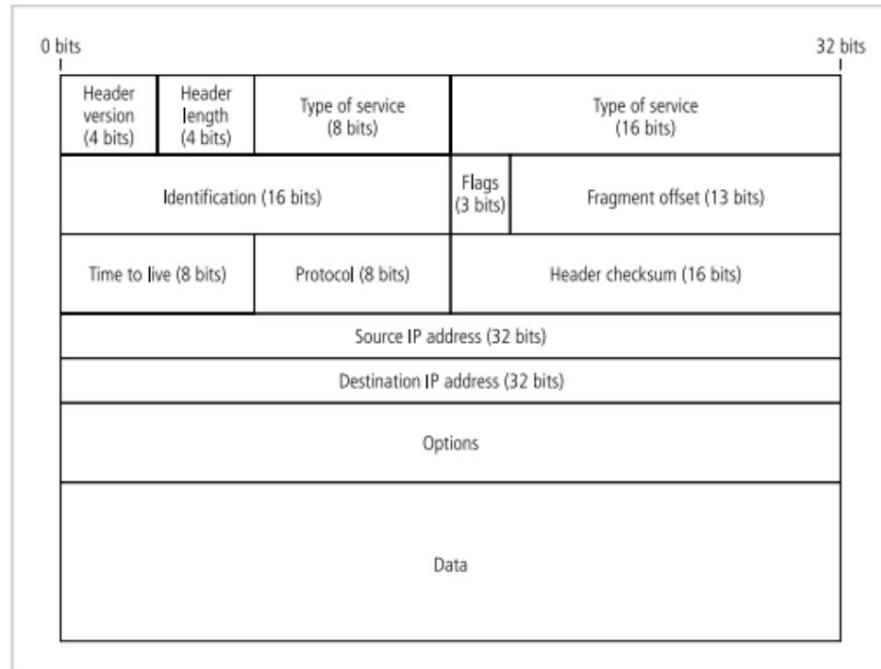
Chế độ xử lý tư ờng lửa (1)

Tư ờng lửa được chia thành năm loại chế độ xử lý chính: tư ờng lửa lọc gói, cổng ứng dụng, cổng mạch, tư ờng lửa lớp MAC và lai.¹ Tư ờng lửa lai sử dụng kết hợp bốn chế độ khác và trong thực tế, hầu hết tư ờng lửa đều thuộc loại này, vì hầu hết các triển khai tư ờng lửa đều sử dụng nhiều cách tiếp cận. Trong phần này chỉ thảo luận về tư ờng lửa lọc gói và phần còn lại sẽ được đề cập sau trong phần đọc thêm.

Tư ờng lửa lọc gói, còn được gọi đơn giản là tư ờng lửa lọc, kiểm tra thông tin tiêu đề của các gói dữ liệu đi vào mạng. Tư ờng lửa lọc gói được cài đặt trên mạng dựa trên TCP/IP thường hoạt động ở cấp độ IP và xác định xem có bỏ gói (từ chối) hay chuyển tiếp gói đến kết nối mạng tiếp theo (cho phép) dựa trên các quy tắc được lập trình trong tư ờng lửa. Tư ờng lửa lọc gói kiểm tra mọi tiêu đề gói đến và có thể lọc có chọn lọc các gói dựa trên thông tin tiêu đề như địa chỉ đích, địa chỉ nguồn, loại gói và thông tin chính khác. **Hình 3-6** cho thấy cấu trúc của một gói tin IPv4.

Tư ờng lửa lọc gói quét các gói dữ liệu mạng để tìm kiếm sự tuân thủ hoặc vi phạm các quy tắc của cơ sở dữ liệu của tư ờng lửa. Tư ờng lửa lọc kiểm tra các gói ở lớp mạng hoặc Lớp 3 của mô hình Kết nối hệ thống mở (OSI), đại diện cho bảy lớp quy trình mạng. (Mô hình OSI được hiển thị ở phần sau của chương này trong Hình 3-6.) Nếu thiết bị tìm thấy một gói phù hợp với một hạn chế, nó sẽ ngăn gói đó di chuyển từ mạng này sang mạng khác. Các hạn chế được triển khai phổ biến nhất trong tư ờng lửa lọc gói dựa trên sự kết hợp của các yếu tố sau:

- Địa chỉ nguồn và đích IP
- Hư ứng (vào hoặc ra)
- Giao thức (dành cho tư ờng lửa có khả năng kiểm tra lớp giao thức IP)
- Giao thức điều khiển truyền dẫn (TCP) hoặc Giao thức gói dữ liệu ngay ời dùng (UDP) yêu cầu cảng nguồn và đích (đối với tư ờng lửa có khả năng kiểm tra lớp TCP/UPD)



Hình 3-6. Cấu trúc gói IP

Cấu trúc gói thay đổi tùy thuộc vào bản chất của gói. Hai loại dịch vụ chính là TCP và UDP (như đã lưu ý ở trên).

Các mô hình tư ờng lửa đơn giản kiểm tra hai khía cạnh của tiêu đề gói: địa chỉ đích và địa chỉ nguồn. Chúng thực thi các hạn chế về địa chỉ, các quy tắc được thiết kế để cấm các gói có địa chỉ nhất định hoặc một phần địa chỉ đi qua thiết bị. Họ thực hiện điều này thông qua ACL, được tạo và sửa đổi bởi quản trị viên tư ờng lửa. **Hình 3-7** cho thấy cách một bộ định tuyến lọc gói tin có thể được sử dụng như một bức tư ờng lửa đơn giản để lọc các gói dữ liệu khỏi các kết nối gửi đến và cho phép các kết nối gửi đi truy cập không hạn chế vào mạng công cộng.

Có ba tập hợp con của tư ờng lửa lọc gói: lọc tĩnh, lọc động và kiểm tra trạng thái. Lọc tĩnh yêu cầu các quy tắc lọc được phát triển và cài đặt với tư ờng lửa. Các quy tắc được tạo và sắp xếp theo trình tự bởi một người trực tiếp chỉnh sửa bộ quy tắc hoặc bởi một người sử dụng

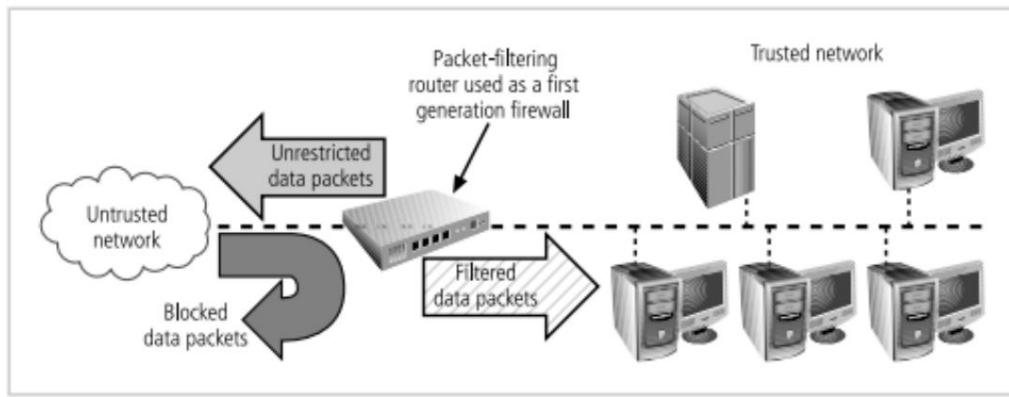
giao diện có thể lập trình để xác định các quy tắc và trình tự. Bất kỳ thay đổi nào đối với các quy tắc đều cần có sự can thiệp của con người. Loại lọc này phổ biến trong các bộ định tuyến và công nghệ.

Tuờng lửa lọc động có thể phản ứng với một sự kiện mới nổi và cập nhật hoặc tạo các quy tắc để xử lý sự kiện đó. Phản ứng này có thể tích cực, chẳng hạn như cho phép người dùng nội bộ tham gia vào một hoạt động cụ thể theo yêu cầu hoặc tiêu cực, như loại bỏ tất cả các gói từ một địa chỉ cụ thể khi phát hiện thấy sự gia tăng của một loại gói không đúng định dạng cụ thể. Trong khi tường lửa lọc tĩnh cho phép toàn bộ một loại gói đi vào để đáp ứng các yêu cầu được ủy quyền, thì tường lửa lọc gói động chỉ cho phép một gói cụ thể có địa chỉ nguồn, đích và công cụ thể đi vào. Nó thực hiện điều này bằng cách mở và đóng các "cánh cửa" trong tường lửa dựa trên thông tin chứa trong tiêu đề gói, làm cho bộ lọc gói động trở thành một dạng trung gian giữa bộ lọc gói tĩnh truyền thống và proxy ứng dụng (sẽ được mô tả sau).

Tuường lửa kiểm tra trạng thái, còn được gọi là tường lửa trạng thái, theo dõi từng kết nối mạng giữa các hệ thống bên trong và bên ngoài bằng cách sử dụng bảng trạng thái. Bảng trạng thái theo dõi trạng thái và ngữ cảnh của từng gói trong cuộc trò chuyện bằng cách ghi lại trạm nào đã gửi gói nào và khi nào. Giống như tường lửa thế hệ đầu tiên, tường lửa kiểm tra trạng thái thực hiện lọc gói, nhưng chúng còn tiến xa hơn một bước.

Trong khi tường lửa lọc gói đơn giản chỉ cho phép hoặc từ chối một số gói nhất định dựa trên địa chỉ của chúng, thì tường lửa có trạng thái có thể đẩy nhanh các gói đến là phản hồi cho các yêu cầu nội bộ. Nếu tường lửa nhận được một gói đến mà nó không khớp với bảng trạng thái của nó, nó sẽ tham chiếu đến ACL của nó để xác định xem có cho phép gói đi qua hay không. Như điểm chính của loại tường lửa này là quá trình xử lý bổ sung cần thiết để quản lý và xác minh các gói dựa trên bảng trạng thái.

Điều này có thể khiến hệ thống dễ bị tấn công DoS hoặc DDoS. Trong một cuộc tấn công như vậy, hệ thống nhận được một số lượng lớn các gói bên ngoài, điều này làm chậm tường lửa vì nó cố gắng so sánh tất cả các gói đến trước với bảng trạng thái và sau đó với ACL. Về mặt tích cực, các tường lửa này có thể theo dõi lưu lượng gói không kết nối, chẳng hạn như lưu lượng truy cập cuộc gọi thủ tục từ xa (RPC) và UDP. Tường lửa lọc trạng thái động giữ một bảng trạng thái động để thực hiện các thay đổi (trong giới hạn được xác định trước) đối với các quy tắc lọc dựa trên các sự kiện khi chúng xảy ra. Bảng trạng thái trông tương tự như bộ quy tắc tường lửa có thêm thông tin.



Hình 3-7. Gói - Bộ định tuyến bộ lọc

2.1. Trả lời các câu hỏi

1. Loại bộ lọc nào phổ biến trong các bộ định tuyến và cổng mạng?
2. Có bao nhiêu tập hợp con tư ờng lừa lọc gói được đề cập trong văn bản?
Họ là ai?
3. Có bao nhiêu loại chế độ xử lý chính được phân loại tư ờng lừa?
Họ là ai?
4. Các mô hình tư ờng lừa đơn giản kiểm tra điều gì?
5. Tư ờng lừa lọc kiểm tra các gói tin ở đâu?
6. Tư ờng lừa lọc gói kiểm tra những gì?
7. Như ợc điểm chính của thanh tra nhà nước là gì

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không thông tin (NI). Sửa cái sai

1. Không có bất kỳ như ợc điểm nào đối với tư ờng lừa trạng thái theo văn bản.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Các hạn chế được thực hiện phổ biến nhất trong lọc gói tư ờng lừa dựa trên sự kết hợp của nguồn IP và địa chỉ đích, hứ ứng, giao thức và TCP.

A. Đúng	B. Sai	C. N.
---------	--------	-------
3. Giống như tư ờng lừa thế hệ thứ nhất, tư ờng lừa kiểm tra trạng thái thực hiện lọc gói, nhưng họ tiến thêm một bước.

A. Đúng	B. Sai	C. NI
---------	--------	-------

4. Khả năng kiểm toán đảm bảo rằng tất cả các hành động trên một hệ thống đều có thể đưa ra
đưa ra cho một danh tính đưa ra xác thực.

A. Đúng

B. Sai

C. NI

5. Theo văn bản, tất cả các chế độ xử lý tự ứng lừa đưa ra hiển thị.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu sau

1. yêu cầu các quy tắc lọc đưa ra phát triển và cài đặt với
tự ứng lừa.

A. lọc gói động

B. Lọc tĩnh

C. lọc trạng thái

D. A & B đúng

2. Trong khi tự ứng lừa lọc tĩnh cho phép toàn bộ một loại gói
enter để đáp ứng các yêu cầu đưa ra ủy quyền, chỉ cho phép một
gói cụ thể với một địa chỉ nguồn, đích và cổng cụ thể để
đi vào.

A. lọc gói động

B. lọc tĩnh

C. Lọc trạng thái

D. A&C đều đúng

3. Cấu trúc gói thay đổi tùy thuộc vào bản chất của gói. Cả hai
các loại dịch vụ chính là

A. UDP

B. TCP

C. A & B đều đúng

NHƯNG, DÌM

4. Từ "họ" trong đoạn 4 đề cập đến điều nào sau đây?

A. hai khía cạnh

B. Mô hình tự ứng lừa đơn giản

C. địa chỉ đích và nguồn

D. quy tắc

5. Tự ứng lừa lọc gói kiểm tra mọi tiêu đề gói đến và có thể
.... lọc gói dựa trên thông tin tiêu đề.

A. tự động

B. thông thư ứng

C. có chọn lọc

D. tính toán

4. Lắng nghe

1. <https://www.youtube.com/watch?v=kDEX1HXybrU>
2. <https://www.youtube.com/watch?v=5cPIukqXe5w>

VIẾT VÀ NÓI

1. Viết khoảng 400 từ về một trong những nội dung sau bằng văn bản của bạn

từ ngữ:

- Tự ờng lửa và lịch sử của nó
- Kiến trúc tự ờng lửa

2. Trình bày các chủ đề sau:

- Tự ờng lửa và lịch sử của nó
- Kiến trúc tự ờng lửa

ĐỌC THÊM

Chế độ xử lý tư ờng lửa (2)

Cỗng ứng dụng

Cỗng ứng dụng, còn được gọi là tư ờng lửa cấp ứng dụng hoặc tư ờng lửa ứng dụng, thư ờng được cài đặt trên một máy tính chuyên dụng, tách biệt với bộ định tuyến lọc, như ng thư ờng được sử dụng cùng với bộ định tuyến lọc. Tư ờng lửa ứng dụng còn được gọi là máy chủ proxy vì nó chạy phần mềm đặc biệt hoạt động như một proxy cho yêu cầu dịch vụ. Ví dụ: một tổ chức chạy máy chủ Web có thể tránh để máy chủ tiếp xúc với lưu lượng người dùng trực tiếp bằng cách cài đặt máy chủ proxy được định cấu hình bằng URL của miền đã đăng ký.

Máy chủ proxy này nhận các yêu cầu cho các trang Web, truy cập máy chủ Web thay mặt cho máy khách bên ngoài và trả lại các trang được yêu cầu cho người dùng. Các máy chủ này có thể lưu trữ các trang được truy cập gần đây nhất trong bộ nhớ cache bên trong của chúng và do đó còn được gọi là máy chủ bộ nhớ cache. Thứ nhất, máy chủ proxy được đặt trong khu vực không an toàn của mạng hoặc trong khu vực phi quân sự (DMZ)–một khu vực trung gian giữa mạng đáng tin cậy và mạng không đáng tin cậy–để nó, thay vì máy chủ Web, tiếp xúc với mức độ rủi ro cao hơn từ các mạng kém tin cậy hơn. Các bộ định tuyến lọc bổ sung có thể được triển khai phía sau máy chủ proxy, hạn chế quyền truy cập vào hệ thống nội bộ an toàn hơn và do đó bảo vệ thêm các hệ thống nội bộ.

Một ví dụ phổ biến về tư ờng lửa cấp ứng dụng (hoặc máy chủ proxy) là tư ờng lửa chặn tất cả các yêu cầu và phản hồi đối với các yêu cầu đối với các trang Web và dịch vụ từ các máy tính nội bộ của một tổ chức và thay vào đó chuyển tất cả các yêu cầu và phản hồi đó sang trung gian. máy tính (hoặc proxy) trong các khu vực ít được bảo vệ hơn trong mạng của tổ chức. Kỹ thuật này vẫn được sử dụng rộng rãi để thực hiện các chức năng thư ờng mại điện tử, mặc dù hầu hết người dùng công nghệ này đã nâng cấp để tận dụng lợi thế của phương pháp DMZ được thảo luận bên dưới.

Như ợc điểm chính của tư ờng lửa cấp ứng dụng là chúng được thiết kế cho một hoặc một vài giao thức cụ thể và không thể dễ dàng cấu hình lại để bảo vệ chống lại các cuộc tấn công vào các giao thức khác. Vì tư ờng lửa ứng dụng hoạt động ở lớp ứng dụng (do đó có tên), nên chúng thư ờng bị giới hạn ở một ứng dụng duy nhất (ví dụ: FTP, Telnet, HTTP, SMTP và SNMP). Thời gian xử lý và tài nguyên cần thiết để đọc từng gói xuống lớp ứng dụng làm giảm khả năng xử lý nhiều loại ứng dụng của các tư ờng lửa này.

Cổng mạch

Tư ờng lửa cổng mạch hoạt động ở lớp vận chuyển. Một lần nữa, các kết nối đư ợc ủy quyền dựa trên địa chỉ. Giống như tư ờng lửa lọc, tư ờng lửa cổng mạch thư ờng không xem xét lưu lư ợng chảy giữa mạng này với mạng khác, nhưng chúng ngăn chặn các kết nối trực tiếp giữa mạng này với mạng khác. Họ thực hiện điều này bằng cách tạo các đường hầm kết nối các quy trình hoặc hệ thống cụ thể ở mỗi bên của tư ờng lửa, sau đó chỉ cho phép lưu lư ợng đư ợc ủy quyền, chẳng hạn như một loại kết nối TCP cụ thể cho người dùng đư ợc ủy quyền, trong các đường hầm này. Cổng mạch là một thành phần tư ờng lửa thư ờng đư ợc bao gồm trong danh mục cổng ứng dụng, nhưng thực tế nó là một loại tư ờng lửa riêng biệt.

Tư ờng lửa lớp MAC

Mặc dù không đư ợc biết đến nhiều hoặc đư ợc tham chiếu rộng rãi như cách tiếp cận tư ờng lửa ở trên, tư ờng lửa lớp MAC đư ợc thiết kế để hoạt động ở lớp con kiểm soát truy cập phư ơng tiện của lớp liên kết dữ liệu (Lớp 2) của mô hình mạng OSI. Điều này cho phép các tư ờng lửa này xem xét danh tính của máy chủ cụ thể, như đư ợc biểu thị bằng địa chỉ MAC hoặc thẻ giao diện mạng (NIC) trong các quyết định lọc của nó. Do đó, tư ờng lửa lớp MAC liên kết địa chỉ của các máy chủ cụ thể với các mục ACL xác định các loại gói cụ thể có thể đư ợc gửi đến từng máy chủ và chặn tất cả lưu lư ợng truy cập khác.

Hình 6-6 cho thấy vị trí trong mô hình OSI, mỗi chế độ xử lý tư ờng lửa sẽ kiểm tra dữ liệu.

Tư ờng lửa hỗn hợp

Tư ờng lửa hỗn hợp kết hợp các yếu tố của các loại tư ờng lửa khác– nghĩa là, các yếu tố lọc gói và dịch vụ proxy, hoặc lọc gói và cổng mạch. Một hệ thống tư ờng lửa lai có thể thực sự bao gồm hai thiết bị tư ờng lửa riêng biệt; mỗi cái là một hệ thống tư ờng lửa riêng biệt, nhưng chúng đư ợc kết nối để hoạt động song song. Ví dụ, một hệ thống tư ờng lửa kết hợp có thể bao gồm một tư ờng lửa lọc gói đư ợc thiết lập để sàng lọc tất cả các yêu cầu có thể chấp nhận đư ợc, sau đó chuyển các yêu cầu tới một máy chủ proxy, máy chủ này sẽ lần lượt yêu cầu các dịch vụ từ một máy chủ Web sâu bên trong mạng của tổ chức. Một lợi thế bổ sung cho phư ơng pháp tư ờng lửa kết hợp là nó cho phép một tổ chức thực hiện cải tiến bảo mật mà không cần thay thế hoàn toàn các tư ờng lửa hiện có.

ĐỌC THÊM

Bộ lọc nội dung

Một tiện ích khác có thể giúp bảo vệ hệ thống của tổ chức khỏi các sự cố từ chối dịch vụ không chủ ý và sử dụng sai mục đích, và thường được liên kết chặt chẽ với tường lửa, là bộ lọc nội dung. Bộ lọc nội dung là một bộ lọc phần mềm—về mặt kỹ thuật không phải là tường lửa—cho phép quản trị viên hạn chế quyền truy cập vào nội dung từ bên trong mạng. Về cơ bản, nó là một tập hợp các tập lệnh hoặc chương trình hạn chế quyền truy cập của người dùng vào các giao thức mạng và vị trí Internet nhất định hoặc hạn chế người dùng nhận các loại chung hoặc ví dụ cụ thể về nội dung Internet. Một số gọi bộ lọc nội dung là tường lửa đảo ngược, vì mục đích chính của chúng là hạn chế quyền truy cập nội bộ vào tài liệu bên ngoài. Trong hầu hết các mô hình triển khai phổ biến, bộ lọc nội dung có hai thành phần: xếp hạng và lọc. Xếp hạng giống như một bộ quy tắc tường lửa cho các trang Web và phổ biến trong các bộ lọc dân cư. Xếp hạng có thể phức tạp, với nhiều cài đặt kiểm soát truy cập cho các cấp khác nhau của tổ chức hoặc có thể đơn giản, với lược đồ cho phép/từ chối cơ bản giống như lược đồ của tường lửa. Lọc là một phương pháp được sử dụng để hạn chế các yêu cầu truy cập cụ thể đối với các tài nguyên đã xác định, có thể là các trang Web, máy chủ hoặc bất kỳ tài nguyên nào mà quản trị viên bộ lọc nội dung định cấu hình. Đây là một loại ACL đảo ngược (về mặt kỹ thuật, bảng khả năng), trong đó ACL thường ghi lại một nhóm người dùng có quyền truy cập vào tài nguyên, danh sách kiểm soát này ghi lại các tài nguyên mà người dùng không thể truy cập.

Các bộ lọc nội dung đầu tiên là các hệ thống được thiết kế để hạn chế quyền truy cập vào các trang Web cụ thể và là các ứng dụng phần mềm độc lập. Chúng có thể được cấu hình theo cách độc quyền hoặc toàn diện. Trong chế độ độc quyền, một số trang nhất định được loại trừ cụ thể. Vấn đề với cách tiếp cận này là có thể có hàng nghìn trang Web mà một tổ chức muốn loại trừ và nhiều trang khác có thể được thêm vào mỗi giờ. Chế độ bao gồm hoạt động từ danh sách các trang web được phép cụ thể. Để có một trang web được thêm vào danh sách, người dùng phải gửi yêu cầu tới trình quản lý bộ lọc nội dung, điều này có thể tồn thời gian và hạn chế hoạt động kinh doanh. Các mô hình mới hơn của bộ lọc nội dung dựa trên giao thức, kiểm tra nội dung khi nó được hiển thị động và hạn chế hoặc cho phép truy cập dựa trên diễn giải hợp lý của nội dung.

Các bộ lọc nội dung phổ biến nhất hạn chế người dùng truy cập các trang Web có tài liệu rõ ràng không liên quan đến kinh doanh, chẳng hạn như nội dung khiêu dâm hoặc từ chối e-mail spam gửi đến. Bộ lọc nội dung có thể là các chương trình phần mềm hỗ trợ nhỏ dành cho gia đình hoặc văn phòng, chẳng hạn như Net Nanny hoặc Surf Control hoặc các ứng dụng của công ty, chẳng hạn như Novell Border Manager. Lợi ích của việc triển khai các bộ lọc nội dung là đảm bảo rằng nhân viên không bị phân tâm bởi các tài liệu phi kinh doanh và không tốn phí thời gian và nguồn lực của tổ chức. Như một điểm là các hệ thống này yêu cầu cấu hình mở rộng và bảo trì liên tục để luôn cập nhật danh sách các điểm đến không được chấp nhận hoặc địa chỉ nguồn cho e-mail bị hạn chế gửi đến. Một số ứng dụng lọc nội dung mới hơn (như các chương trình chống vi-rút mới hơn) đi kèm với dịch vụ các tệp có thể tải xuống để cập nhật cơ sở dữ liệu về các hạn chế. Các ứng dụng này hoạt động bằng cách đối sánh danh sách các trang Web bị từ chối hoặc được chấp thuận và bằng cách đối sánh các từ có nội dung chính, chẳng hạn như "không thân" và "tình dục". Tuy nhiên, những người tạo nội dung bị hạn chế đã nhận ra điều này và cố gắng vượt qua các hạn chế bằng cách loại bỏ các loại từ chuyên đi này, do đó tạo thêm các vấn đề cho các chuyên gia mạng và bảo mật.

BÀI 4: CÔNG NGHỆ AN NINH

ĐỌC VÀ NÓI 1

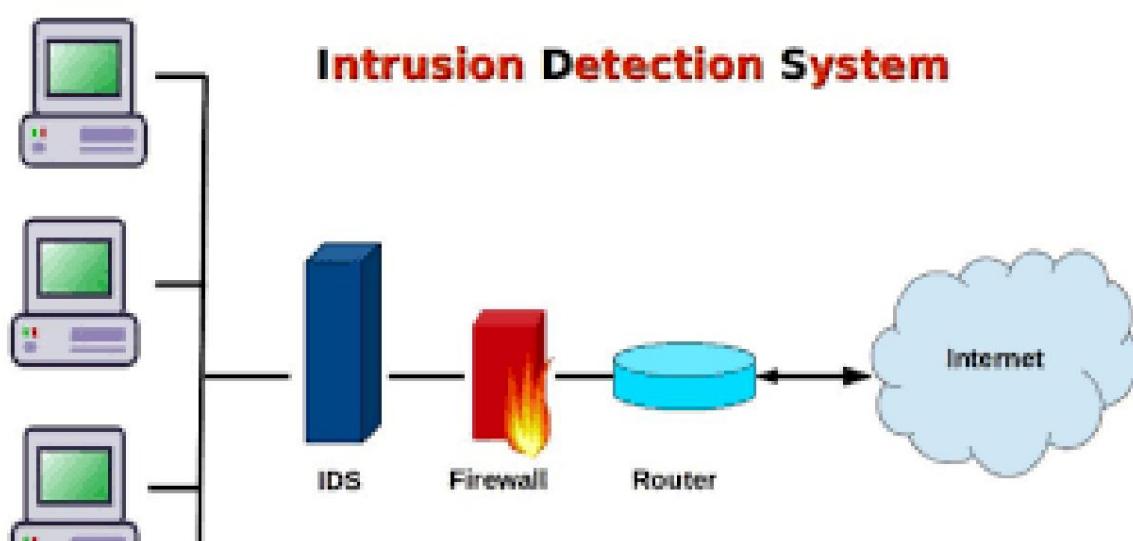
1. Thảo luận các câu hỏi

1. IDPS là viết tắt của từ gì? Nó có nghĩa là gì trong ngôn ngữ của bạn?
2. Bạn biết gì về IDPS?
3. IDPS dùng để làm gì?
4. Từ "xâm nhập" nghĩa là gì?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Hệ thống phát hiện và ngăn chặn xâm nhập

Hệ thống phát hiện xâm nhập (IDS) (xem Hình 4-1) là một thiết bị hoặc ứng dụng phần mềm giám sát mạng hoặc hệ thống để phát hiện hoạt động độc hại hoặc vi phạm chính sách. Bất kỳ hoạt động hoặc vi phạm độc hại nào thư ờng được báo cáo cho quản trị viên hoặc được thu thập tập trung bằng cách sử dụng hệ thống quản lý sự kiện và thông tin bảo mật (SIEM). Một hệ thống SIEM kết hợp các đầu ra từ nhiều nguồn và sử dụng các kỹ thuật lọc cảnh báo để phân biệt hoạt động độc hại với các cảnh báo sai.



Hình 4-1. Hệ thống phát hiện xâm nhập

Các hệ thống phát hiện xâm nhập bảo mật thông tin (IDS) đã có mặt trên thị trường vào cuối những năm 1990. IDS hoạt động giống như thiết bị báo trộm ở chỗ nó phát hiện hành vi vi phạm (một số hoạt động của hệ thống tự ngưng tự như cửa sổ bị mở hoặc bị hỏng) và kích hoạt báo động. Báo động này có thể là âm thanh và/hoặc hình ảnh (tương ứng tạo ra tiếng ồn và đèn) hoặc có thể ở chế độ im lặng (thông báo e-mail hoặc cảnh báo máy nhắn tin). Với hầu hết tất cả các IDS, quản trị viên hệ thống có thể chọn cấu hình của các cảnh báo khác nhau và các mức cảnh báo liên quan đến từng loại cảnh báo. Nhiều IDS cho phép quản trị viên cấu hình hệ thống để thông báo cho họ về sự cố trực tiếp qua e-mail hoặc máy nhắn tin. Các hệ thống này cũng có thể được cấu hình một lần nữa giống như hệ thống báo động chống trộm—để thông báo cho tổ chức dịch vụ an ninh bên ngoài về một vụ “đột nhập”. Các cấu hình cho phép IDS cung cấp các mức phát hiện và phản hồi tùy chỉnh khá phức tạp. Một phần mở rộng hiện tại của công nghệ IDS là hệ thống ngăn chặn xâm nhập (IPS), có thể phát hiện một sự xâm nhập và cũng ngăn chặn sự xâm nhập đó tấn công thành công bằng một phản ứng tích cực. Bởi vì hai hệ thống thường cùng tồn tại, thuật ngữ kết hợp hệ thống phát hiện và ngăn chặn xâm nhập (IDPS) thường được sử dụng để mô tả các công nghệ chống xâm nhập hiện tại.

Tại sao nên sử dụng IDPS?

Theo tài liệu của NIST về các phương pháp hay nhất trong ngành, có một số lý do thuyết phục để mua và sử dụng IDPS:

1. Để ngăn chặn các hành vi có vấn đề bằng cách tăng nguy cơ bị phát hiện và trừng phạt đối với những người săn tấn công hoặc lạm dụng hệ thống
2. Để phát hiện các cuộc tấn công và vi phạm an ninh khác không được ngăn chặn bởi các biện pháp an ninh khác
3. Để phát hiện và đối phó với các dấu hiệu mở đầu của các cuộc tấn công (thường gấp phải khi thăm dò mạng và các hoạt động “lách cách nấm cửa” khác)
4. Để ghi lại mối đe dọa hiện có đối với một tổ chức
5. Đóng vai trò kiểm soát chất lượng cho thiết kế và quản trị an ninh, đặc biệt là trong doanh nghiệp lớn và phức tạp
6. Cung cấp thông tin hữu ích về các xâm nhập đang diễn ra, cho phép cải thiện chẩn đoán, phục hồi và khắc phục các yếu tố gây bệnh

Một trong những lý do tốt nhất để cài đặt IDPS là chúng đóng vai trò ngăn chặn bằng cách làm tăng nỗi sợ bị phát hiện giữa những kẻ tấn công tiềm năng. Nếu người dùng nội bộ và bên ngoài biết rằng một tổ chức có hệ thống ngăn chặn và phát hiện xâm nhập, họ sẽ ít có khả năng thăm dò hoặc cố gắng xâm phạm hệ thống đó, cũng như bọn tội phạm ít có khả năng đột nhập vào một ngôi nhà có chuông báo trộm rõ ràng.

Một lý do khác để cài đặt IDPS là để bảo vệ tổ chức khi mạng của tổ chức không thể tự bảo vệ mình trước các lỗ hổng đã biết hoặc không thể phản ứng với mối đe dọa thay đổi nhanh chóng. Có nhiều yếu tố có thể trì hoãn hoặc làm suy yếu khả năng của một tổ chức trong việc bảo vệ hệ thống của mình khỏi bị tấn công và mất mát sau đó.

IDPS cũng có thể giúp quản trị viên phát hiện các phần mở đầu của các cuộc tấn công. Hầu hết các cuộc tấn công đều bắt đầu bằng việc thăm dò có tổ chức và kỹ lưỡng môi trường mạng của tổ chức và hệ thống phòng thủ của nó. Ước tính ban đầu này về trạng thái phòng thủ của một mạng và hệ thống của tổ chức được gọi là tiếng lạch cách của tay nắm cửa và được thực hiện bằng phương pháp in chân (các hoạt động thu thập thông tin về tổ chức cũng như các hoạt động và tài sản mạng của tổ chức) và lấy dấu vân tay (các hoạt động quét các vị trí mạng để tìm các hệ thống đang hoạt động và sau đó xác định các dịch vụ mạng được cung cấp bởi các hệ thống máy chủ). Một hệ thống có khả năng phát hiện các dấu hiệu cảnh báo sớm về việc in dấu chân và lấy dấu vân tay có chức năng giống như một người giám sát khu phố phát hiện ra những kẻ trộm có thể đang kiểm tra cửa ra vào và cửa sổ, cho phép quản trị viên chuẩn bị cho một cuộc tấn công tiềm tàng hoặc thực hiện các hành động để giảm thiểu tổn thất có thể xảy ra từ một cuộc tấn công.

Lý do thứ tư để có được IDPS là tài liệu về mối đe dọa. Việc triển khai công nghệ bảo mật thư ờng yêu cầu những người dùng đề xuất dự án ghi lại mối đe dọa mà tổ chức phải được bảo vệ. IDPS là một phương tiện để thu thập dữ liệu đó. (Để thu thập thông tin tấn công nhằm hỗ trợ triển khai IDPS, bạn có thể bắt đầu với công cụ IDPS phần mềm miễn phí chẳng hạn như Snort).

Cuối cùng, ngay cả khi IDPS không thể ngăn chặn một cuộc xâm nhập, nó vẫn có thể hỗ trợ việc xem xét sau cuộc tấn công bằng cách cung cấp thông tin về cách thức cuộc tấn công xảy ra, những gì kẻ xâm nhập đã thực hiện và những phương pháp mà kẻ tấn công đã sử dụng. Thông tin này có thể được sử dụng để khắc phục những thiếu sót và chuẩn bị môi trường mạng của tổ chức cho các cuộc tấn công trong tương lai. IDPS cũng có thể cung cấp thông tin pháp y có thể hữu ích nếu kẻ tấn công bị bắt và truy tố hoặc kiện.

2.1. Trả lời các câu hỏi

1. Khi nào các hệ thống phát hiện xâm nhập an toàn thông tin được thư ứng mại hóa có sẵn?
2. Nhiều IDS hỗ trợ người quản trị làm gì?
3. IPS là gì? Nó có thể làm gì?
4. Hệ thống phát hiện xâm nhập là gì?
5. IDS hoạt động như thế nào?
6. Có bao nhiêu lý do cần cài đặt IDPS?
7. Một trong những lý do quan trọng nhất để cài đặt IDPS là gì?
8. Đưa ra một số mô tả về IDS.

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không

thông tin (NI)

1. IDS hoạt động giống như đồng hồ báo thức ở chỗ nó phát hiện vi phạm và kích hoạt một báo động.
A. Đúng B. Sai C. NI
2. Theo văn bản, bốn lý do được đưa ra để chỉ ra rằng các IDS cần cài đặt.
A. Đúng B. Sai C. NI
3. Khi hoạt động độc hại hoặc vi phạm xuất hiện, quản trị viên thường được thông báo theo một cách nào đó.
A. Đúng B. Sai C. NI
4. Viết và triển khai chính sách bảo mật thông tin doanh nghiệp tốt là các hoạt động phòng chống xâm nhập quan trọng.
A. Đúng B. Sai C. NI
5. Trì hoãn hoặc làm suy yếu khả năng của một tổ chức trong việc bảo vệ hệ thống của mình khỏi bị tấn công và mất mát sau đó phụ thuộc vào nhiều yếu tố.
A. Đúng B. Sai C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu sau

1. Hệ thống nào kết hợp đầu ra từ nhiều nguồn và sử dụng kỹ thuật lọc báo động để phân biệt hoạt động độc hại với báo động giả?

A. Một hệ thống IDPS

B. Một hệ thống SIEM

C. IDP

D. A&C đều đúng

2. Để thu thập thông tin tấn công nhằm hỗ trợ triển khai IDPS, bạn có thể bắt đầu bằngchẳng hạn như Snort.

A. IDPS phần cứng

B. phần sụn IDPS

C. một công cụ IDPS phần mềm miễn phí

D. gói phần mềm

3. Thuật ngữ IDPS và IPS thư ờng được sử dụng để làm gì?

A. để mô tả các chương trình diệt virus

B. để mô tả các công nghệ chống xâm nhập hiện tại

C. để mô tả các chế độ IDPS

D. B & C đều đúng

4. IDPS cũng có thể cung cấp thông tin pháp y có thể hữu ích nếu kẻ tấn công là

A. bị bắt

B. bị kiện

C. truy tố

D. tất cả đều đúng

5. IDS làgiám sát mạng hoặc hệ thống để phát hiện hoạt động độc hại hoặc vi phạm chính sách.

Một phần mềm

B. thiết bị

đơn vị C.

D. A & B đúng

3. Nói

1. Trình bày hệ thống phát hiện và ngăn chặn xâm nhập (IDPS)

2. Trình bày lý do tại sao một IDPS được cài đặt.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi

1. NIDS là viết tắt của từ gì? Nó có nghĩa là gì?
2. HIDS là viết tắt của từ gì? Nó có nghĩa là gì?
3. NIDS và HIDS dùng để làm gì?
4. Cụm từ Mạng nơ -ron nhân tạo có nghĩa là gì nghĩa là?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

NIDS & HIDS

Hệ thống phát hiện xâm nhập mạng (NIDS) được đặt tại một hoặc nhiều điểm chiến lược trong mạng để giám sát lưu lượng đến và đi từ tất cả các thiết bị trên mạng.

Nó thực hiện phân tích lưu lượng truy cập trên toàn bộ mạng con và so khớp lưu lượng truy cập được truyền trên các mạng con với thư viện các cuộc tấn công đã biết. Khi một cuộc tấn công được xác định hoặc hành vi bất thường được cảm nhận, cảnh báo có thể được gửi đến quản trị viên. Một ví dụ về NIDS sẽ cài đặt nó trên mạng con nơi i đặt tường lửa để xem liệu có ai đó đang cố đột nhập vào tường lửa hay không.

Lý do nhất là quét tất cả lưu lượng truy cập vào và ra, tuy nhiên, làm như vậy có thể tạo ra nút cản chia làm giảm tốc độ chung của mạng.

OPNET và NetSim là những công cụ thử nghiệm được sử dụng để mô phỏng các hệ thống phát hiện xâm nhập mạng. Hệ thống NID cũng có khả năng so sánh chữ ký cho các gói tương tự để liên kết và loại bỏ các gói được phát hiện có hại có chữ ký khớp với các bản ghi trong NIDS. Khi chúng tôi phân loại thiết kế của NIDS theo thuộc tính tương tác hệ thống, có hai loại: NIDS trực tuyến và ngoại tuyến, thường được gọi tương ứng là chế độ nội tuyến và chế độ chậm. NIDS trực tuyến xử lý mạng trong thời gian thực. Nó phân tích các gói Ethernet và áp dụng một số quy tắc để quyết định xem đó có phải là một cuộc tấn công hay không. NIDS ngoại tuyến xử lý dữ liệu được lưu trữ và chuyển dữ liệu đó qua một số quy trình để quyết định xem đó có phải là một cuộc tấn công hay không.

NIDS cũng có thể được kết hợp với các công nghệ khác để tăng tỷ lệ phát hiện và dự đoán. IDS dựa trên Mạng nơ -ron nhân tạo có khả năng phân tích khôi lưu lượng dữ liệu khổng lồ, theo cách thông minh, do cấu trúc tự tổ chức cho phép INS IDS nhận dạng các mẫu xâm nhập hiệu quả hơn. Mạng lưu trữ thần kinh hỗ trợ IDS trong việc dự đoán các cuộc tấn công bằng cách học hỏi từ những sai lầm; INN IDS giúp phát triển

một hệ thống cảnh báo sớm, dựa trên hai lớp. Lớp đầu tiên chấp nhận các giá trị đơn lẻ, trong khi lớp thứ hai lấy ra của lớp đầu tiên làm đầu vào; chu kỳ lặp lại và cho phép hệ thống tự động nhận dạng các mẫu mới không lưu trữ trước được trong mạng. Hệ thống này có thể phát hiện và phân loại tỷ lệ trung bình 99,9%, dựa trên kết quả nghiên cứu của 24 cuộc tấn công mạng, được chia thành bốn loại: DOS, Probe, Remote-to-Local và user-to-root.

Hệ thống phát hiện xâm nhập dựa trên máy chủ (HIDS) là một hệ thống phát hiện xâm nhập có khả năng giám sát và phân tích các phần bên trong của hệ thống máy tính cũng như các gói mạng trên các giao diện mạng của nó, tương tự như cách hệ thống phát hiện xâm nhập dựa trên mạng (NIDS) hoạt động. Đây là loại phần mềm phát hiện xâm nhập đầu tiên được thiết kế, với hệ thống mục tiêu ban đầu là máy tính lớn, nơi không thường xuyên có tương tác bên ngoài.

IDS dựa trên máy chủ có khả năng giám sát tất cả hoặc một phần hành vi động và trạng thái của hệ thống máy tính, dựa trên cách nó được cấu hình. Bên cạnh các hoạt động như kiểm tra động các gói mạng được nhắm mục tiêu vào máy chủ cụ thể này (thành phần tùy chọn với hầu hết các giải pháp phần mềm có sẵn trên thị trường), HIDS có thể phát hiện chương trình nào truy cập tài nguyên nào và phát hiện ra rằng, ví dụ: một trình xử lý văn bản đã bắt đầu sửa đổi đột ngột và không thể giải thích được. cơ sở dữ liệu mật khẩu hệ thống. Tương tự, một HIDS có thể xem xét trạng thái của hệ thống, thông tin được lưu trữ của nó, cho dù trong RAM, trong hệ thống tệp, tệp nhật ký hay bất kỳ nơi nào khác; và kiểm tra xem nội dung của chúng có xuất hiện như mong đợi không, ví dụ: không bị thay đổi bởi những kẻ xâm nhập.

Người ta có thể coi HIDS như một tác nhân giám sát xem bất kỳ thứ gì hoặc bất kỳ ai, dù là bên trong hay bên ngoài, có phá vỡ chính sách bảo mật của hệ thống hay không.

Bảo vệ HIDS

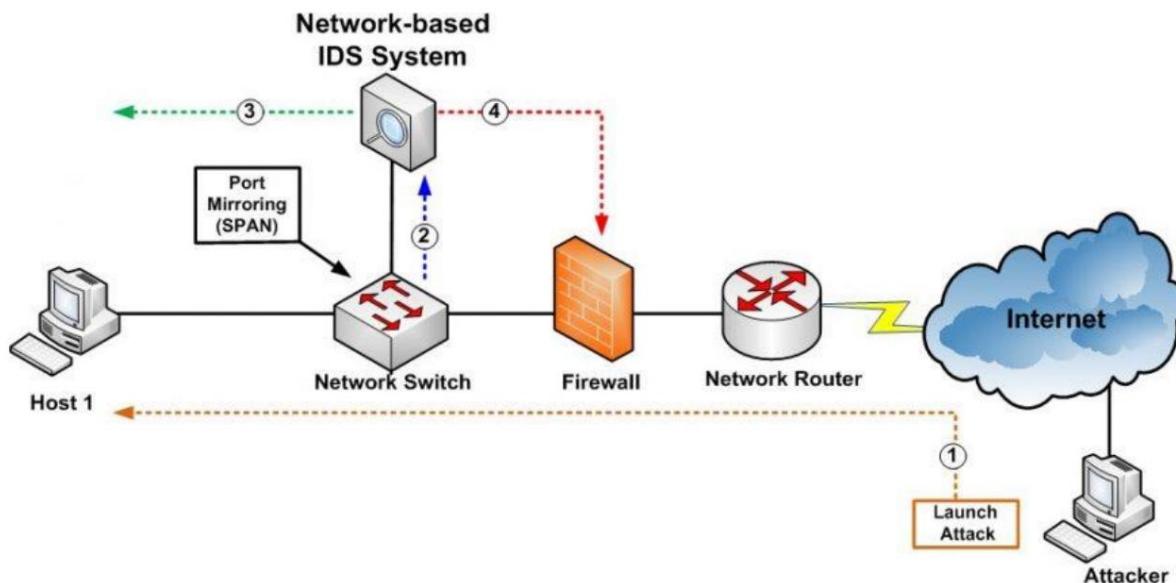
Một HIDS thường sẽ cố gắng hết sức để ngăn cơ sở dữ liệu đổi tương ứng, cơ sở dữ liệu tổng kiểm tra và các báo cáo của nó khỏi bất kỳ hình thức giả mạo nào. Xét cho cùng, nếu những kẻ xâm nhập thành công trong việc sửa đổi bất kỳ đối tượng nào mà HIDS giám sát, thì không gì có thể ngăn cản những kẻ xâm nhập đó tự sửa đổi HIDS - trừ khi người quản trị an ninh thực hiện các biện pháp phòng ngừa thích hợp. Ví dụ, nhiều sâu và vi-rút sẽ cố gắng vô hiệu hóa các công cụ chống vi-rút.

Ngoài các kỹ thuật mật mã, HIDS có thể cho phép quản trị viên lưu trữ cơ sở dữ liệu trên đĩa CD-ROM hoặc trên các thiết bị bộ nhớ chỉ đọc khác (một yếu tố khác

ngăn chặn các bản cập nhật không thư ờng xuyên...) hoặc lưu trữ chúng trong một số bộ nhớ ngoài hệ thống. Từ ờng tự như vậy, một HIDS thư ờng sẽ gửi nhật ký ra khỏi hệ thống ngay lập tức - điển hình là sử dụng các kênh VPN tới một số hệ thống quản lý trung tâm.

Người ta có thể lập luận rằng mô-đun nền tảng đáng tin cậy bao gồm một loại HIDS.

Mặc dù phạm vi của nó khác với phạm vi của HIDS theo nhiều cách, nhưng về cơ bản, nó cung cấp một phương tiện để xác định xem có bất kỳ thứ gì/bất kỳ ai nào đã can thiệp vào một phần của máy tính hay không. Về mặt kiến trúc, điều này cung cấp khả năng phát hiện xâm nhập dựa trên máy chủ (ít nhất là tại thời điểm này), phụ thuộc vào phần cứng bên ngoài của chính CPU, do đó khiến kẻ xâm nhập khó làm hỏng đổi tư ờng của nó hơn nhiều và cơ sở dữ liệu tổng kiểm tra.



Hình 4-2. Hệ thống phát hiện xâm nhập dựa trên mạng

2.1. Trả lời các câu hỏi

1. Chức năng của NIDS là gì?
2. Sự khác biệt giữa NIDS trực tuyến và NIDS ngoại tuyến là gì?
3. Hệ thống phát hiện xâm nhập dựa trên máy chủ là gì?
4. IDS dựa trên máy chủ có khả năng làm gì?
5. OPNET và NetSim là gì? Chúng nó được dùng cho cái gì?
6. Điều gì có thể xảy ra nếu những kẻ xâm nhập thành công trong việc sửa đổi bất kỳ đối tượng nào mà Màn hình HIDS?

7. HIDS có thể làm gì ngoài kỹ thuật mã hóa?
8. Những loại NIDS nào được đề cập trong văn bản? Bạn dựa vào cái gì phân loại thiết kế của NIDS?
- 2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Theo văn bản, nhờ mạng Neural, IDS có thể dự đoán các cuộc tấn công khi chúng xuất hiện.
- A. Đúng B. Sai C. NI
2. Bản thân quản trị viên có thể xác định một cuộc tấn công mà không cần hệ thống phát hiện xâm nhập.
- A. Đúng B. Sai C. NI
3. Để kiểm soát lưu lượng đến và đi từ tất cả các thiết bị trên mạng Hệ thống phát hiện xâm nhập mạng được đặt tại một hoặc nhiều điểm chiến lược trong mạng.
- A. Đúng B. Sai C. NI
4. Các giải pháp phần mềm có sẵn trên thị trường thường tư duy quan với các phát hiện từ NIDS và HIDS để tìm hiểu xem kẻ xâm nhập mạng có thành công hay không tại máy chủ được nhắm mục tiêu.
- A. Đúng B. Sai C. NI
5. Cả NIDS và HIDS đều có khả năng riêng để thực hiện các chức năng khác nhau.
- A. Đúng B. Sai C. NI
- 2.3. Chọn câu trả lời đúng nhất để hoàn thành các câu hỏi và câu sau
1. NIDS có bao nhiêu loại theo thuộc tính tư duy tác của hệ thống? Họ là ai?
- A. Nó có hai loại: NIDS trực tuyến và ngoại tuyến
- B. Nó có một: NIDS ngoại tuyến
- C. Nó chỉ có một: NIDS trực tuyến
- D. B & C đều đúng
2. Tại sao các hệ thống phát hiện xâm nhập mạng được đặt tại một điểm chiến lược hoặc các điểm trong mạng?

- A. Để kiểm soát lưu lư ợng đến và đi từ tất cả các thiết bị trên mạng.
 - B. Để giám sát lưu lư ợng đến và đi từ tất cả các thiết bị trên mạng.
 - C. Để giám sát lưu lư ợng truy cập từ và đến tất cả các thiết bị trên mạng.
 - D. B & C đều đúng
3. Hệ thống NIDso sánh chữ ký cho các gói tương tự để liên kết và loại bỏ các gói được phát hiện có hại có chữ ký khớp với các bản ghi trong NIDS.
- A. cũng có thể
 - B. chịu trách nhiệm về
 - C. cũng có khả năng
 - D. A & C đều đúng
4.cũng có thể được kết hợp với các công nghệ khác để tăng tỷ lệ phát hiện và dự đoán.
- A. HIDS
 - B. NIDS
 - C. INN
 - D. ÂN
5. Tại sao HIDS thường có độ dài lớn?
- A. Để ngăn cơ sở dữ liệu đối tượng, cơ sở dữ liệu tổng kiểm tra
 - B. Để báo cáo từ bất kỳ hình thức giả mạo nào.
 - C. A & B đều đúng
 - D. Để phát hiện object-database, checksum-database

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào?
2. Trình bày các nội dung sau:
 - NIDS
 - HIDS
 - Sự khác biệt giữa NIDS và HIDS

ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi

1. Từ phư ơ ng pháp có nghĩa là gì?
2. Bạn biết phư ơ ng pháp IDPS nào?
3. Bạn biết bao nhiêu phư ơ ng pháp IDPS? Họ là ai?
4. Các thuật ngữ: IDPS dựa trên chữ ký, IDPS dựa trên bắt thư ờng thống kê và IDPS phân tích giao thức trạng thái có nghĩa là gì trong ngôn ngữ của bạn?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Phư ơ ng pháp phát hiện IDPS

IDPS sử dụng nhiều phư ơ ng pháp phát hiện khác nhau để giám sát và đánh giá lưu lư ợng mạng. Ba phư ơ ng pháp chiếm ưu thế: phư ơ ng pháp dựa trên chữ ký, phư ơ ng pháp bắt thư ờng thống kê và phư ơ ng pháp kiểm tra gói trạng thái.

IDPS dựa trên chữ ký

IDPS dựa trên chữ ký (đôi khi được gọi là IDPS dựa trên kiến thức hoặc IDPS phát hiện sử dụng sai) kiểm tra lưu lư ợng mạng để tìm kiếm các mẫu khớp với các chữ ký đã biết-tức là các mẫu tấn công được định cấu hình trước, được định cấu hình trước. Công nghệ IDPS dựa trên chữ ký được sử dụng rộng rãi vì nhiều cuộc tấn công có chữ ký rõ ràng và khác biệt, ví dụ: (1) hoạt động in dấu chân và lấy dấu vân tay sử dụng ICMP, truy vấn DNS và phân tích định tuyến e-mail; (2) khai thác sử dụng một chuỗi tấn công cụ thể được thiết kế để lợi dụng lỗ hổng để giành quyền truy cập vào hệ thống; (3) Các cuộc tấn công DoS và DDoS, trong đó kẻ tấn công cố gắng ngăn chặn việc sử dụng bình thường của hệ thống, làm quá tải hệ thống với các yêu cầu khiến khả năng xử lý chúng một cách hiệu quả của hệ thống bị tổn hại hoặc gián đoạn.

Một vấn đề tiềm ẩn với cách tiếp cận dựa trên chữ ký là các chiến lư ợc tấn công mới phải liên tục được bổ sung vào cơ sở dữ liệu chữ ký của IDPS; nếu không, các cuộc tấn công sử dụng các chiến lư ợc mới sẽ không được công nhận và có thể thành công. Một điểm yếu khác của phư ơ ng pháp dựa trên chữ ký là một cuộc tấn công chậm, có phư ơ ng pháp có thể thoát khỏi sự phát hiện nếu chữ ký tấn công IDPS có liên quan có khung thời gian ngắn hơn. Cách duy nhất IDPS dựa trên chữ ký có thể giải quyết lỗ hổng này là thu thập và

phân tích dữ liệu trong khoảng thời gian dài hơn, một quy trình đòi hỏi khả năng lưu trữ dữ liệu lớn hơn đáng kể và khả năng xử lý bổ sung.

IDPS dựa trên bắt thư ờng thông kê

IDPS dựa trên sự bắt thư ờng thông kê (IDPS thống kê) hoặc IDPS dựa trên hành vi thu thập các bản tóm tắt thông kê bằng cách quan sát lưu lượn đư ợc biết là bình thư ờng. Khoảng thời gian đánh giá bình thư ờng này thiết lập một đư ờng cơ sở hiệu suất. Khi đư ờng cơ sở đư ợc thiết lập, thông kê IDPS định kỳ lấy mẫu hoạt động mạng và sử dụng các phư ơng pháp thống kê, so sánh hoạt động mạng đư ợc lấy mẫu với đư ờng cơ sở này. Khi hoạt động đư ợc đo nằm ngoài các tham số cơ sở-vư ợt quá mức đư ợc gọi là mức cắt –IDPS sẽ gửi cảnh báo cho quản trị viên. Dữ liệu cơ sở có thể bao gồm các biến như bộ nhớ máy chủ hoặc mức sử dụng CPU, loại gói mạng và số lưu lượng gói.

Ưu điểm của phư ơng pháp tiếp cận dựa trên sự bắt thư ờng thông kê là IDPS có thể phát hiện các kiểu tấn công mới, vì nó tìm kiếm hoạt động bắt thư ờng thuộc bất kỳ kiểu nào.

Thật không may, các hệ thống này yêu cầu nhiều chi phí hoạt động và năng lực xử lý hơn so với các IDPS dựa trên chữ ký, bởi vì chúng phải liên tục so sánh các mẫu hoạt động với đư ờng cơ sở. Một nhược điểm khác là các hệ thống này có thể không phát hiện những thay đổi nhỏ đối với các biến hệ thống và có thể tạo ra nhiều thông tin sai lệch. Nếu hành động của người dùng hoặc hệ thống trên mạng rất khác nhau, với các khoảng thời gian ít hoạt động xen kẽ với các khoảng thời gian có lưu lượng gói lớn, thì loại IDPS này có thể không phù hợp, vì sự thay đổi đột ngột từ cấp độ này sang cấp độ khác gần như chắc chắn sẽ tạo ra sai lệch. báo động. Do tính phức tạp và tác động của nó đối với tài điện toán chung của máy tính chủ cũng như số lưu lượng thông báo sai mà nó có thể tạo ra, nên loại IDPS này ít đư ợc sử dụng hơn loại dựa trên chữ ký.

Phân tích giao thức trạng thái IDPS

Theo SP 800-94, Phân tích giao thức trạng thái (SPA) là một quá trình so sánh các cấu hình đư ợc xác định trước của các định nghĩa đư ợc chấp nhận chung về hoạt động lành tính đối với từng trạng thái giao thức đối với các sự kiện đư ợc quan sát để xác định độ lệch.

Phân tích giao thức trạng thái dựa trên các cấu hình phổ quát do nhà cung cấp phát triển chỉ định cách sử dụng và không nên sử dụng các giao thức cụ thể." Về cơ bản, IDPS biết cách thức hoạt động của một giao thức, chẳng hạn như FTP, và do đó có thể phát hiện hành vi bắt thư ờng. Bằng cách lưu trữ dữ liệu có liên quan đư ợc phát hiện trong một phiên và sau đó sử dụng

dữ liệu đó để xác định các cuộc xâm nhập liên quan đến nhiều yêu cầu và phản hồi, IDPS có thể phát hiện các cuộc tấn công chuyên biệt, nhiều phiên tốt hơn. Quá trình này đôi khi được gọi là kiểm tra gói sâu vì SPA kiểm tra chặt chẽ các gói ở lớp ứng dụng để biết thông tin cho biết có thể có sự xâm nhập. Phân tích giao thức trạng thái cũng có thể kiểm tra các phiên xác thực để tìm hoạt động đáng ngờ cũng như các cuộc tấn công kết hợp "các chuỗi lệnh không mong muốn, chẳng hạn như phát đi phát lại cùng một lệnh hoặc phát lệnh mà không phát lệnh trước mà nó phụ thuộc, cũng như 'tính hợp lý' cho các lệnh chẳng hạn như độ dài tối thiểu và tối đa cho các đối số.

Các mô hình được sử dụng cho SPA tương tự như chữ ký ở chỗ chúng được cung cấp bởi các nhà cung cấp. Các mô hình này dựa trên các tiêu chuẩn giao thức ngành được thiết lập bởi các thực thể như Lực lượng đặc nhiệm kỹ thuật Internet, nhưng chúng khác nhau cùng với việc triển khai giao thức trong các tài liệu đó. Ngoài ra, các giao thức độc quyền không được xuất bản đầy đủ chi tiết để cho phép IDPS cung cấp các đánh giá chính xác và toàn diện.

Thật không may, sự phức tạp trong phân tích của các đánh giá dựa trên phiên là như điểm chính của loại phương pháp IDPS này, phương pháp này cũng yêu cầu chi phí xử lý lớn để theo dõi nhiều kết nối đồng thời. Ngoài ra, trừ khi một giao thức vi phạm hành vi cơ bản của nó, phương pháp IDPS này hoàn toàn có thể không phát hiện được sự xâm nhập. Một vấn đề cuối cùng là IDPS trên thực tế có thể can thiệp vào các hoạt động bình thường của giao thức mà nó đang kiểm tra, đặc biệt là với các hoạt động phân biệt giữa máy khách và máy chủ.

2.1. Trả lời các câu hỏi

1. Điểm yếu của cách tiếp cận dựa trên chữ ký là gì?
2. Như ợc điểm của phương pháp dựa trên sự bắt thư ờng thống kê là gì?
3. Tại sao IDPS dựa trên bắt thư ờng thống kê ít được sử dụng hơn so với loại dựa trên chữ ký?
4. Giải pháp cho những điểm yếu của cách tiếp cận dựa trên chữ ký là gì? --
5. Lợi ích của cách tiếp cận dựa trên sự bắt thư ờng thống kê là gì?
6. Tại sao công nghệ IDPS dựa trên chữ ký được sử dụng rộng rãi?
7. SPA là viết tắt của từ gì? Nó là gì?

8. Các mô hình sử dụng cho SPA dựa trên cơ sở nào?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Kiểm tra gói dựa trên chữ ký, sự bất thư ờng về thống kê và trạng thái là những cách tiếp cận nổi bật được IDPS sử dụng.

- A. Đúng B. Sai C. NI

2. Cách tiếp cận dựa trên bất thư ờng thống kê được sử dụng phổ biến hơn phuơng pháp dựa trên chữ ký.

- A. Đúng B. Sai C. NI

3. IDPS dựa trên chữ ký không bao giờ sai nên kẻ tấn công không thể làm gì với nó.

- A. Đúng B. Sai C. NI

4. IDPS có thể được triển khai thông qua một trong ba chiến lược kiểm soát cơ bản.

- A. Đúng B. Sai C. NI

5. Một trong những ưu điểm của IDPS Phân tích Giao thức Trạng thái là IDPS trên thực tế có thể can thiệp vào các hoạt động bình thường của giao thức mà nó đang kiểm tra, đặc biệt là với các hoạt động phân biệt giữa máy khách và máy chủ.

- A. Đúng B. Sai C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu và câu hỏi sau

1. Bởi dữ liệu liên quan được phát hiện trong một phiên và sau đó sử dụng dữ liệu đó để xác định các xâm nhập liên quan đến nhiều yêu cầu và phản hồi, IDPS có thể phát hiện tốt hơn các cuộc tấn công đa phiên, chuyên biệt.

- A. lưu trữ B. chuyển mạch
C. truyền D. chêbién

2. IDPS nào sau đây có thể không phù hợp nếu hành động của người dùng hoặc hệ thống trên mạng rất khác nhau, xen kẽ với các khoảng thời gian ít hoạt động với thời gian lưu lượng gói lớn?

- A. Phân tích giao thức trạng thái IDPS B. Chữ ký - IDPS dựa trên
C. IDPS dựa trên sự bất thư ờng về thống kê D. Không có câu nào đúng

3. IDPS đã sử dụng cách tiếp cận nào sau đây?

- A. Dựa trên chữ ký
- B. thống kê bắt thư ờng
- C. kiểm tra gói trạng thái
- D. Tất cả đều đúng

4. Đôi khi IDPS dựa trên tri thức có tên khác. Nó là

.....

- A. IDPS dựa trên chữ ký
- B. IDPS phát hiện sử dụng sai mục đích
- TAXI
- D. Không có câu nào đúng

5. IDPS dựa trên hành vi thu thập các bản tóm tắt thống kê theolưu lưu lượng truy cập đó được biết là bình thường.

- A. Theo dõi
- B. kiểm soát
- C. quan sát
- D. B & C đều đúng

3. Phát biểu:

1. Chọn một trong các phương pháp phát hiện IDPS trong văn bản và trình bày.
2. Trình bày các phương pháp phát hiện IDPS

ĐỌC VÀ NÓI 4

1. Thảo luận các câu hỏi

1. Bạn biết những công cụ bảo mật mạnh mẽ nào?
2. Từ độn ô có nghĩa là gì? Bạn biết gì về nó?
3. Từ honeypot nghĩa là gì? Bạn biết gì về nó?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Honeypots, Honeynets và hệ thống tέ bào đệm

Một nhóm các công cụ bảo mật mạnh vượt xa khả năng phát hiện xâm nhập thông thư ờng đư ợc biết đến với nhiều tên gọi khác nhau như honeypots, honeynets hoặc hệ thống tέ bào đệm. Để hiểu tại sao những công cụ này chưa đư ợc sử dụng rộng rãi, trước tiên bạn phải hiểu chúng khác nhau như thế nào từ một IDPS truyền thống.

Honeypots là hệ thống mồi nhử đư ợc thiết kế để dụ những kẻ tấn công tiềm năng ra khỏi các hệ thống quan trọng. Trong ngành, chúng còn đư ợc gọi là mồi nhử, mồi nhử và bẫy ruồi. Khi một tập hợp các honeypot kết nối một số hệ thống honeypot trên một mạng con, nó có thể đư ợc gọi là một honeynet. Hệ thống honeypot (hoặc trong trường hợp của honeynet là toàn bộ mạng con) chứa các dịch vụ giả mô phỏng các dịch vụ nổi tiếng, như ng đư ợc định cấu hình theo cách khiến nó trông dễ bị tấn công. Sự kết hợp này nhằm thu hút những kẻ tấn công tiềm năng thực hiện một cuộc tấn công, từ đó tiết lộ bản thân–y tư ờng là một khi các tổ chức đã phát hiện ra những kẻ tấn công này, họ có thể bảo vệ mạng của mình tốt hơn trước các cuộc tấn công trong tương lai nhằm vào tài sản thực. Tóm lại, honeypots đư ợc thiết kế để thực hiện những việc sau:

- Chuyển hướng kẻ tấn công khỏi các hệ thống quan trọng
- Thu thập thông tin về hoạt động của kẻ tấn công
- Khuyến khích kẻ tấn công ở lại hệ thống đủ lâu để

quản trị viên để ghi lại sự kiện và, có lẽ, trả lời.

Bởi vì thông tin trong honeypot đư ờng như có giá trị nên bất kỳ truy cập trái phép nào vào nó đều cấu thành hoạt động đáng ngờ. Honeypots đư ợc trang bị các màn hình nhạy cảm và bộ ghi sự kiện phát hiện các nỗ lực truy cập hệ thống và thu thập thông tin về các hoạt động của kẻ tấn công tiềm năng. Ảnh chụp màn hình từ một IDPS đơn giản chuyên về kỹ thuật honeypot, đư ợc gọi là Bộ công cụ lừa dối.

Ảnh chụp màn hình này hiển thị cấu hình của honeypot khi nó đang chờ một cuộc tấn công.

Ô đậm là một honeypot đã được bảo vệ để nó không thể dễ dàng bị xâm phạm—nói cách khác, một honeypot cứng. Ngoài việc thu hút những kẻ tấn công bằng dữ liệu hấp dẫn, một ô đậm hoạt động song song với IDPS truyền thống. Khi IDPS phát hiện những kẻ tấn công, nó sẽ liên tục chuyển chúng sang một môi trường mô phỏng đặc biệt, nơi chúng không thể gây hại—bản chất của môi trường máy chủ này là thứ mang lại cho phương pháp này cái tên “ô đậm”. Như trong honeypots, môi trường này có thể chứa đầy dữ liệu thú vị, có thể thuyết phục kẻ tấn công rằng cuộc tấn công đang diễn ra theo đúng kế hoạch. Giống như honeypots, các ô đậm được trang bị tốt và mang lại cơ hội duy nhất cho tổ chức mục tiêu theo dõi hành động của kẻ tấn công. Các nhà nghiên cứu IDPS đã sử dụng các hệ thống tέ bào đậm và honeypot từ cuối những năm 1980, nhưng cho đến gần đây không có phiên bản thương mại nào của các sản phẩm này. Những ưu điểm và nhược điểm của việc sử dụng phương pháp tiếp cận tέ bào đậm hoặc honeypot được tóm tắt dưới đây

Thuận lợi:

- Những kẻ tấn công có thể bị chuyển hướng đến những mục tiêu mà chúng không thể gây sát thương.
- Quản trị viên có thời gian để quyết định cách đối phó với kẻ tấn công
- Hành động của kẻ tấn công có thể được theo dõi dễ dàng và rộng rãi hơn, và hồ sơ có thể được sử dụng để tinh chỉnh các mô hình mối đe dọa và cải thiện hệ thống bảo vệ.
- Honeypots có thể hiệu quả trong việc bắt những kẻ nội gián đang rình mò xung quanh một mạng.

Nhược điểm:

- Ý nghĩa pháp lý của việc sử dụng các thiết bị như vậy không được hiểu rõ.
- Honeypots và các tέ bào đậm nói chung chưa được chứng minh là hữu ích các công nghệ bảo mật.
- Một kẻ tấn công lão luyện, một khi bị chuyển hướng vào hệ thống mới nhử, có thể trở nên tức giận và khởi động một cuộc tấn công mạnh mẽ hơn vào các hệ thống của tổ chức.
- Người quản trị và quản lý bảo mật cần có trình độ chuyên môn cao để sử dụng các hệ thống này.

Hệ thống Trap-and-Trace

Các ứng dụng trap-and-trace đang ngày càng phổ biến. Các hệ thống này sử dụng kết hợp các kỹ thuật để phát hiện sự xâm nhập và sau đó truy ngược lại nguồn gốc của nó.

Bẫy thư ờng bao gồm một hũ mật ong hoặc ô có đệm và một chuông báo động. Trong khi những kẻ xâm nhập bị phân tâm hoặc bị mắc kẹt bởi những gì chúng cho là xâm nhập thành công, hệ thống sẽ thông báo cho quản trị viên về sự hiện diện của chúng. Tính năng theo dõi là một phần mở rộng cho phương pháp tiếp cận tinh bão đệm hoặc honeypot. Theo dõi-tư duy tự như ID người gọi-là một quá trình mà tổ chức cố gắng xác định một thực thể được phát hiện trong các khu vực trái phép của mạng hoặc hệ thống. Nếu kẻ xâm nhập là một ngườiօi nào đó bên trong tổ chức, các quản trị viên hoàn toàn có quyền theo dõi cá nhân đó và giao ngườiօi đó cho các cơ quan nội bộ hoặc bên ngoài. Nếu kẻ xâm nhập nằm ngoài phạm vi bảo mật của tổ chức, thì sẽ nảy sinh nhiều vấn đề pháp lý.

Nhin bে ngoài, các hệ thống bẫy và theo dõi có vẻ như là một giải pháp lý tưởng. An ninh không còn giới hạn trong phòng thủ. Bây giờ quản trị viên an ninh có thể tiếp tục hành vi phạm tội. Họ có thể truy tìm thủ phạm và chuyển chúng cho các cơ quan có thẩm quyền thích hợp.

Dưới chiêu bài công lý, một số quản trị viên kém cẩn trọng hơn thậm chí có thể bị cảm dỗ tấn công ngườiօi hoặc xâm nhập vào hệ thống của tin tức để tìm hiểu càng nhiều càng tốt về tin tức.

Có nhiều hạn chế pháp lý hơn đối với bẫy và dấu vết. Phần bẫy thư ờng liên quan đến việc sử dụng honeypots hoặc honeynets. Khi sử dụng honeypots và honeynets, quản trị viên nên cẩn thận để không vướng qua ranh giới giữa dụ dỗ và

Cái bẫy. Lôi kéo là hành động thu hút sự chú ý đến một hệ thống bằng cách đặt thông tin hấp dẫn ở những vị trí quan trọng. Cạm bẫy là hành động dụ dỗ một cá nhân phạm tội để bị kết án. Sự dụ dỗ là hợp pháp và có đạo đức, trong khi sự gài bẫy thì không.

Chủ động phòng chống xâm nhập

Một số tổ chức muốn làm nhiều hơn là chỉ chờ đợi cuộc tấn công tiếp theo và thực hiện các biện pháp đối phó tích cực để ngăn chặn các cuộc tấn công. Một công cụ cung cấp khả năng ngăn chặn xâm nhập tích cực được gọi là LaBrea. LaBrea là một honeypot và IDPS "dính" và hoạt động bằng cách chiếm không gian địa chỉ IP không được sử dụng trong mạng. Khi LaBrea ghi nhận một yêu cầu ARP, nó sẽ kiểm tra xem địa chỉ IP được yêu cầu có thực sự hợp lệ trên mạng hay không. Nếu địa chỉ hiện không được sử dụng bởi một ngườiօi thực

máy tính hoặc thiết bị mạng, LaBrea giả vờ là một máy tính ở địa chỉ IP đó và cho phép kẻ tấn công hoàn thành yêu cầu kết nối TCP/IP, đư ợc gọi là bắt tay ba bứ ớc. Khi bắt tay hoàn tất, LaBrea thay đổi kích thước cửa sổ tru ợt TCP thành một số thấp để giữ kết nối TCP mở từ kẻ tấn công trong nhiều giờ, nhiều ngày hoặc thậm chí nhiều tháng. Giữ kết nối mở như ng không hoạt động sẽ làm chậm đáng kể các sâu dựa trên mạng và các cuộc tấn công khác. Nó cho phép hệ thống LaBrea có thời gian thông báo cho quản trị viên hệ thống và mạng về hành vi bất thường trên mạng.

2.1. Trả lời các câu hỏi

1. Hệ thống honeypot bao gồm những gì?
2. LaBrea là gì? Làm thế nào nó hoạt động?
3. Các nhà nghiên cứu của IDPS đã sử dụng hệ thống té bào đệm và honeypot trong bao lâu?
4. Quản trị viên nên làm gì khi sử dụng honeypots và honeynets?
5. Honeypots là gì? Chúng đư ợc thiết kế để làm gì?
6. Hệ thống nào sử dụng kết hợp các kỹ thuật để phát hiện xâm nhập và sau đó truy tìm nó trở lại nguồn của nó?
7. LaBrea làm gì khi ghi chú một yêu cầu ARP?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Ảnh chụp màn hình từ một IDPS đơn giản chuyên về kỹ thuật honeypot, đư ợc gọi là Bộ công cụ lừa dối.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Thu thập thông tin về hoạt động của kẻ tấn công là một trong những Mục đích của Honeypots.

A. Đúng	B. Sai	C. NI
---------	--------	-------
3. IDPS là một hệ thống phức tạp ở chỗ nó liên quan đến nhiều tác nhân giám sát từ xa yêu cầu cấu hình phù hợp để có đư ợc xác thực và ủy quyền phù hợp.

A. Đúng	B. Sai	C. NI
---------	--------	-------

4. Cả gài bẫy và dụ dỗ đều là hành động dụ dỗ một cá nhân phạm tội đến.

A. Đúng

B. Sai

C. NI

5. Khi thực hiện công việc của mình, hacker chưa bao giờ bị sập bẫy.

B. Đúng

B. Sai

C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và các câu lệnh

1. thông tin trong honeypot thường như có giá trị, bất kỳ truy cập trái phép nào vào thông tin đó đều cấu thành hoạt động đáng ngờ.

A. Tuy nhiên,

B. Mặc dù

C. Để

D. Vì

2. Ưu điểm của honeypot là gì?

A. Những kẻ tấn công có thể bị chuyển hướng đến các mục tiêu mà chúng không thể gây sát thương

B. Ý nghĩa pháp lý của việc sử dụng các thiết bị như vậy không được hiểu rõ

C. Quản trị viên và người quản lý bảo mật cần có trình độ chuyên môn cao để sử dụng các hệ thống này.

D. Không có câu nào đúng

3. kẻ xâm nhập nằm ngoài vành đai an ninh của tổ chức, nhiều vấn đề pháp lý phát sinh.

A. Nếu

B. Trừ khi

C. Khi nào

D. Trong khi

4. được trang bị các bộ theo dõi nhạy cảm và bộ ghi sự kiện để phát hiện các nỗ lực truy cập hệ thống và thu thập thông tin về các hoạt động của kẻ tấn công tiềm năng.

A. Tế bào đệm

B. Honeypots

C. Mồi nhử

D. B & C đều đúng

5. là một honeypot đã được bảo vệ để nó không thể dễ dàng bị xâm phạm.

A. mồi nhử

B. lọ mật ong

C. thu hút

D. tế bào đệm

3. Phát biểu:

1. Chọn một trong các công cụ bảo mật trong văn bản và trình bày nó.
2. Trình bày ưu u như ợc điểm của honeypots.

4. Lắng nghe

1. <https://www.youtube.com/watch?v=cMH4yGE73iQ&t=97s>
2. <https://www.youtube.com/watch?v=2baGjq10ZCY>
3. <https://www.youtube.com/watch?v=mmt4B60xSj0>
4. <https://www.youtube.com/watch?v=FihkG72z7MQ>

VIẾT VÀ NÓI

1. Viết khoảng 350-400 từ về một trong những chủ đề sau theo cách của riêng bạn từ ngữ:

- IDPS
- NIDS
- HIDS
- So sánh NIDS và HIDS

2. Trình bày các nội dung sau:

- IDPS
- NIDS
- HIDS
- So sánh NIDS và HIDS

BÀI 5: MẬT MẠI LÀ GÌ?

ĐỌC VÀ NÓI 1

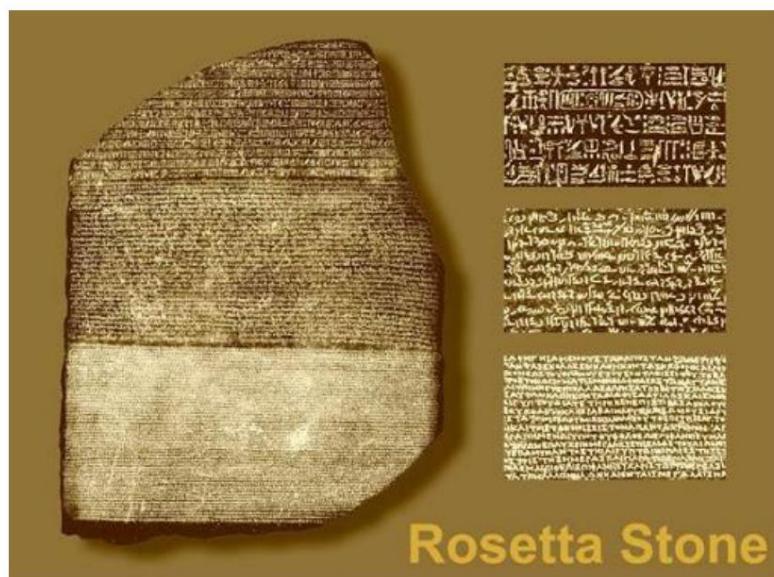
1. Thảo luận các câu hỏi

1. Bạn đã bao giờ nghe đến từ “cryptography” chưa? Nếu có, nó làm gì có nghĩa là trong ngôn ngữ của bạn?
2. Mật mã học liên quan đến những lĩnh vực nào?
3. Mật mã được áp dụng trong những lĩnh vực nào?
4. Mật mã học có những mục tiêu gì?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Mật mã là gì?

Từ “cryptography” có nguồn gốc từ tiếng Hy Lạp kryptos, nghĩa là ẩn, và graphien, nghĩa là viết. Các nhà sử học tin rằng chữ tượng hình Ai Cập, bắt đầu vào khoảng năm 1900 trước Công nguyên, là một ví dụ ban đầu về mã hóa. Chìa khóa mở ra bí mật về chữ tượng hình là Phiến đá Rosetta, được phát hiện vào năm 1799 ở vùng hạ Ai Cập và hiện nằm trong Bảo tàng Anh ở London. Francois Champollion, sử dụng Đá Rosetta, xem Hình 5-1, đã giải mã chữ tượng hình vào năm 1822. Mặc dù mật mã Ai Cập khá mang tính giai thoại, nhưng lịch sử bao gồm nhiều cách sử dụng mật mã khác. Giao tiếp với các mã bí mật thư ờng được yêu cầu cho quyền riêng tư ngoại giao, trong chiến tranh, cá nhân hoặc công ty.



Hình 5-1 Đá Rosetta

Mật mã học là nghiên cứu về các kỹ thuật toán học liên quan đến các khía cạnh của bảo mật thông tin như bảo mật, toàn vẹn dữ liệu, xác thực thực thể và xác thực nguồn gốc dữ liệu.

Thông tin có thể đọc đư ợc chư a đư ợc xử lý đư ợc gọi là văn bản gốc hoặc dữ liệu thuần túy. Quá trình làm cho thông tin không thể đọc đư ợc đư ợc gọi là mã hóa hoặc mã hóa. Kết quả của mã hóa là một bản mã hoặc mật mã. Đảo ngược quá trình này và truy xuất thông tin ban đầu có thể đọc đư ợc đư ợc gọi là giải mã hoặc giải mã. Để mã hóa hoặc giải mã thông tin, một thuật toán hay còn gọi là mật mã đư ợc sử dụng.

Cách thức hoạt động của một thuật toán mã hóa, đư ợc kiểm soát bởi một khóa bí mật, đôi khi đư ợc gọi là mật khẩu hoặc cụm mật khẩu (trên các máy mã hóa, khóa là cài đặt của máy). Chìa khóa chỉ đư ợc biết bởi những người đư ợc phép đọc thông tin. Nếu không biết khóa, sẽ không thể đảo ngược quá trình mã hóa hoặc thời gian để cố gắng đảo ngược quá trình sẽ cần

mất quá nhiều thời gian đến nỗi thông tin sẽ trở nên vô dụng.

Phân tích mật mã hoặc phân tích mật mã là nghiên cứu và phân tích các thuật toán mã hóa hoặc mật mã hiện có, (hoặc Phân tích mật mã là quá trình lấy thông điệp gốc (đư ợc gọi là bản rõ) từ một thông điệp đư ợc mã hóa (gọi là bản mã) mà không cần biết các thuật toán và khóa đư ợc sử dụng để thực hiện mã hóa) nhằm đánh giá chất lượng của chúng, tìm ra điểm yếu hoặc tìm cách đảo ngược quá trình mã hóa khi không có khóa. Giải mã mà không cần khóa (thường cũng không đư ợc phép) là một cuộc tấn công phân tích mật mã, đư ợc gọi là phá vỡ hoặc bẻ khóa mật mã.

Một cuộc tấn công phân tích mật mã có thể khai thác các điểm yếu trong chính thuật toán hoặc thiết bị mật mã, khai thác các quy trình triển khai của nó hoặc thử tất cả các khóa có thể (một cuộc tấn công vũ phu). Nói chung, có hai loại tấn công: Tấn công chỉ vào bản mã, trong đó nhà giải mã hoặc kẻ tấn công chỉ có quyền truy cập vào bản mã và tấn công vào bản rõ đã biết, trong đó nhà giải mã có quyền truy cập vào cả bản mã và bản rõ tương ứng của nó hoặc bản rõ giả định., để lấy khóa tương ứng.

Mật mã học bao gồm cả mật mã (tạo) và phân tích mật mã (phá vỡ).

Các biểu thức 'mã', 'mã hóa' và 'giải mã' thường đư ợc sử dụng trong mật mã. Tuy nhiên, mã là sự thay thế thông tin đơn giản bằng thông tin khác và không sử dụng thuật toán. Nói chung, đây là những cuốn sách hoặc bảng mã chuyển đổi một giá trị (chữ cái, từ hoặc cụm từ) thành giá trị khác (chữ cái

trình tự, giá trị số hoặc ký hiệu đặc biệt). Mặt khác, mật mã học sử dụng một thuật toán (thường là sự kết hợp của phân số, chuyển vị và thay thế) để thao tác thông tin. Mặc dù sai về mặt kỹ thuật, cụm từ 'mã hóa' thường được sử dụng để biểu thị mã hóa hoặc mã hóa và do đó, người ta nên xem xét ngữ cảnh sử dụng các cụm từ đó.

Một số sử dụng thuật ngữ mật mã và mật mã thay thế cho nhau bằng tiếng Anh, trong khi những thuật ngữ khác (bao gồm cả thực tiễn quân sự của Hoa Kỳ nói chung) sử dụng mật mã để chỉ cụ thể việc sử dụng và thực hành các kỹ thuật mật mã và mật mã để chỉ nghiên cứu kết hợp về mật mã và phân tích mật mã. Tiếng Anh linh hoạt hơn một số ngôn ngữ khác, trong đó mật mã học (được thực hiện bởi các nhà mật mã học) luôn được sử dụng theo nghĩa thứ hai ở trên. Trong Wikipedia tiếng Anh, thuật ngữ chung được sử dụng cho toàn bộ lĩnh vực này là mật mã học (được thực hiện bởi các nhà mật mã học). Việc nghiên cứu các đặc điểm của ngôn ngữ có một số ứng dụng trong mật mã (hoặc mật mã học), tức là dữ liệu tần số, tổ hợp chữ cái, mẫu phổ quát, v.v., được gọi là ngôn ngữ học mật mã.

Mục tiêu mật mã

Mật mã không phải là phưƠng tiện duy nhất để cung cấp bảo mật thông tin, mà là một tập hợp các kỹ thuật.

Bảo mật là một dịch vụ được sử dụng để giữ nội dung thông tin khỏi tất cả trừ những người được phép có nó. Bí mật là một thuật ngữ đồng nghĩa với bảo mật và quyền riêng tư. Có nhiều cách tiếp cận để cung cấp tính bảo mật, từ bảo vệ vật lý đến các thuật toán toán học khiến dữ liệu trở nên khó hiểu.

Toàn vẹn dữ liệu là một dịch vụ giải quyết việc thay đổi dữ liệu trái phép. Để đảm bảo tính toàn vẹn của dữ liệu, người ta phải có khả năng phát hiện thao tác dữ liệu của các bên trái phép. Thao tác dữ liệu bao gồm những thao tác như chèn, xóa, và thay thế.

Xác thực là một dịch vụ liên quan đến nhận dạng. Chức năng này áp dụng cho cả thực thể và thông tin. Hai bên tham gia giao tiếp nên xác định lẫn nhau. Thông tin được gửi qua một kênh phải được xác thực về nguồn gốc, ngày xuất xứ, nội dung dữ liệu, thời gian gửi, v.v. Vì những lý do này, khía cạnh mật mã này thường được chia thành hai loại chính: xác thực thực thể và xác thực nguồn gốc dữ liệu. Xác thực nguồn gốc dữ liệu hoàn toàn cung cấp tính toàn vẹn của dữ liệu (vì nếu một thông báo được sửa đổi, nguồn đã thay đổi).

Chóng thoái thác là một dịch vụ ngăn chặn một thực thể từ chối các cam kết hoặc hành động trục đó. Khi tranh chấp phát sinh do một thực thể phủ nhận rằng một số hành động nhất định đã được thực hiện, thì cần phải có một biện pháp để giải quyết tình huống. Ví dụ: một thực thể có thể cho phép thực thể khác mua tài sản và sau đó từ chối cấp phép đó. Một thủ tục liên quan đến một bên thứ ba đáng tin cậy là cần thiết để giải quyết tranh chấp.

Mục tiêu cơ bản của mật mã là giải quyết thỏa đáng bốn lĩnh vực này trong cả lý thuyết và thực hành. Mật mã học là về việc ngăn chặn và phát hiện gian lận và các hoạt động độc hại khác.

2.1. Trả lời các câu hỏi

1. Mật mã là gì? Cái này đư ợc dùng để làm gì?
2. Mật mã bắt nguồn từ đâu và có ý nghĩa gì?
3. Mật mã liên quan đến những khía cạnh nào của bảo mật thông tin?
4. Phân tích mật mã là gì?
5. Mã hóa là gì? Giải mã là gì?
6. Tại sao thám mĩ nghiên cứu và phân tích mật mã hoặc mã hóa hiện có thuật toán?
7. Mật mã học có bao nhiêu mục tiêu? Họ là ai?
8. Những lớp xác thực chính nào thư ờng đư ợc chia nhỏ? Tại sao lại như vậy chia nhỏ như vậy?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Phân tích mật mã là thuật ngữ đư ợc sử dụng để nghiên cứu các phương pháp để có đư ợc ý nghĩa của thông tin đư ợc mã hóa mà không cần truy cập vào khóa thư ờng đư ợc yêu cầu để làm như vậy.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Trong mật mã, hệ thống mật mã là một bộ các thuật toán mật mã cần thiết để triển khai một dịch vụ bảo mật cụ thể, phổ biến nhất là để đạt đư ợc tính bảo mật.

A. Đúng	B. Sai	C. NI
---------	--------	-------

3. Mã hóa là quá trình mã hóa thông tin, chuyển đổi dạng biểu diễn ban đầu của thông tin gọi là bản rõ thành dạng thay thế gọi là bản mã.

A. Đúng

B. Sai

C. NI

4. Không cần phải tìm mọi cách để giải quyết tình huống khi cả hai các bên có tranh chấp gay gắt.

A. Đúng

B. Sai

C. NI

5. Thuật ngữ "mã" và "mật mã" là giống nhau và chúng có thể thay đổi đư ợc.

A. Đúng

B. Sai

C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và các câu lệnh

1. Quy trình nào cần key?

A. mã hóa

B. giải mã

C. A & B đều đúng

D. khôi phục thông tin ban đầu

2. Những loại tấn công đư ợc đề cập trong văn bản?

A. Tấn công vũ phu

B. Tấn công chỉ vào bản mã

C. Đã biết - tấn công bản rõ

D. Tất cả những điều trên đều đúng

3. A là giải quyết thỏa đáng tính bảo mật, tính toàn vẹn của dữ liệu, xác thực và chống từ chối trong cả lý thuyết và thực hành.

A. mục tiêu cơ bản của mật mã

B. đối tượng chung của mật mã

C. mục tiêu cơ bản của mật mã học

D. đối tượng chung của thám mã

4. là một dịch vụ ngăn chặn một thực thể từ chối tru ớc đó cam kết hoặc hành động.

A. Chống thoái thác

B. Xác thực

C. Toàn vẹn dữ liệu

D. Bảo mật

5. Điều gì đư ợc coi là ví dụ ban đầu của mã hóa?

A. Đá Rosetta

B. Chữ tượng hình Ai Cập

C. Lư ỡi hái

D. Một cuốn sách mật mã

6.là một dịch vụ liên quan đến xác minh và nó áp dụng cho cả thực thể và chính thông tin.

A. Toàn vẹn dữ liệu

B. Chống chối bỏ

C. Xác thực

D. Bảo mật

7. Về mặt lý thuyết, cuộc tấn công nào sau đây có thể được sử dụng để cò găng giải mã bất kỳ dữ liệu được mã hóa?

A. Một cuộc tấn công vũ phu

B. tấn công từ điển

C. A & B đều đúng

D. Tấn công trung gian

8. Nghiên cứu phân tích hệ thống thông tin nhằm mục đích nghiên cứu những khía cạnh tiềm ẩn của hệ thống là nghiên cứu nào sau đây?

A. Mật mã

B. Mật mã học

C. Phân tích mật mã

D. A & B đúng

1. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?
2. Trình bày mật mã học và mục tiêu của nó.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi

1. Mật mã ra đời khi nào? Ai là người sử dụng nó đầu tiên?
2. Các dạng mật mã sớm nhất là gì?
3. Theo bạn, mật mã học đã trải qua những giai đoạn lịch sử nào?
4. Từ cryptographer có nghĩa là gì?
5. Bạn có biết hoặc đã từng nghe nói về nhà mật mã học nổi tiếng nào không? Nếu vâng, cung cấp một số thông tin để hỗ trợ câu trả lời của bạn.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Cơ sở của Mật mã học

1900 TCN Những người ghi chép Ai Cập đã sử dụng chữ tượng hình không chuẩn trong khi ghi các viên đất sét; đây là tài liệu đầu tiên sử dụng mật mã bằng văn bản.

Mật mã của người Lur Ông Hà vào năm 1500 trước Công nguyên đã vươn qua mật mã của người Ai Cập. Điều này được thể hiện qua một tấm bảng được phát hiện có chứa công thức mã hóa cho men gồm; máy tính bảng đã sử dụng các ký hiệu có ý nghĩa khác với khi được sử dụng trong các ngữ cảnh khác.

500 TCN Những người ghi chép tiếng Do Thái viết sách Jeremiah đã sử dụng một mật mã thay thế bảng chữ cái đảo ngược được gọi là ATBASH.

487 TCN Người Sparta của Hy Lạp đã phát triển scytale, một hệ thống bao gồm một dải giấy coi quấn quanh một cây gậy gỗ. Các tin nhắn được viết dài bằng cây truồng, và giấy coi được mở ra. Quá trình giải mã liên quan đến việc quấn giấy coi quanh một trục có đường kính tươn tự.

50 TCN Julius Caesar đã sử dụng một mật mã thay thế đơn giản để đảm bảo thông tin liên lạc của quân đội và chính phủ. Để tạo thành một văn bản được mã hóa, Caesar đã dịch chuyển chữ cái trong bảng chữ cái ba vị trí. Ngoài mật mã thay thế một bảng chữ cái này, Caesar đã tăng cường khả năng mã hóa của mình bằng cách thay thế các chữ cái Hy Lạp cho các chữ cái Latinh.

Thế kỷ thứ tư đến thứ sáu Kama Sutra của Vatsayana đã liệt kê mật mã là thứ 44 và 45 trong số 64 nghệ thuật (yoga) mà đàn ông và phụ nữ nên thực hành: (44)

Nghệ thuật hiểu cách viết bằng mật mã và cách viết các từ theo một cách đặc biệt; (45) Nghệ thuật nói bằng cách thay đổi hình thức của từ.

725 Abu 'Abd al-Rahman al-Khalil ibn Ahman ibn' Amr ibn Tammam al Farahidi al-Zadi al Yahmadi đã viết một cuốn sách (hiện đã thất lạc) về mật mã; ông cũng giải một mật mã Hy Lạp bằng cách đoán phần mở đầu của bản rõ.

855 Abu Wahshiyyaan-Nabati, một học giả, đã xuất bản một số bảng chữ cái mật mã đư ợc sử dụng để mã hóa các công thức ma thuật.

1250 Roger Bacon, một tu sĩ người Anh, đã viết Thư tín của Roger Bacon về Công trình Bí mật của Nghệ thuật và Tự nhiên và Ngoài ra về Tính vô hiệu của Phép thuật, trong đó ông mô tả một số mật mã đơn giản.

1392 The Equatorie of the Planetis, một văn bản đầu tiên có thể đư ợc viết bởi Geoffrey Chaucer, chứa một đoạn văn trong một mật mã thay thế đơn giản.

1412 Subhalasha, một bộ bách khoa toàn thư tiếng Ả Rập gồm 14 tập, có một phần về mật mã, bao gồm cả mật mã thay thế và chuyển vị, cũng như mật mã có nhiều thay thế, một kỹ thuật chưa từng đư ợc sử dụng trước đây.

1466 Leon Battista Alberti, cha đẻ của mật mã phuơng Tây, đã làm việc với sự thay thế đa bảng chữ cái và cũng phát minh ra một thiết bị dựa trên hai đĩa đồng tâm giúp đơn giản hóa việc sử dụng mật mã Caesar.

1518 Johannes Trithemius đã viết cuốn sách in đầu tiên về mật mã và phát minh ra mật mã ẩn, trong đó mỗi chữ cái đư ợc biểu diễn dưới dạng một từ đư ợc lấy từ một loạt các cột. Ông cũng mô tả một phuơng pháp mã hóa đa bảng chữ cái sử dụng định dạng thay thế hình chữ nhật hiện đang đư ợc sử dụng phổ biến. Ông đư ợc ghi nhận là người đã giới thiệu phuơng pháp thay đổi bảng chữ cái thay thế cho mỗi chữ cái khi nó đư ợc giải mã.

1553 Giovan Batista Belaso đưa ra ý tư ởng về cụm mật khẩu (password) như một chìa khóa để mã hóa; phuơng pháp mã hóa đa bảng chữ cái này đư ợc đặt tên sai cho một người khác, người sau này đã sử dụng kỹ thuật này và đư ợc gọi là "Mật mã Vigenère" ngày nay.

1563 Giovanni Battista Porta đã viết một văn bản phân loại về các phuơng pháp mã hóa, phân loại chúng thành chuyển vị, thay thế và thay thế ký hiệu.

1623 Ngài Francis Bacon đã mô tả một phuơng pháp mã hóa sử dụng một trong những cách sử dụng đầu tiên của kỹ thuật giấu tin; anh ấy đã mã hóa tin nhắn của mình bằng cách thay đổi một chút kiểu chữ của một văn bản ngẫu nhiên để mỗi chữ cái của mật mã đư ợc ẩn bên trong chữ.

Trên thực tế, mật mã đa bảng chữ cái đư ợc phát minh bởi ba đóng góp chính bao gồm Johannes Trithemius (1462-1516), Giovanni Battista Porta (1535-1615) và Blaise de Vigenere (1523-1596)

Những năm 1790 Thomas Jefferson đã tạo ra một mật mã bánh xe gồm 26 ký tự, mà ông đã sử dụng để liên lạc chính thức khi còn là đại sứ tại Pháp; khái niệm về mật mã bánh xe sẽ được phát minh lại vào năm 1854 và một lần nữa vào năm 1913.

1854 Charles Babbage phát minh lại mật mã bánh xe của Thomas Jefferson. Ông đã phát triển các kỹ thuật phân tích đa tần số.

1861-1865 Trong Nội chiến Hoa Kỳ, các lực lượng của Liên minh đã sử dụng phương pháp mã hóa thay thế dựa trên các từ cụ thể và Liên minh miền Nam đã sử dụng mật mã đa bảng chữ cái có giải pháp đã được xuất bản trước khi bắt đầu Nội chiến.

Vào cuối thế kỷ 19, các bức quan trọng đã được thực hiện trong sự phát triển của mật mã. Auguste Kerckhoff là một trong những người quan trọng nhất đã thay đổi mật mã học từ nghệ thuật hắc ám thành một ngành khoa học dựa trên toán học.

1914-1917 Trong Chiến tranh thế giới thứ nhất, người Đức, Anh và Pháp đã sử dụng một loạt mật mã chuyển vị và thay thế trong liên lạc vô tuyến trong suốt cuộc chiến. Tất cả các bên đã nỗ lực đáng kể để cò găng chặn và giải mã thông tin liên lạc, và do đó tạo ra khoa học về phân tích mật mã. Các nhà mật mã học người Anh đã phá vỡ Bức điện Zimmerman, trong đó người Đức đề nghị Mexico lãnh thổ Hoa Kỳ để đổi lấy sự hỗ trợ của Mexico. Việc giải mã này đã giúp đưa Hoa Kỳ vào cuộc chiến.

1917 William Frederick Friedman, cha đẻ của ngành phân tích mật mã Hoa Kỳ, và vợ ông, Elizabeth, được chính phủ Hoa Kỳ tuyển dụng làm nhà phân tích mật mã dân sự. Friedman sau đó đã thành lập một trung tâm phân tích mật mã ở Riverbank, Illinois.

1917 Gilbert S. Vernam, một nhân viên của AT&T, đã phát minh ra một máy mật mã đa bảng chữ cái sử dụng một khóa ngẫu nhiên không lặp lại. Anh ấy cũng đã phát minh ra mã hóa pad một lần cho Telex Traffic.

1919 Hugo Alexander Koch đã nộp bằng sáng chế ở Hà Lan cho một máy mật mã dựa trên cánh quạt; vào năm 1927, Koch đã giao quyền sáng chế cho Arthur Scherbius, người phát minh ra máy Enigma, một loại mật mã thay thế cơ học.

1927-1933 Trong thời gian Cấm, bọn tội phạm ở Hoa Kỳ bắt đầu sử dụng mật mã để bảo vệ tính riêng tư của các tin nhắn được sử dụng trong các hoạt động tội phạm.

Sự kiện năm 1937 Người Nhật đã phát triển cỗ máy Tím, dựa trên các nguyên tắc tương tự như của Enigma và sử dụng các rơ le cơ học từ hệ thống điện thoại để mã hóa các thông điệp ngoại giao. Vào cuối năm 1940, một nhóm do William Friedman đứng đầu đã phá được mã do cỗ máy này tạo ra và chế tạo một cỗ máy có thể nhanh chóng giải mã các mật mã của Purple.

1939 -1942 Đồng minh đã bí mật phá vỡ mật mã Enigma, chắc chắn rút ngắn Thế chiến II.

1942 Những người nói mật mã Navajo tham gia Thế chiến thứ hai; ngoài việc nói một ngôn ngữ không được biết đến bên ngoài một nhóm tư ngô đồng nhỏ ở Hoa Kỳ, người Navajos đã phát triển các từ mã cho các chủ đề và ý tưởng không tồn tại trong tiếng mẹ đẻ của họ.

1948 Claude Elwood Shannon đề xuất sử dụng tần suất và phân tích thống kê trong giải pháp mật mã thay thế. Chính Claude Elwood Shannon là người đặt nền móng cho mật mã học hiện đại và là cha đẻ của Lý thuyết thông tin.

1970 Tiến sĩ Horst Feistel lãnh đạo một nhóm nghiên cứu của IBM trong việc phát triển mật mã Lucifer. Một trong những mật mã khôi đầu tiên - quá trình mã hóa được thực hiện trên khối bit dữ liệu là mật mã Lucifer, do Feistel và Coppersmith thiết kế cho IBM và dựa trên cái được gọi là mạng Feistel. Nó là tiền thân của DES.

1976 Một thiết kế dựa trên Lucifer đã được Cơ quan An ninh Quốc gia Hoa Kỳ chọn làm Tiêu chuẩn Mã hóa Dữ liệu và được chấp nhận trên toàn thế giới.

1976 Whitefield Diffie và Martin Hellman đưa ra ý tưởng về mật mã khóa công khai trong đó các thuật toán dựa trên vấn đề phức tạp tính toán. Thuật toán Diffie-Hellman dựa trên bài toán logarit rời rạc. Một trong những đóng góp quan trọng nhất được cung cấp bởi mật mã khóa công khai là chữ ký số.

1977 Ronald Rivest, Adi Shamir và Leonard Adleman đã phát triển một mật mã khóa công khai thực tế cho cả chữ ký số và bảo mật; họ thuật toán mã hóa máy tính RSA ra đời. Họ đã phát minh ra thuật toán RSA dựa trên bài toán phân tích thừa số nguyên tố lớn. Do giải pháp của chúng cho vấn đề phân phối khóa bí mật, thuật toán Diffie-Hellman và RSA nằm trong số các thuật toán mật mã được sử dụng rộng rãi nhất trên thế giới.

1992 Thuật toán RSA ban đầu được xuất bản trong Truyền thông của ACM.

1991 Phil Zimmermann phát hành phiên bản đầu tiên của PGP (Pretty Good Privacy); PGP được phát hành dưới dạng phần mềm miễn phí và trở thành tiêu chuẩn toàn cầu cho các hệ thống mật mã công cộng. Tiêu chuẩn quốc tế đầu tiên về chữ ký số (ISO/IES 9796) đã được thông qua.

2000 Mật mã của Rijndael được chọn làm Tiêu chuẩn mã hóa nâng cao. AES là một tập hợp con của mật mã khôi Rijndael được phát triển bởi hai nhà mật mã học người Bỉ, Vincent Rijmen và Joan Daemen, những người đã gửi đề xuất tới NIST trong quá trình lựa chọn AES.

2.1. Trả lời các câu hỏi

1. Mật mã học đã thay đổi từ nghệ thuật hắc ám thành khoa học dựa trên toán học khi nào? Ai đã thay đổi nó?
2. Ai là cha đẻ của Lý thuyết thông tin?
3. Thiết bị nào đã được phát triển và sử dụng từ đầu đến giờ thế kỷ 20 để bảo vệ thông tin liên lạc thư ơng mại, ngoại giao và quân sự?
4. Ai đã phát minh ra máy Enigma và nó được phát minh khi nào?
5. Ai đã đưa ra ý tưởng về mật mã khóa công khai? Thuật toán của nó dựa trên cái gì? bài toán độ phức tạp tính toán.
6. Thiết bị nào được phát triển bởi người Sparta ở Hy Lạp? Khi là nó đã phát triển?
7. Leon Battista Alberti đã phát minh ra cái gì?
8. Thuật toán nào được sử dụng rộng rãi nhất trên thế giới trong tiền điện tử thuật toán?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Giovan Batista Belaso đã phát minh ra một thiết bị dựa trên hai đĩa đồng tâm đơ n giản hóa việc sử dụng mật mã Caesar.
A. Đúng B. Sai C. NI
2. Ý tưởng về mật mã khóa công khai thuộc về Ronald Rivest, Adi Shamir và Leonard Adleman.
A. Đúng B. Sai C. NI
3. Charles Babbage đã phát triển kỹ thuật phân tích đa tần số.
A. Đúng B. Sai C. NI
4. Leon Battista Alberti là một tác giả, nghệ sĩ theo chủ nghĩa nhân văn thời Phục hưng người Ý, kiến trúc sư, nhà thơ, linh mục, nhà ngôn ngữ học, triết gia và nhà mật mã học.
A. Đúng B. Sai C. NI
5. Vincent Rijmen và Joan Daemen, người đã gửi đề xuất cho NIST trong quá trình lựa chọn AES là người Bỉ.
A. Đúng B. Sai C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi sau

1. Ai đã phát minh ra mã hóa một lần cho Telex Traffic?

A. Hugo Alexander Koch

B. Gilbert S. Vernam

C. Tiết sĩ Horst Feistel

D. Bép cải Charles

2. Julius Caesar đã sử dụng mật mã nào để đảm bảo thông tin liên lạc của quân đội và chính phủ?

A. Mật mã thay thế đơn chữ cái Mật mã thay thế đơn giản BA

C. A & B sai

D. Mật mã chuyển vị

3. Một trong những đóng góp quan trọng nhất được cung cấp bởi khóa công khai là gì? mật mã?

A. Tâm điểm dùng một lần

B. Phân phối khóa

C. Phân tích tần số

D. Chữ ký điện tử

4. Mật mã Enigma bị phá khi nào? Ai đã phá vỡ nó?

A. Trong Thế chiến II/Người Nhật

B. Năm 1939 -1942/Đồng minh

C. Trong Thế chiến I/Người Mỹ

D. Vào năm 1942/Người Anh

5. Cái nào sau đây là một trong những mật mã khôi đầu tiên?

A. Mật mã Caesar

B. Mật mã bánh xe

C. Mật mã Lucifer

D. Mật mã Vigenère

6. Ai đã phá mật mã của Purple?

A. William Friedman

B. Gilbert S. Vernam

C. Horst Feistel

D. Phil Zimmermann

7. Những loại mật mã nào đã được sử dụng trong liên lạc vô tuyến trong Thế giới

Chiến tranh tối?

A. Mật mã chuyển vị

B. Mật mã thay thế

C. Mật mã bí ẩn

D. A & B đúng

8. Tại sao Hoa Kỳ quyết định tham gia Thế chiến thứ hai?

A. Bởi vì Zimmerman Telegram đã bị hỏng.

B. Vì cỗ máy Enigma bị hỏng.

C. Vì đã sử dụng máy Tím.

D. Bởi vì mật mã Lucifer đã được sử dụng.

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào?
2. Trình bày những mô hình lịch sử quan trọng của mật mã.
3. Chọn bốn người viết mật mã đại diện cho bốn lịch sử cụm từ trong văn bản và trình bày chúng.

ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi

1. Thuật ngữ từ có nghĩa là gì?
2. Thuật ngữ là gì?
3. Thuật ngữ mật mã là gì?
4. Bạn biết thuật ngữ mật mã nào của Việt Nam?
5. Bạn biết những thuật ngữ tiếng Anh nào về mật mã? họ làm gì tiếng Việt nghĩa là gì?

Một số thuật ngữ và khái niệm cơ bản

Miền mã hóa và tên miền mã hóa

- A biểu thị một tập hợp hữu hạn được gọi là bảng chữ cái định nghĩa. Ví dụ, $A = \{0, 1\}$, bảng chữ cái nhị phân, là bảng chữ cái định nghĩa thư ờng được sử dụng. Lưu ý rằng bất kỳ bảng chữ cái nào cũng có thể được mã hóa theo bảng chữ cái nhị phân. Ví dụ: vì có 32 chuỗi nhị phân có độ dài năm; mỗi chữ cái trong bảng chữ cái tiếng Anh có thể được gán một chuỗi nhị phân duy nhất có độ dài năm.

- M biểu thị một tập hợp được gọi là không gian tin nhắn. M bao gồm các chuỗi ký hiệu từ một bảng chữ cái của định nghĩa. Một phần tử của M được gọi là bản rõ hay đơn giản là bản rõ. Ví dụ, M có thể bao gồm các chuỗi nhị phân, văn bản tiếng Anh, mã máy tính, v.v.

- C biểu thị một tập hợp được gọi là không gian bản mã. C bao gồm các chuỗi ký hiệu từ bảng chữ cái định nghĩa, có thể khác với bảng chữ cái định nghĩa cho M. Một phần tử của C được gọi là bản mã.

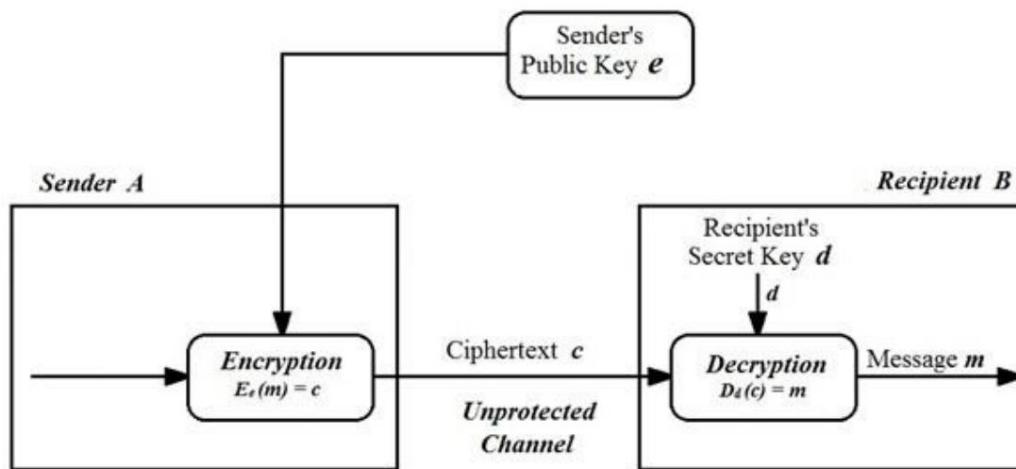
Chuyển đổi mã hóa và giải mã

- K biểu thị một tập hợp được gọi là không gian khóa. Phần tử của K được gọi là khóa.
 - Mỗi phần tử e $\in K$ xác định duy nhất một song ánh từ M đến C, ký hiệu là Ee được gọi là hàm mã hóa hay phép biến đổi mã hóa. Lưu ý rằng Ee phải là một song ánh nếu quy trình được đảo ngược và một thông điệp văn bản gốc duy nhất được phục hồi cho mỗi văn bản mã hóa riêng biệt.
 - Với mỗi d $\in K$, Dd biểu thị một song ánh từ C đến M (nghĩa là $Dd : C \rightarrow M$). dd là

gọi là hàm giải mã hay phép biến đổi giải mã.

- Quá trình áp dụng phép biến đổi E_e cho một thông điệp m . M thư ờng là đư ợc gọi là mã hóa m hoặc mã hóa m .
- Quá trình áp dụng phép biến đổi D_d thành bản mã c thư ờng là đư ợc gọi là giải mã c hoặc giải mã c.
- Một sơ đồ mã hóa bao gồm tập $\{E_e : e \in K\}$ mã hóa $K\}$ giải mã K các phép biến đổi và một tập hợp tương ứng $\{D_d : d \in K\}$ các phép biến đổi với thuộc tính mà đối với mỗi $e \in K$ có một khóa duy nhất d sao cho $D_d = E_e$ đôi khi ¹đủ_{để} $D_d(E_e(m)) = m$ với mọi $m \in M$. Một lưu ý sơ đồ mã hóa là

- Các khóa e và d trong định nghĩa trước đư ợc gọi là một cặp khóa và đôi khi đư ợc ký hiệu là (e, d) . Lưu ý rằng e và d có thể giống nhau.
- Để xây dựng một sơ đồ mã hóa cần chọn không gian bản tin M , không gian bản mã C , không gian khóa K , tập các phép biến đổi mã hóa $\{E_e : e \in K\}$ và tập các phép biến đổi giải mã tương ứng $\{D_d : d \in K\}$.



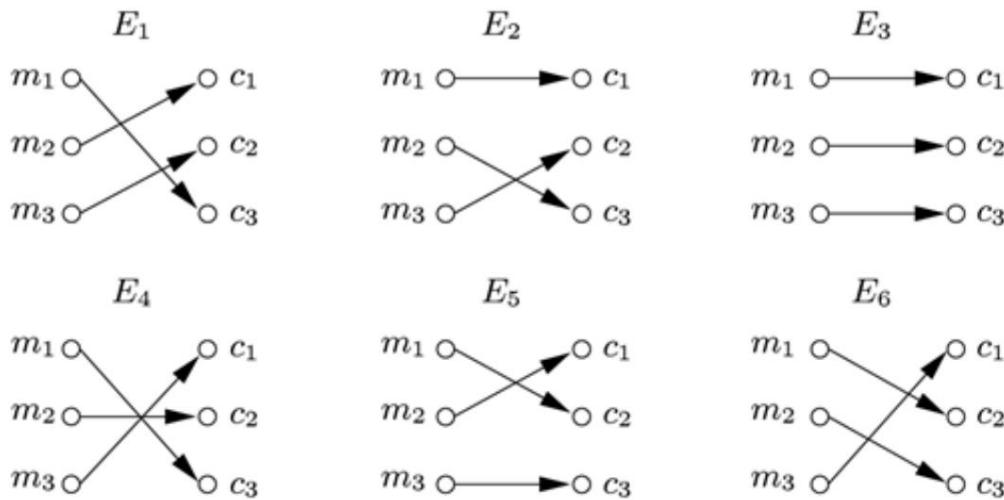
Hình 5-2. Ví dụ về lư ợc sơ đồ mã hóa

đạt đư ợc bí mật

Một sơ đồ mã hóa có thể đư ợc sử dụng như sau với mục đích đạt đư ợc tính bảo mật. Đầu tiên, hai bên Alice và Bob bí mật chọn hoặc bí mật trao đổi một cặp khóa (e, d). Tại một thời điểm tiếp theo, nếu Alice muốn gửi một tin nhắn $m \in M$ cho Bob, cô ấy tính $c = E_e(m)$ và truyền tin nhắn này cho Bob. Khi nhận đư ợc c , Bob tính toán $D_d(c) = m$ và do đó khôi phục đư ợc thông điệp ban đầu m .

Câu hỏi đặt ra là tại sao các khóa lại cần thiết. (Tại sao không chỉ chọn một chức năng mã hóa và chức năng giải mã tương ứng của nó?) Có các phép biến đổi, rất giống nhau như ngadget trung bởi các khóa có nghĩa là nếu một số phép biến đổi mã hóa/giải mã cụ thể được tiết lộ thì người ta không phải thiết kế lại toàn bộ sơ đồ mà chỉ cần thay đổi chìa khóa. Việc thay đổi khóa (chuyển đổi mã hóa/giải mã) thường xuyên là một thực hành mật mã hợp lý. Là một chất tư duy tự vật lý, hãy xem xét một khóa kết hợp có thể đặt lại thông thường. Cấu trúc của khóa có sẵn cho bất kỳ ai muốn mua như sự kết hợp do chủ sở hữu lựa chọn và thiết lập. Nếu chủ sở hữu nghi ngờ rằng sự kết hợp đã bị tiết lộ, anh ta có thể dễ dàng đặt lại nó mà không cần thay thế vật lý cơ chế.

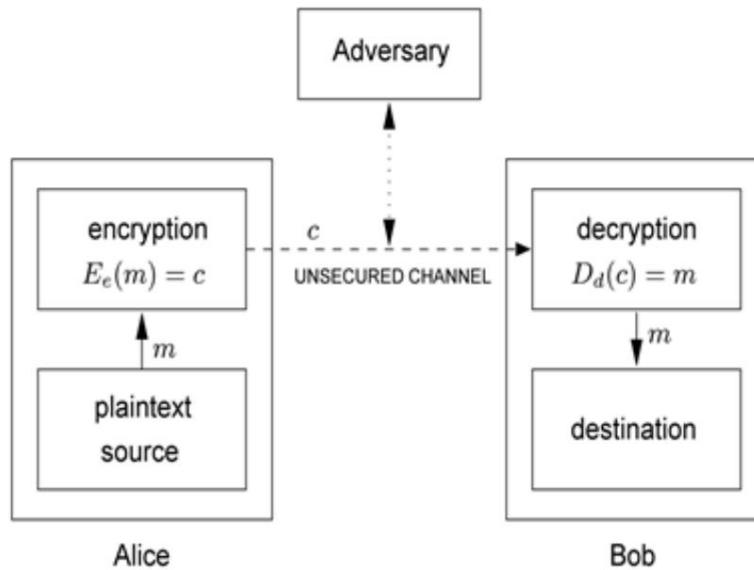
Ví dụ (sơ đồ mã hóa) Cho $M = \{m_1, m_2, m_3\}$ và $C = \{c_1, c_2, c_3\}$ và. Có chính xác $3! = 6$ phép loại từ M đến C . Không gian khóa $K = \{1, 2, 3, 4, 5, 6\}$ có sáu phần tử trong đó, mỗi phần tử xác định một trong các phép biến đổi. Hình 1 minh họa sáu chức năng mã hóa được ký hiệu là E_i , $1 \leq i \leq 6$. Alice và Bob đồng ý về một phép biến đổi, chẳng hạn như E_1 . Để mã hóa thông điệp m_1 , Alice tính $E_1(m_1) = c_3$ và gửi c_3 cho Bob. Bob giải mã c_3 bằng cách đảo ngược các mũi tên trên sơ đồ cho E_1 và quan sát rằng c_3 trở về m_1 .



Hình 5-3. Sơ đồ của một sơ đồ mã hóa đơn giản

Khi là một tập hợp nhỏ, sơ đồ chức năng là một phương tiện trực quan đơn giản để mô tả ánh xạ. Trong mật mã, tập hợp thường có tỷ lệ thiên văn và do đó, mô tả trực quan là không khả thi. Những gì được yêu cầu, trong những trường hợp này, là một số

các phư ơ ng tiện đơn giản khác để mô tả các phép biến đổi mã hóa và giải mã, chẳng hạn như các thuật toán toán học. **Hình 5.4** cung cấp một mô hình đơn giản về giao tiếp giữa hai bên sử dụng mã hóa.



Hình 5-4. Sơ đồ giao tiếp hai bên sử dụng mã hóa

2.1. Trả lời các câu hỏi

1. Chữ A, M, C, K biểu thị điều gì?
2. Những chữ cái nào biểu thị một cặp khóa?
3. Dđ gọi là gì?
4. Sơ đồ mã hóa bao gồm những gì?
5. Người ta phải làm gì để xây dựng sơ đồ mã hóa?
6. Người sở hữu khóa sẽ làm gì nếu anh ta nghi ngờ rằng tổ hợp đó có đư ợc tiết lộ?
7. Sơ đồ mã hóa đư ợc sử dụng như thế nào để đạt đư ợc tính bảo mật?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không thông tin (NI). Sửa lỗi sai (F)

1. Một chữ cái trong bảng chữ cái tiếng Anh có thể đư ợc gán các chuỗi nhị phân duy nhất của chiều dài năm.

A. Đúng

B. Sai

C. NI

2. Cấu trúc của khóa có sẵn cho bất cứ ai muốn mua một cái

như ng sự kết hợp đư ợc lựa chọn và thiết lập bởi chủ sở hữu.

A. Đúng

B. Sai

C. NI

3. M bao gồm các chuỗi ký hiệu từ bảng chữ cái nhị phân.

A. Đúng

B. Sai

C. NI

4. Có 23 xâu nhị phân độ dài 9

A. Đúng

B. Sai

C. NI

5. Sơ đồ giải mã bao gồm một tập {Ee : e K} giải mã phép biến hình.

A. Đúng

B. Sai

C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu sau

1. Một phần tử của M có tên là.....

A. một không gian bản mã

B. bản mã

C. sơ đồ giải mã

D. một thông báo rõ ràng hoặc đơn giản là một văn bản rõ ràng

2. Một phần tử của K được gọi là

A. bảng chữ cái định nghĩa

B. một chìa khóa

C. bản mã

D. bản rõ

3. Một phần tử của C có tên là

A. một không gian bản mã

B. sơ đồ giải mã

C. bản mã

D. một cặp khóa

4. Người ta phải nếu một số mã hóa hoặc giải mã cụ thể biến đổi đư ợc tiết lộ.

A. thay đổi chìa khóa

B. thiết kế lại toàn bộ sơ đồ

C. thay đổi chìa khóa

D. đặt lại chìa khóa

5. Cấu tạo của khóa..... như ng sự kết hợp đư ợc chọn và do chủ nhân đặt ra.

A. có sẵn cho bất cứ ai muốn mua một cái

B. không có sẵn cho bất cứ ai muốn mua một cái

C. A & B đúng

D. Tất cả những điều trên

6. Sơ đồ **hình 5-3**. Sơ đồ của một sơ đồ mã hóa đơn giản là

tốt cho việc mô tả sơ đồ mã hóa.....

A. khi tập hợp thư ờng có tỷ lệ thiên văn

B. Khi tập nhỏ

C. Khi nào là tập hợp nhỏ

D. B & C đều đúng

3. Nói

1. Đưa ra định nghĩa cho các thuật ngữ cơ bản của mật mã theo chữ.

2. Trình bày các nội dung sau:

- Lực đỡ mã hóa

- Làm thế nào để đạt được bí mật

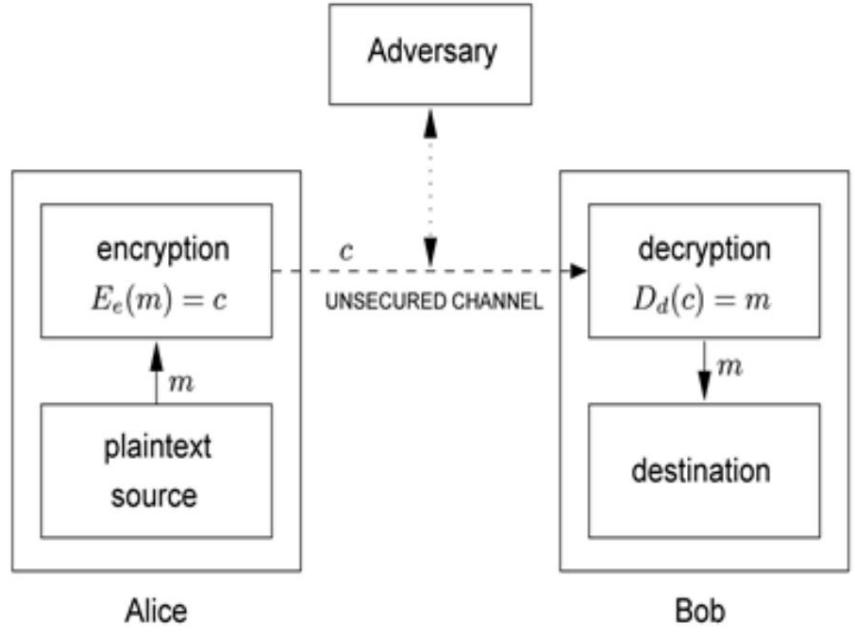
3. Mô tả **Hình 5-4**

ĐỌC VÀ NÓI 4

1. Thảo luận các câu hỏi

1. Bạn nghĩ thông thư ờng có bao nhiêu bên tham gia vào giao tiếp hai chiều?
Họ là ai?
2. Điều gì giúp họ truyền đạt thông tin cho nhau?
3. Bạn có nghĩ rằng thông tin được truyền qua một phương tiện giao tiếp kênh luôn an toàn? Tại sao và tại sao không?
4. Theo bạn, ai có thể đánh cắp thông tin đó và có những cách nào để ngăn chặn vấn đề này?

người tham gia truyền thông

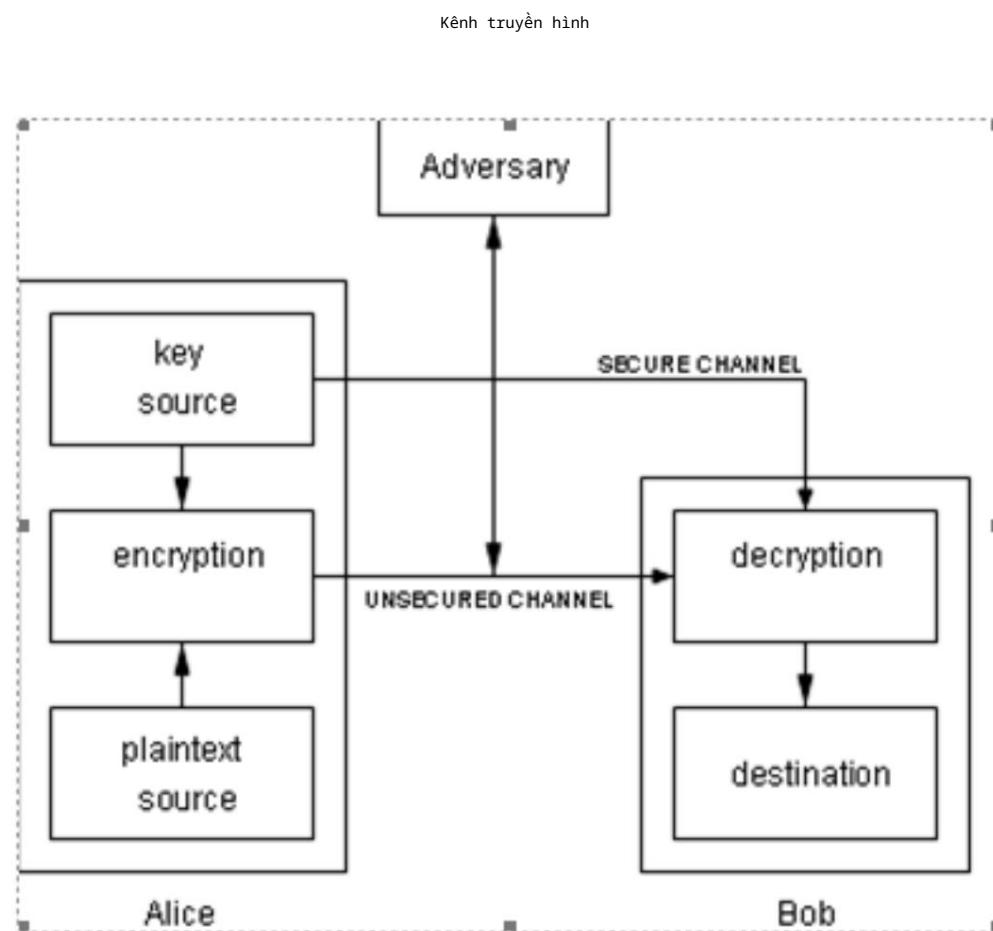


Hình 5-5. Sơ đồ giao tiếp hai bên sử dụng mã hóa

Tham khảo Hình 2, thuật ngữ sau đây được định nghĩa như sau:

- Một thực thể hoặc một bên là một ai đó hoặc một cái gì đó gửi, nhận hoặc thao tác thông tin. Alice và Bob là các thực thể trong Ví dụ ([xem hình 5-5](#)).
- Một thực thể có thể là một người, một thiết bị đầu cuối máy tính, v.v. • Người gửi là một thực thể trong giao tiếp hai bên hợp pháp máy phát thông tin. [Trong Hình 5-5](#), người gửi là Alice.
- Người nhận là một thực thể trong giao tiếp hai bên, là người nhận thông tin dự kiến. [Trong Hình 5-5](#), người nhận là Bob.

- Đối thủ là một thực thể trong giao tiếp hai bên không phải là người gửi cũng không phải người nhận và có gắng đánh bại dịch vụ bảo mật thông tin được cung cấp giữa người gửi và người nhận. Nhiều tên khác đồng nghĩa với kẻ thù như kẻ thù, kẻ tấn công, đối thủ, kẻ khai thác, kẻ nghe trộm, kẻ xâm nhập, kẻ xen vào và kẻ đánh chặn. Kẻ thù thường sẽ cố gắng đóng vai trò của người gửi hợp pháp hoặc người nhận hợp pháp.



Hình 5-6: Giao tiếp hai bên sử dụng mã hóa, với một kênh an toàn để trao đổi khóa. Khóa giải mã có thể được tính toán hiệu quả từ khóa mã hóa.

Tham khảo [Hình 5-6](#), thuật ngữ sau đây được định nghĩa như sau:

- Kênh là phương tiện chuyển tải thông tin từ thực thể này sang thực thể khác.
- Kênh an toàn vật lý hoặc kênh an toàn là kênh không vật lý có thể tiếp cận với đối thủ.
- Kênh không an toàn là kênh mà từ đó thông tin dự định có thể được sắp xếp lại, xóa, chèn hoặc đọc.
- Kênh được bảo mật là kênh mà đối thủ không có khả năng sắp xếp lại, xóa, chèn hoặc đọc.

Bảo vệ

- Tiền đề cơ bản trong mật mã là các tập M, C, K {Ee : e ∈ K}, {Dd : d ∈ K} là tri thức cõi giao tiếp về mật mã giao tiếp có thể là mã hóa mà đồ trang hoa, định và cặp khóa mà họ phải chọn. Người ta có thể đạt được bảo mật bổ sung bằng cách giữ bí mật lớp biến đổi mã hóa và giải mã như ngay người ta không nên đặt cơ sở bảo mật của toàn bộ lục ợc đồ trên phu ơng pháp này. Lịch sử đã chỉ ra rằng việc giữ bí mật về các phép biến hình thực sự rất khó khăn.

- Một số đồ mã hóa đư ợc cho là có thể phá đư ợc nếu một bên thứ ba, không biết trước ợc về cặp khóa (e, d), có thể khôi phục một cách có hệ thống văn bản rõ từ văn bản mật mã tư ơng ứng trong một khoảng thời gian thích hợp.

Một khung thời gian thích hợp sẽ là một chức năng của tuổi thọ hữu ích của dữ liệu đư ợc bảo vệ. Ví dụ, một chỉ thị mua một cổ phiếu nào đó có thể chỉ cần đư ợc giữ bí mật trong vài phút trong khi các bí mật quốc gia có thể cần đư ợc giữ bí mật vô thời hạn.

- Một lục ợc đồ mã hóa có thể bị phá vỡ bằng cách thử tất cả các khóa có thể để xem các bên giao tiếp đang sử dụng khóa nào (giả sử rằng lớp chức năng mã hóa là kiến thức công khai). Điều này đư ợc gọi là tìm kiếm toàn diện của không gian khóa. Sau đó, số lục ợng khóa (nghĩa là kích thước của không gian khóa) phải đủ lớn để làm cho phu ơng pháp này không khả thi về mặt tính toán. Mục tiêu của người thiết kế sơ đồ mã hóa là đây là cách tiếp cận tốt nhất để phá vỡ hệ thống.

Bảo mật thông tin nói chung

- Dịch vụ an toàn thông tin là phu ơng thức cung cấp một số khía cạnh cụ thể của Bảo vệ. Ví dụ: tính toàn vẹn của dữ liệu đư ợc truyền là mục tiêu bảo mật và một phu ơng pháp để đảm bảo khía cạnh này là dịch vụ bảo mật thông tin.

- Phá vỡ một dịch vụ bảo mật thông tin (thường liên quan đến nhiều hơn chỉ đơn giản là mã hóa) nguy ý đánh bại mục tiêu của dịch vụ dự định. • Đối thủ thụ động là đối thủ chỉ có khả năng đọc thông tin từ một kênh không an toàn.
- Đối thủ đang hoạt động là đối thủ cũng có thể truyền, thay đổi hoặc xóa thông tin trên một kênh không an toàn.

2.1. Trả lời các câu hỏi

1. Sự khác biệt giữa người gửi, người nhận và đối thủ là gì?

2. Thé nào là kenh bảo mật và kenh bảo mật?
3. Điều duy nhất mà hai bên giữ bí mật khi sử dụng sơ đồ mã hóa là gì?
4. Có thể phá vỡ sơ đồ mã hóa không? Khi nào và như thế nào?
5. Từ This trong đoạn văn cuối cùng đề cập đến điều gì?
6. Mục tiêu của người thiết kế sơ đồ mã hóa là gì?
7. Dịch vụ bảo mật thông tin là gì? Đưa ra vài ví dụ.
8. Sự khác biệt giữa một đối thủ chủ động và một đối thủ bị động là gì?
- đối thủ?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa lỗi sai (F)..)

1. Thuật ngữ kẻ thù có năm tên khác bao gồm kẻ thù, kẻ tấn công, đối thủ, kẻ khai thác và kẻ nghe lén.
A. Đúng B. Sai C. NI
2. Một khung thời gian thích hợp sẽ không bao giờ là một chức năng của tuổi thọ hữu ích của dữ liệu đang được bảo vệ.
A. Đúng B. Sai C. NI
3. Việc giữ bí mật các phép biến hình quả thực rất khó.
A. Đúng B. Sai C. NI
4. Có nhiều thuật ngữ khác nhau thay thế từ đối thủ có gắng đóng vai trò là người nhận hợp pháp hoặc người gửi hợp pháp.
A. Đúng B. Sai C. NI
5. Kênh không an toàn là kênh mà từ đó đối thủ không có quyền khả năng sắp xếp lại, xóa, chèn hoặc đọc.
A. Đúng B. Sai C. NI

2.3. Chọn đáp án đúng nhất để hoàn thành các câu hỏi sau và các câu lệnh

1. Đối phư ơng không truy cập được vào kênh nào?
A. Kênh an toàn vật lý hoặc kênh bảo mật

- B. Kênh không an toàn
- C. Một kênh bảo mật
- kênh an toàn DA
2. Đôi thủ có gắng đóng vai trò nào trong giao tiếp hai chiều?
- A. ngư ời gửi bất hợp pháp hoặc ngư ời nhận bất hợp pháp
- B. Chỉ đóng vai trò là ngư ời gửi
- C. ngư ời gửi hợp pháp hoặc ngư ời nhận hợp pháp
- D. Chỉ đóng vai trò máy thu
3. Tiền đề cơ bản trong mật mã học là gì?
- A. tập hợp A, C, K {Ee : e K}, {Dd : d K}
- B. các tập hợp M, C, K {Ee : e K}, {Dd : d K}
- C. A hoặc B
- D. Cả A và B
4. A/An là một thực thể trong giao dịch hai bên, là bên truyền thông tin hợp pháp.
- A. ngư ời gửi B. ngư ời nhận
- C. đối thủ D. kênh
5. A/An..... là một thực thể trong giao dịch hai bên là bên ngư ời nhận thông tin dự định.
- Kênh B. đối thủ
- C. ngư ời gửi D. ngư ời nhận
- 6..... là một dịch vụ bảo mật thông tin có nghĩa là đánh bại mục tiêu của dịch vụ dự kiến.
- A. Truyền B. Đánh bại
- C. Phá vỡ D. Vận chuyển
7. A/An là đối thủ chỉ có khả năng đọc thông tin từ một kênh không an toàn.
- A. đối thủ thụ động B. đối thủ tích cực
- C. thực thể D. bữa tiệc

8. A/An..... là phư ơ ng tiện truyền đạt thông tin từ đối tư ợng này sang đối tư ợng khác.

- | | |
|-----------------------|------------------------------|
| A. đối thủ | B. dịch vụ bảo mật thông tin |
| C. tìm kiếm toàn diện | D. kênh |

9. Mộtlà một đối thủ cũng có thẻ truyền, thay đổi hoặc xóa thông tin trên một kênh không an toàn.

- | | |
|---------------------|-------------|
| A. đối thủ thụ động | B. thực thẻ |
| C. đối thủ tích cực | D. bữa tiệc |

10.....là một phư ơ ng pháp cung cấp một số khía cạnh cụ thể của bảo mật.

- | | |
|-----------------------|------------------------------|
| Kênh | B. Dịch vụ bảo mật thông tin |
| C. tìm kiếm toàn diện | D. Bảo mật kênh |

3. Nói

1. Định nghĩa các thuật ngữ trong Hình 5-5 và Hình 5-6.
2. Trình bày các đối tư ợng và kênh truyền thông.
3. Mô tả hình 5-5 và hình 5-6.

4. Lắng nghe

1. <https://www.binance.vision/security/history-of-cryptography>
2. <https://www.youtube.com/watch?v=QqTWyl58Rvw>

VIẾT VÀ NÓI

1. Viết khoảng 350 -400 từ về một trong các chủ đề sau theo cách của bạn từ ngữ.

- Mật mã học
- Mục tiêu của mật mã
- Sơ lược về lịch sử mật mã

2. Trình bày các nội dung sau:

- Mật mã học
- Mục tiêu của mật mã
- Sơ lược về lịch sử mật mã

BÀI 6: MẬT MÃ HIỆN ĐẠI

ĐỌC VÀ NÓI 1

1. Thảo luận các câu hỏi

1. Mật mã hiện đại ra đời khi nào?
2. Bạn đã từng biết đến những nhà mật mã học nổi tiếng nào? Họ đáng chú ý là gì phân phối trong các lĩnh vực mật mã
3. Cụm từ hàm băm nghĩa là gì? Nó là gì?
4. Bạn biết những hàm băm nào?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

hàm băm

Mật mã hiện đại chủ yếu dựa trên lý thuyết toán học và thực hành khoa học máy tính; các thuật toán mật mã được thiết kế xung quanh các giả định về độ cứng tính toán, làm cho các thuật toán như vậy khó bị phá vỡ trong thực tế bởi bất kỳ đối thủ nào. Về mặt lý thuyết, có thể phá vỡ một hệ thống như vậy nhưng không thể làm như vậy bằng bất kỳ phương tiện thực tế nào đã biết. Do đó, các chương trình này được gọi là an toàn tính toán.

Cho đến nay, nhiều phương pháp mật mã đã được sử dụng như mật mã thay thế, mật mã chuyển vị, OR độc quyền, mật mã Vernam, mật mã sách hoặc chạy, và hàm băm. Tuy nhiên, trong phần này chỉ thảo luận về Hàm băm.

Các hàm băm là các thuật toán toán học tạo ra một bản tóm tắt hoặc thông báo tin nhắn (đôi khi được gọi là dấu vân tay) để xác nhận danh tính của một tin nhắn cụ thể và để xác nhận rằng không có bất kỳ thay đổi nào đối với nội dung. Mặc dù chúng không tạo ra bản mã, nhưng các hàm băm xác nhận danh tính và tính toàn vẹn của thông báo, cả hai đều là các chức năng quan trọng trong thương mại điện tử. Thuật toán băm là các hàm công khai tạo ra giá trị băm, còn được gọi là thông báo tóm tắt, bằng cách chuyển đổi các thông báo có độ dài thay đổi thành một giá trị có độ dài cố định. Thông báo tóm tắt là dấu vân tay của thông báo của tác giả được so sánh với hàm băm được tính cục bộ của người nhận của cùng một thông báo. Nếu cả hai giá trị băm giống hệt nhau sau khi truyền, thông báo đã đến mà không cần sửa đổi. Các hàm băm được coi là hoạt động một chiều trong đó cùng một thông báo luôn cung cấp cùng

giá trị băm, như ng bản thân giá trị băm không thể đư ợc sử dụng để xác định nội dung của thông điệp.

Hàm băm không yêu cầu sử dụng khóa, như ng có thẻ đính kèm mã xác thực thông báo (MAC)—một hàm băm một chiều, phụ thuộc vào khóa—chỉ cho phép những ngư ời nhận cụ thể (ngư ời nắm giữ khóa đôi xứng) truy cập thông báo tóm tắt . Vì các hàm băm là một chiều nên chúng đư ợc sử dụng trong các hệ thống xác minh mật khẩu để xác nhận danh tính của ngư ời dùng. Trong các hệ thống như vậy, giá trị băm hoặc thông báo tóm tắt đư ợc tính toán dựa trên mật khẩu đư ợc cấp ban đầu và thông báo thông báo này đư ợc lưu trữ để so sánh sau này. Khi ngư ời dùng đăng nhập cho phiên tiếp theo, hệ thống sẽ tính toán giá trị băm dựa trên đầu vào mật khẩu của ngư ời dùng và giá trị này đư ợc so sánh với giá trị đư ợc lưu trữ để xác nhận danh tính.

Tiêu chuẩn Hash an toàn (SHS) là một tiêu chuẩn do Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) ban hành. Tài liệu tiêu chuẩn FIPS 180-1 chỉ định SHA 1 (Thuật toán băm an toàn 1) là thuật toán an toàn để tính toán biểu diễn cô đọng của tệp tin hoặc dữ liệu. SHA-1 tạo ra thông báo tóm tắt 160 bit, có thẻ đư ợc sử dụng làm đầu vào cho thuật toán chữ ký số. SHA-1 dựa trên các nguyên tắc đư ợc mô hình hóa sau MD4 (là một phần của họ thuật toán băm MDx do Ronald Rivest tạo ra). Các thuật toán băm mới (SHA-256, SHA-384 và SHA 512) đã đư ợc NIST đề xuất làm tiêu chuẩn cho 128, 192 và 256 bit tương ứng. Số bit đư ợc sử dụng trong thuật toán băm là thước đo sức mạnh của thuật toán chống lại các cuộc tấn công xung đột. SHA-256 về cơ bản là thuật toán mật mã khối 256 bit tạo khóa bằng cách mã hóa giá trị băm trung gian, với khóa thông báo hoạt động như khóa. Chức năng nén hoạt động trên mỗi khóa thông báo 512 bit và thông báo trung gian 256 bit.

Một phương pháp tấn công gần đây có tên là bẻ khóa cầu vòng đã tạo ra mối lo ngại về sức mạnh của các quy trình đư ợc sử dụng để băm mật khẩu. Nói chung, nếu những kẻ tấn công giành đư ợc quyền truy cập vào một tệp mật khẩu băm, chúng có thẻ sử dụng kết hợp các cuộc tấn công từ điển và vũ phu để tiết lộ mật khẩu của ngư ời dùng. Mật khẩu là các từ trong từ điển hoặc đư ợc xây dựng kém có thể dễ dàng bị bẻ khóa. Các mật khẩu đư ợc xây dựng tốt mất nhiều thời gian để bẻ khóa ngay cả khi sử dụng các máy tính nhanh nhất, như ng bằng cách sử dụng bảng cầu vòng—cơ sở dữ liệu về các giá trị băm đư ợc tính toán trước từ các mật khẩu đư ợc tính toán tuần tự—công cụ bẻ khóa cầu vòng chỉ cần tra cứu mật khẩu đã băm và đọc phiên bản văn bản, không vũ phu cần thiết. Kiểu tấn công này đư ợc phân loại đúng hơ n là tấn công đánh đổi thời gian-bộ nhớ.

Để chống lại kiểu tấn công này, trước tiên bạn phải bảo vệ tệp mật khẩu đã băm và triển khai các giới hạn nghiêm ngặt đối với số lần thử được phép cho mỗi phiên đăng nhập. Bạn cũng có thể sử dụng một phương pháp gọi là muối băm mật khẩu. Salting là quá trình cung cấp một phần dữ liệu ngẫu nhiên, không bí mật cho hàm băm khi hàm băm được tính lần đầu tiên. Việc sử dụng giá trị muối tạo ra một hàm băm khác và khi một tập hợp lớn các giá trị muối được sử dụng, quá trình bẻ khóa câu vòng không thành công do sự đánh đổi bộ nhớ thời gian không còn có lợi cho kẻ tấn công. Giá trị muối không được giữ bí mật: nó được lưu trữ cùng với mã định danh tài khoản để có thể tạo lại giá trị băm trong quá trình xác thực.

Hàm băm mật mã là một hàm băm; nghĩa là, một thuật toán lấy một khối dữ liệu tùy ý và trả về một chuỗi bit có kích thước cố định, giá trị băm (mã hóa), sao cho bất kỳ thay đổi nào (vô tình hoặc cố ý) đối với dữ liệu sẽ thay đổi giá trị băm. Dữ liệu được mã hóa thường được gọi là "thông báo" và giá trị băm đôi khi được gọi là thông báo thông báo hoặc đơn giản là thông báo.

Hàm băm mật mã lý tưởng có bốn thuộc tính chính:

- Dễ dàng tính toán giá trị băm cho bất kỳ thông báo nào • Không thể tạo một thông báo có hàm băm nhất định • Không thể sửa đổi một thông báo mà không thay đổi hàm băm • Không thể tìm thấy hai thông báo khác nhau có cùng giá trị băm.

Các hàm băm mật mã có nhiều ứng dụng bảo mật thông tin, đáng chú ý là trong chữ ký số, mã xác thực thông báo (MAC) và các hình thức xác thực khác. Chúng cũng có thể được sử dụng như các hàm băm thông thường, để lập chỉ mục dữ liệu trong bảng băm, để lấy dấu vân tay, để phát hiện dữ liệu trùng lặp hoặc xác định duy nhất các tệp và dữ liệu dạng tổng kiểm tra để phát hiện hỏng dữ liệu ngẫu nhiên. Thật vậy, trong bối cảnh bảo mật thông tin, các giá trị băm mật mã đôi khi được gọi là dấu vân tay (kỹ thuật số), tổng kiểm tra hoặc chỉ giá trị băm, mặc dù tất cả các thuật ngữ này đại diện cho các hàm có các thuộc tính và mục đích khá khác nhau.

2.1. Trả lời các câu hỏi

1. Hàm băm là gì?
2. Tại sao các hàm băm được coi là hoạt động một chiều?
3. Bản tóm tắt thông điệp là gì?
4. Tại sao hàm băm được sử dụng rộng rãi trong thương mại điện tử?

5. SHS là viết tắt của từ gì? Nó là gì?
6. Thuật toán băm là gì?
7. Phép đo sức mạnh của thuật toán chống va chạm là gì

các cuộc tấn công?

8. Phư ơng pháp tấn công nào đã trở thành mối quan tâm về sức mạnh của các quy trình đư ợc sử dụng để băm mật khẩu?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa Sai (F)

1. Cho dù mật khẩu đư ợc xây dựng tốt đến đâu, chúng vẫn bị hỏng hoặc bị bẻ khóa thậm chí sử dụng máy tính nhanh nhất.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Vết nứt cầu vòng không bao giờ bị nứt nên nó đã trở thành mối lo ngại về sức mạnh của các quy trình đư ợc sử dụng để băm mật khẩu.

A. Đúng	B. Sai	C. NI
---------	--------	-------
3. Hàm băm tính toán giá trị băm dựa trên đầu vào mật khẩu của người dùng.

A. Đúng	B. Sai	C. NI
---------	--------	-------
4. Người dùng chỉ phải bảo vệ tệp mật khẩu băm và thực hiện giới hạn nghiêm ngặt đối với số lần thử đư ợc phép cho mỗi phiên đăng nhập để ngăn nứt cầu vòng.

A. Đúng	B. Sai	C. NI
---------	--------	-------
5. Không có các chương trình bảo mật thông tin về mặt lý thuyết

A. Đúng	B. Sai	C. NI
---------	--------	-------

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1. Tại sao các hàm băm đư ợc sử dụng trong các hệ thống xác minh mật khẩu để xác nhận danh tính của người dùng?

A. Vì hàm băm là thuật toán toán học.	B. Vì hàm băm là một chiều.	C. Vì hàm băm là hàm công bố.
---------------------------------------	-----------------------------	-------------------------------
- D. Vì hàm băm không yêu cầu sử dụng khóa.

2. Kẻ tấn công sẽ làm gì nếu họ có quyền truy cập vào tệp mật khẩu đư ợc băm?

- A. Họ có thể sử dụng kết hợp vũ lực
- B. Họ có thể sử dụng các cuộc tấn công từ điển để tiết lộ mật khẩu ngư ời dùng
- C. A & B đều đúng
- D. Chúng có thể tạo một bản tóm tắt hoặc thông báo về thông báo.

3. Ngư ời dùng phải làm gì để chống rạn nứt cầu vồng?

- A. Họ phải bảo vệ tệp mật khẩu băm
- B. Họ phải thực hiện các giới hạn nghiêm ngặt đối với số lần thử đư ợc phép cho mỗi phiên đăng nhập
- C. Họ phải sử dụng phư ơng pháp băm mật khẩu
- D. Tất cả đều đúng

4. Những mật khẩu nào đư ợc coi là dễ bị bẻ khóa?

- A. Mật khẩu là từ điển
- B. Mật khẩu đư ợc xây dựng kém
- C. Mật khẩu là từ điển và đư ợc xây dựng kém.
- D. Mật khẩu không đủ dài.

5. Bằng cách sử dụngcác cuộc tấn công để tiết lộ mật khẩu ngư ời dùng, kẻ tấn công có quyền truy cập vào một tập tin mật khẩu băm.

- A. sự kết hợp của vũ lực
- B. từ điển
- C. một bản rõ đã biết
- D. A & B đúng

6. Điều gì chỉ định SHA-1 là một thuật toán an toàn để tính toán một đại diện của một tin nhắn hoặc tập tin dữ liệu?

- A. Tài liệu tiêu chuẩn FIPS 180-2
- B. Viện Tiêu chuẩn và Công nghệ Quốc gia
- C. A & B đều đúng
- D. Tài liệu tiêu chuẩn FIPS 180-1

7. Ứng dụng nào trong an toàn thông tin thực hiện băm mật mã

chức năng mang lại?

- A. chữ ký số, mã xác thực thông điệp
- B. và các hình thức chứng thực khác.
- C. A & B đều đúng
- D. mã xác thực tin nhắn

8. Tính chất nào sau đây mà một hàm băm mật mã lý thuyết cần phải có?

- A. Dễ dàng tính toán giá trị băm cho bất kỳ thông báo nào
- B. Không thể tạo một thông báo có hàm băm nhất định và sửa đổi một tin nhắn mà không thay đổi hàm băm
- C. Không thể tìm thấy hai thông báo khác nhau có cùng hàm băm.
- D. Tất cả đều đúng

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?
2. Trình bày hàm băm

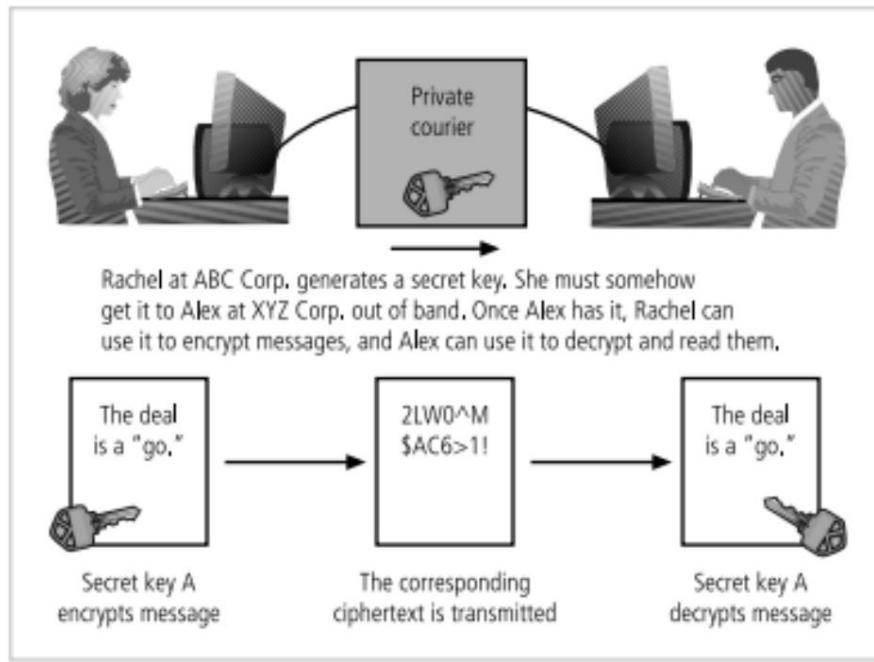
ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi

1. Từ đối xứng nghĩa là gì? Liệt kê một số từ đi với nó.
2. Cụm từ mã hóa đối xứng nghĩa là gì?
3. Bạn biết gì về mã hóa đối xứng?
4. Thuật toán nào thường được sử dụng trong mã hóa đối xứng?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Mã hóa đối xứng



Hình 6-1. Ví dụ về mã hóa đối xứng

Nói chung, các thuật toán mật mã thường được nhóm thành hai loại đối xứng và bất đối xứng—như ng trên thực tế, các hệ thống mật mã phổ biến ngày nay sử dụng kết hợp lai giữa các thuật toán đối xứng và bất đối xứng. Các thuật toán đối xứng và bất đối xứng thường được phân biệt bởi các loại khóa mà chúng sử dụng cho các hoạt động mã hóa và giải mã.

Mã hóa đối xứng

Các phương pháp mã hóa yêu cầu cùng một khóa bí mật để mã hóa và giải mã thông báo đang sử dụng cái được gọi là mã hóa khóa riêng hoặc mã hóa đối xứng. Phương pháp mã hóa đối xứng sử dụng toán học

các hoạt động có thể được lập trình thành các thuật toán điện toán cực nhanh để quá trình mã hóa và giải mã được thực hiện nhanh chóng bởi ngay cả các máy tính nhỏ. Như bạn có thể thấy trong **Hình 6-1**, một trong những thách thức là cả người gửi và người nhận đều phải có khóa bí mật. Ngoài ra, nếu một trong hai bản sao của khóa rơi vào tay kẻ xâm, tin nhắn có thể bị người khác giải mã và người gửi cũng như người nhận dự định có thể không biết tin nhắn đã bị chặn. Thách thức chính của mã hóa khóa đối xứng là lấy được khóa cho người nhận, một quá trình phải được thực hiện ngoài băng tần (có nghĩa là thông qua một kênh hoặc băng tần khác với kênh mang bản mã) để tránh bị chặn.

Có một số hệ thống mật mã mã hóa đối xứng phổ biến. Một trong những tiêu chuẩn được biết đến rộng rãi nhất là Tiêu chuẩn mã hóa dữ liệu (DES), do IBM phát triển và dựa trên thuật toán Lucifer của công ty, sử dụng độ dài khóa là 128 bit. Khi được triển khai, DES sử dụng kích thước khối 64 bit và khóa 56 bit. DES được NIST thông qua vào năm 1976 như một tiêu chuẩn liên bang để mã hóa thông tin không được phân loại, sau đó nó được sử dụng rộng rãi trong các ứng dụng thương mại. DES ngày càng phổ biến trong gần 20 năm, cho đến năm 1997, khi người dùng nhận ra rằng kích thước khóa 56 bit không cung cấp mức độ bảo mật chấp nhận được. Năm 1998, một nhóm có tên là Electronic Frontier Foundation (www.eff.org), sử dụng một máy tính được thiết kế đặc biệt, đã phá khóa DES trong vòng chưa đầy ba ngày (chính xác là hơn 56 giờ). Kể từ đó, người ta đưa ra giả thuyết rằng một cuộc tấn công chuyên dụng được hỗ trợ bởi phần cứng thích hợp (không nhất thiết phải là máy tính chuyên dụng) có thể phá khóa DES trong vòng chưa đầy bốn giờ. Triple DES (3DES) được tạo ra để cung cấp mức độ bảo mật vượt xa mức độ bảo mật của DES. 3DES là một ứng dụng nâng cao của DES và mặc dù nó đã thực hiện được lời hứa về sức mạnh mã hóa vượt xa DES, nhưng nó đã sớm tỏ ra quá yếu để tồn tại vô thời hạn—đặc biệt là khi sức mạnh tính toán tiếp tục tăng gấp đôi sau mỗi 18 tháng. Chỉ trong vài năm, 3DES cần phải được thay thế.

Người kế nhiệm 3DES là Tiêu chuẩn mã hóa nâng cao (AES). AES là một tiêu chuẩn xử lý thông tin liên bang (FIPS) chỉ định một thuật toán mật mã được sử dụng trong chính phủ Hoa Kỳ để bảo vệ thông tin trong các cơ quan liên bang không phải là một phần của cơ sở hạ tầng quốc phòng. (Các cơ quan được coi là một phần của quốc phòng sử dụng các phương pháp mã hóa khác, an toàn hơn do Cơ quan An ninh Quốc gia cung cấp.) Các yêu cầu đối với AES quy định rằng thuật toán phải không được phân loại, công khai

đư ợc tiết lộ và có sẵn miễn phí bản quyền trên toàn thế giới. AES đã đư ợc phát triển để thay thế cả DES và 3DES. Mặc dù 3DES vẫn là một thuật toán đư ợc phê duyệt cho một số mục đích sử dụng, như ng thời gian sử dụng hữu ích dự kiến của nó bị hạn chế. Trước đây, các tiêu chuẩn mật mã đư ợc FIPS phê duyệt đã đư ợc các tổ chức bên ngoài các tổ chức chính phủ áp dụng trên cơ sở tự nguyện. Quá trình lựa chọn AES liên quan đến sự hợp tác giữa chính phủ Hoa Kỳ, ngành công nghiệp tư nhân và học viện từ khắp nơi trên thế giới. AES đã đư ợc Bộ trưởng Thư ờng Thương mại phê duyệt là tiêu chuẩn chính thức của chính phủ liên bang vào ngày 26 tháng 5 năm 2002.

AES triển khai một mật mã khóa đư ợc gọi là Mật mã khóa Rijndael với độ dài khóa thay đổi và độ dài khóa là 128, 192 hoặc 256 bit. Các chuyên gia ước tính rằng máy tính đặc biệt đư ợc Electronic Frontier Foundation sử dụng để bẻ khóa DES trong vòng vài ngày sẽ cần khoảng 4.698.864 triệu tỷ năm ($4.698.864.000.000.000.000.000$) để bẻ khóa AES.

2.1. Trả lời các câu hỏi

1. Thách thức chính của mã hóa khóa đối xứng là gì?
2. Hệ mật mã hóa đối xứng nào phổ biến nhất đư ợc sử dụng? Cung cấp một số thông tin về họ.
3. Thế nào gọi là mã hóa đối xứng?
4. Khóa DES bị hỏng khi nào và ai là người đã phá?
5. Tại sao các phương pháp mã hóa đối xứng sử dụng các phép toán có thể đư ợc lập trình thành các thuật toán tính toán cực nhanh?
6. Như ợc điểm của phương pháp mã hóa đối xứng là gì?
7. Tại sao Advanced Encryption Standard ra đời?
8. Sự khác biệt giữa DES và AES là gì?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa Sai (F)

1. 3DES có mức độ bảo mật cao hơn DES.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Bộ trưởng Thư ờng Thương mại đã phê duyệt AES là tiêu chuẩn chính thức của chính phủ liên bang vào cuối tháng 5 năm 2002.

A. Đúng

B. Sai

C. NI

3. Phư ơ ng pháp mã hóa đối xứng không có nhú ợc điểm và nó đã bị kiện vì một thời gian dài.

A. Đúng

B. Sai

C. NI

4. Chỉ có chính phủ Hoa Kỳ chọn AES làm chính phủ liên bang Tiêu chuẩn.

A. Đúng

B. Sai

C. NI

5. AES dựa trên mật mã Rijndael đư ợc phát triển bởi hai nhà mật mã ngư ời Nga.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu sau

1. Tiêu chuẩn mã hóa dữ liệu dựa trên cái gì?

A. Mật mã Rijndael

B. Thuật toán Lucifer

C. độ cứng tính toán

D. Không có câu nào đúng

2. Các yêu cầu đối với AES quy định rằng thuật toán phải

A. không đư ợc phân loại

B. đư ợc tiết lộ công khai.

C. miễn phí bản quyền trên toàn thế giới D. Tất cả đều đúng

3. Tiêu chuẩn mã hóa dữ liệu đư ợc phát hiện là không an toàn khi nào?

A. Năm 1976

B. Năm 1998

C. Năm 1997

D. Năm 2002

4. Cơ quan nào sau đây ở Hoa Kỳ đư ợc phép sử dụng AES để bảo vệ thông tin?

A. Cơ quan đư ợc coi là một bộ phận của quốc phòng.

B. Cơ quan không thuộc cơ sở hạ tầng quốc phòng.

C. A & B đúng

D. Các cơ quan đư ợc coi là một phần của cảnh sát quốc gia.

5. Cái nào sau đây có mức độ bảo mật cao nhất?

MỘT.DES

B. Bộ ba DES

C.AES

D. RSA

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?
2. Trình bày các nội dung sau:
 - Mã hóa đối xứng
 - DES, 3DES, AES

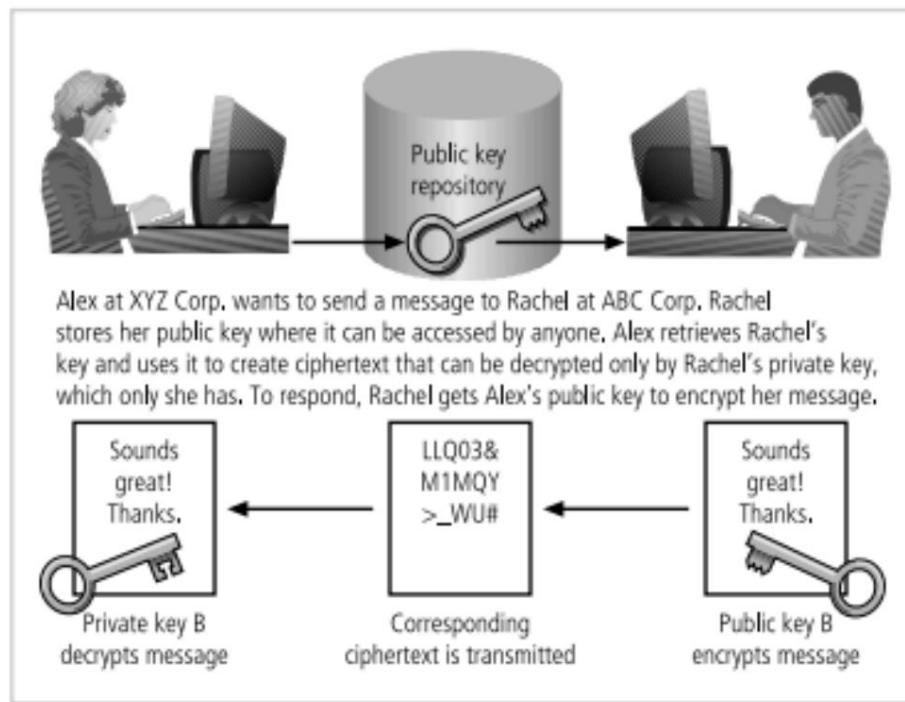
ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi

1. Từ bắt đầu xứng có nghĩa là gì? Những từ nào đi với nó?
2. Mã hóa bắt đầu xứng là gì? Bạn biết gì về nó?
3. Bạn đã bao giờ nghe "RSA" và bẫy cửa chua? Nếu có, vậy chúng là gì?
4. Cho biết một số thông tin về RSA.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Mã hóa bắt đầu xứng



Hình 6-2. Ví dụ về mã hóa bắt đầu xứng

Trong khi các hệ thống mã hóa đối xứng sử dụng một khóa duy nhất để mã hóa và giải mã một tin nhắn, mã hóa bắt đầu xứng sử dụng hai khóa khác nhau như ng có liên quan với nhau và một trong hai khóa có thể đư ợc sử dụng để mã hóa hoặc giải mã tin nhắn. Tuy nhiên, nếu khóa A đư ợc sử dụng để mã hóa tin nhắn thì chỉ có khóa B mới có thể giải mã đư ợc và nếu khóa B đư ợc sử dụng để mã hóa tin nhắn thì chỉ có khóa A mới có thể giải mã đư ợc. Mã hóa bắt đầu xứng có thể đư ợc sử dụng để cung cấp các giải pháp tinh tế cho các vấn đề về bảo mật và xác minh. Kỹ thuật này có giá trị cao nhất khi một khóa đư ợc sử dụng làm khóa riêng, nghĩa là nó đư ợc giữ

bí mật (giống như khóa trong mã hóa đối xứng), chỉ chủ sở hữu của cặp khóa mới biết và khóa còn lại đóng vai trò là khóa chung, nghĩa là nó được lưu trữ ở vị trí công khai mà bất kỳ ai cũng có thể sử dụng. Đây là lý do tại sao tên phổ biến hơn cho mã hóa bắt đối xứng là mã hóa khóa công khai.

Xem xét ví dụ sau, **đư ợc minh họa trong Hình 6-2**. Alex tại XYZ Corporation muốn gửi một tin nhắn đư ợc mã hóa tới Rachel tại ABC Corporation.

Alex đến cơ quan đăng ký khóa công khai và lấy đư ợc khóa công khai của Rachel. Hãy nhớ rằng nền tảng của mã hóa bắt đối xứng là không thể sử dụng cùng một khóa để mã hóa và giải mã cùng một thông điệp. Vì vậy, khi khóa chung của Rachel đư ợc sử dụng để mã hóa tin nhắn, thì chỉ có khóa riêng của Rachel mới có thể đư ợc sử dụng để giải mã tin nhắn và khóa riêng đó do một mình Rachel nắm giữ. Từ ơ ng tự như vậy, nếu Rachel muốn trả lời tin nhắn của Alex, cô ấy sẽ đến số đăng ký nơi i khóa công khai của Alex đư ợc giữ và sử dụng nó để mã hóa tin nhắn của mình, tất nhiên khóa này chỉ có thể đọc đư ợc bằng khóa riêng của Alex. Cách tiếp cận này, giúp giữ bí mật các khóa riêng và khuyến khích chia sẻ các khóa chung trong các thư mục đáng tin cậy, là một giải pháp tinh tế cho các vấn đề quản lý khóa của các ứng dụng khóa đối xứng.

Các thuật toán bắt đối xứng là các hàm một chiều. Hàm một chiều rất đơn giản để tính toán theo một hư ớng, như ng phức tạp để tính toán theo hư ớng ngược lại. Đây là nền tảng của mã hóa khóa công khai. Mã hóa khóa công khai dựa trên giá trị băm, như bạn đã học trước đó trong chương này, đư ợc tính toán từ một số đầu vào bằng thuật toán băm. Giá trị băm này về cơ bản là một bản tóm tắt các giá trị đầu vào ban đầu. Hầu như không thể lấy đư ợc các giá trị ban đầu nếu không biết các giá trị đó đư ợc sử dụng như thế nào để tạo ra giá trị băm. Ví dụ: nếu bạn nhân 45 với 235, bạn sẽ nhận đư ợc 10,575. Điều này là đủ đơn giản. Như ng nếu bạn chỉ đư ợc cho số 10,575, bạn có thể xác định hai số nào đã đư ợc nhân với nhau để xác định số này không? Nay giờ, giả sử rằng mỗi số nhân có 200 chữ số và là số nguyên tố. Tích của phép nhân thu đư ợc sẽ dài tới 400 chữ số.

Hãy tư ờng tư ợng thời gian bạn cần để tính toán điều đó.

Tuy nhiên, có một lối tắt. Trong toán học, nó đư ợc gọi là cửa sập (khác với cửa sập phần mềm). Cửa bẫy toán học là một "cơ chế bí mật cho phép bạn dễ dàng thực hiện hàm đảo ngược trong hàm một chiều". Với một cửa sập, bạn có thể sử dụng một khóa để mã hóa hoặc giải mã bản mã, như ng không thể sử dụng cả hai, do đó cần có hai khóa. Khóa chung trở thành khóa thực và khóa riêng đư ợc lấy từ khóa chung bằng cách sử dụng cửa sập.

Một trong những hệ thống mật mã khóa công khai phổ biến nhất là RSA, có tên bắt nguồn từ Rivest-Shamir-Adleman, nhà phát triển thuật toán. Thuật toán RSA là thuật toán mã hóa khóa công khai đầu tiên được phát triển (năm 1977) và được xuất bản cho mục đích thương mại. Nó rất phổ biến và đã được nhúng trong cả trình duyệt Web của Microsoft và Netscape để cho phép chúng cung cấp bảo mật cho các ứng dụng thư thương mại điện tử. Thuật toán RSA được cấp bằng sáng chế trên thực tế đã trở thành tiêu chuẩn trên thực tế cho các ứng dụng mã hóa sử dụng công cộng. Để tìm hiểu cách thức hoạt động của thuật toán này, hãy xem hộp Chi tiết kỹ thuật có tiêu đề "Thuật toán RSA". Vấn đề với mã hóa bắt đôi xứng, như đã chỉ ra trước đó trong ví dụ ở Hình 8-6, là việc tổ chức một cuộc hội thoại duy nhất giữa hai bên yêu cầu bốn khóa. Hơn nữa, nếu bốn tổ chức muốn trao đổi thông tin liên lạc, mỗi bên phải quản lý khóa riêng và bốn khóa chung của mình. Trong những tình huống như vậy, việc xác định khóa công khai nào là cần thiết để mã hóa một thông báo cụ thể có thể trở thành một vấn đề khá khó hiểu và với nhiều tổ chức hơn trong vòng lặp, vấn đề sẽ mở rộng. Đây là lý do tại sao mã hóa bắt đôi xứng đôi khi được các chuyên gia coi là không hiệu quả. So với mã hóa đối xứng, mã hóa bắt đôi xứng cũng không hiệu quả về mặt tính toán CPU. Do đó, các hệ thống kết hợp, chẳng hạn như các hệ thống được mô tả trong phần của chương này có tiêu đề "Cơ sở hạ tầng khóa công khai (PKI)," được sử dụng phổ biến hơn các hệ thống bắt đôi xứng thuận túy.

2.1. Trả lời các câu hỏi

1. Mã hóa bắt đôi xứng là gì?
2. Hệ thống mật mã hóa đối xứng nào là một trong những hệ thống phổ biến nhất hệ thống mật mã khóa công khai?
3. Nền tảng của mã hóa khóa công khai là gì?
4. Giá trị cao nhất của mã hóa bắt đôi xứng là bao nhiêu khi một khóa được sử dụng làm khóa riêng?
5. Cửa sổ toán học là gì?
6. Mã hóa khóa công khai dựa trên cái gì?
7. Người dùng có thể làm gì và không thể làm gì với cửa sổ?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không thông tin (NI). Sửa Sai (F)

1. Ưu điểm lớn của mật mã khóa riêng là bất kỳ hai bên nào ở bất kỳ đâu có phần mềm khóa riêng đều có thể trao đổi tin nhắn một cách an toàn mà không cần phải thực hiện bất kỳ thỏa thuận nào trước.

- A. Đúng B. Sai C. NI

2. Với một cửa sổ, việc mã hóa và giải mã được thực hiện bằng cách sử dụng cùng một khóa.

- A. Đúng B. Sai C. NI

3. Mã hóa bắt đối xứng còn được gọi là mã hóa khóa công khai vì một cặp khóa, một khóa được lưu trữ ở nơi công cộng mà ai cũng có thể sử dụng được.

- A. Đúng B. Sai C. NI

4. Những người đang sử dụng mật mã khóa công khai phải chuyển sang 150 chữ số hoặc số nguyên tố 200 chữ số nếu họ muốn bảo mật.

- A. Đúng B. Sai C. NI

5. Phuơng pháp mã hóa đối xứng không tốt bằng phuơng pháp mã hóa bắt đối xứng nên không có phuơng pháp nào thay thế được.

- A. Đúng B. Sai C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1. Ai đã phát triển thuật toán RSA?

- A. Ron Rivest B. Adi Shamir
C. Leonard Adleman D. Tất cả đều đúng

2. Như ợc điểm của RSA là gì?

- A. Tổ chức một cuộc trò chuyện duy nhất giữa hai bên yêu cầu bốn phím.
B. Phân phối khóa
C. Tổ chức một cuộc hội thoại giữa hai bên cần có hai cặp
của các phím.
D. A&C đều đúng

3. Bốn tổ chức phải làm gì nếu muốn giao tiếp?

- A. Mỗi bên phải kiểm soát khóa chung và bốn khóa riêng của mình.
B. Mỗi bên phải quản lý khóa công khai và bốn khóa riêng của mình.
C. A & B đều đúng

D. Mỗi bên phải quản lý khóa riêng và bốn khóa chung của mình.

4. RSA hữu ích trong trường hợp nào sau đây?

A. Sử dụng thư ng mại

B. Sử dụng thư ng mại

C. Sử dụng toán học

D. Sử dụng máy tính

5. RSA được nhúng ở đâu?

A. Trong các trang web của Netscape

B. Trong Microsoft

C. Trong trình duyệt Web của Microsoft và Netscape

D. A&C đều đúng

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? Bạn biết gì về họ?

2. Trình bày các nội dung sau:

- Mã hóa bắt đầu xứng

- RSA

ĐỌC VÀ NÓI 4

1. Thảo luận các câu hỏi

1. PKI là viết tắt của từ gì? Nó có nghĩa là gì?
2. PKI là gì? Cái này được dùng để làm gì?
3. Những lĩnh vực nào nó được sử dụng rộng rãi?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Cơ sở hạ tầng nội công cộng

Khả năng che giấu nội dung của các thư nhạy cảm và xác minh nội dung của thư cũng như danh tính của người gửi có khả năng hữu ích trong mọi lĩnh vực kinh doanh. Để thực sự hữu ích, các khả năng mã hóa này phải được thể hiện trong các công cụ cho phép các nhà thực hành CNTT và bảo mật thông tin áp dụng các yếu tố của mật mã trong thế giới điện toán hàng ngày. Phần này đề cập đến một số công cụ được sử dụng rộng rãi hơn để mang lại các chức năng của mật mã cho thế giới hệ thống thông tin.

Cơ sở hạ tầng khóa công khai (PKI) là một hệ thống tích hợp phần mềm, phương pháp mã hóa, giao thức, thỏa thuận pháp lý và dịch vụ của bên thứ ba cho phép người dùng giao tiếp an toàn. Các hệ thống PKI dựa trên các hệ thống mật mã khóa công khai và bao gồm các chứng chỉ kỹ thuật số và cơ quan cấp chứng chỉ (CA).

Chứng chỉ kỹ thuật số là các tệp chứa khóa công khai cho phép các chương trình máy tính xác thực khóa và xác định người sở hữu khóa đó. PKI và các cơ quan đăng ký chứng chỉ kỹ thuật số mà chúng chứa cho phép bảo vệ tài sản thông tin bằng cách cung cấp các chứng chỉ kỹ thuật số có thể kiểm chứng sẵn có cho các ứng dụng kinh doanh. Đổi lại, điều này cho phép các ứng dụng triển khai một số đặc điểm chính của bảo mật thông tin và tích hợp các đặc điểm này vào hoạt động kinh doanh trong toàn tổ chức. Các quy trình này bao gồm:

- Xác thực: Các cá nhân, tổ chức và máy chủ Web có thể xác thực danh tính của mỗi bên trong một giao dịch Internet.
- Tính toàn vẹn: Nội dung được ký bởi chứng chỉ được biết là không bị thay đổi trong khi chuyển từ máy chủ này sang máy chủ khác hoặc máy chủ này sang máy khách khác.
- Quyền riêng tư: Thông tin được bảo vệ khỏi bị chặn trong quá trình truyền. Ủy quyền: Danh tính đã được xác thực của người dùng và chương trình

có thể kích hoạt các quy tắc ủy quyền vẫn được duy trì trong suốt thời gian giao dịch; điều này làm giảm một số chi phí hoạt động và cho phép kiểm soát nhiều hơn các đặc quyền truy cập đối với các giao dịch cụ thể.

- Chóng từ chối: Khách hàng hoặc đối tác có thể chịu trách nhiệm về các giao dịch, chẳng hạn như mua hàng trực tuyến, mà sau này họ không thể tranh chấp.

Một giải pháp PKI điển hình bảo vệ việc truyền và nhận thông tin an toàn bằng cách tích hợp các thành phần sau:

- Cơ quan cấp chứng chỉ (CA), phát hành, quản lý, xác thực, ký và thu hồi chứng chỉ kỹ thuật số của người dùng, chứng chỉ này thường chứa tên người dùng, khóa chung và thông tin nhận dạng khác.
- Cơ quan đăng ký (RA), hoạt động dưới sự cộng tác đáng tin cậy của cơ quan cấp chứng chỉ và có thể xử lý các chức năng nhận hàng ngày, chẳng hạn như xác minh thông tin đăng ký, tạo khóa người dùng cuối, thu hồi chứng chỉ và xác thực chứng chỉ người dùng.
- Thư mục chứng chỉ, là vị trí trung tâm để lưu trữ chứng chỉ

cung cấp một điểm truy cập duy nhất để quản trị và phân phối.

- Các giao thức quản lý, tổ chức và quản lý thông tin liên lạc giữa các CA, RA và người dùng cuối. Điều này bao gồm các chức năng và quy trình để thiết lập người dùng mới, phát hành khóa, khôi phục khóa, cập nhật khóa, thu hồi khóa và cho phép chuyển giao chứng chỉ và thông tin trạng thái giữa các bên tham gia vào khu vực thẩm quyền của PKI.

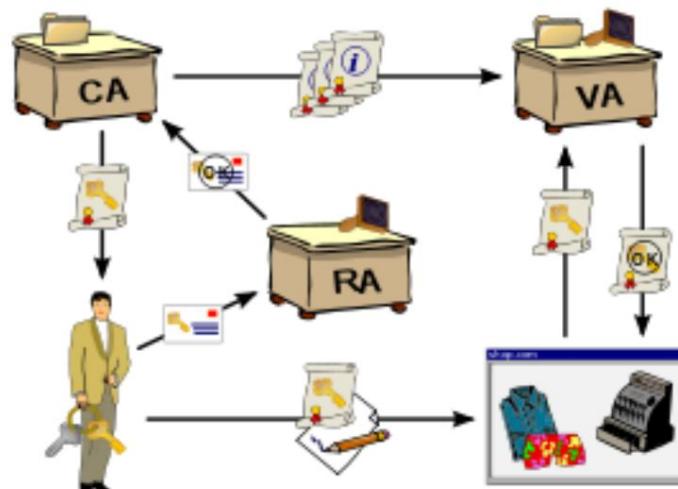
- Các chính sách và thủ tục hỗ trợ một tổ chức trong việc áp dụng và quản lý các chứng chỉ, trong việc chính thức hóa các trách nhiệm và giới hạn pháp lý, và trong thực tế sử dụng kinh doanh.

Việc triển khai PKI phổ biến bao gồm các hệ thống cấp chứng chỉ kỹ thuật số cho người dùng và máy chủ; tuyển sinh thư mục; hệ thống phát hành khóa; công cụ quản lý việc cấp khóa; và xác minh và trả lại giấy chứng nhận. Các hệ thống này cho phép các tổ chức áp dụng giải pháp toàn doanh nghiệp cung cấp cho người dùng trong khu vực thẩm quyền của PKI phuơng tiện để tham gia vào các hoạt động được xác thực và bảo mật. thông tin liên lạc và giao dịch.

CA thực hiện nhiều hoạt động về sinh liên quan đến việc sử dụng các khóa và chứng chỉ có vấn đề và được sử dụng trong khu vực có thẩm quyền của mình. Mỗi người dùng tự xác thực với CA và CA có thể cấp khóa mới hoặc khóa thay thế, theo dõi khóa đã cấp, cung cấp thư mục chứa các giá trị khóa công khai cho tất cả người dùng đã biết và

thực hiện các hoạt động quản lý khác. Khi khóa riêng tư bị xâm phạm hoặc khi người dùng mất đặc quyền sử dụng khóa trong khu vực có thẩm quyền, CA có thể thu hồi khóa của người dùng. CA phân phối định kỳ danh sách thu hồi chứng chỉ (CRL) cho tất cả người dùng. Khi các sự kiện quan trọng xảy ra, các ứng dụng cụ thể có thể đưa ra yêu cầu thời gian thực tới CA để xác minh bất kỳ người dùng nào đối với CRL hiện tại. Việc CA cấp chứng chỉ (và các khóa bên trong chứng chỉ) cho phép các giao dịch kinh doanh điện tử an toàn, được mã hóa và không thể chối bỏ. Một số ứng dụng cho phép người dùng tạo chứng chỉ của riêng họ (và các khóa bên trong chứng chỉ), như một cặp khóa do người dùng cuối tạo chỉ có thể cung cấp khả năng mã hóa không từ chối và không đáng tin cậy. Một hệ thống trung tâm do CA hoặc RA vận hành có thể tạo các khóa mật mã mạnh được tất cả người dùng coi là đáng tin cậy độc lập và có thể cung cấp các dịch vụ cho người dùng như sao lưu khóa riêng, khôi phục khóa và thu hồi khóa.

Sức mạnh của một hệ thống mật mã phụ thuộc vào cả sức mạnh thô của độ phức tạp của khóa và chất lượng tổng thể của các quy trình bảo mật quản lý khóa của nó. Các giải pháp PKI có thể cung cấp một số cơ chế để hạn chế quyền truy cập và khả năng lộ các khóa riêng tư. Các cơ chế này bao gồm bảo vệ bằng mật khẩu, thẻ thông minh, mã thông báo phần cứng và các thiết bị lưu trữ khóa dựa trên phần cứng khác có khả năng hỗ trợ bộ nhớ (như bộ nhớ flash hoặc thẻ nhớ PC). Người dùng PKI nên chọn cơ chế bảo mật khóa cung cấp mức độ bảo vệ khóa phù hợp với nhu cầu của họ. Việc quản lý tính bảo mật và tính toàn vẹn của các khóa riêng được sử dụng để chống từ chối hoặc mã hóa các tệp dữ liệu là rất quan trọng để sử dụng thành công các dịch vụ mã hóa và chống từ chối trong khu vực tin cậy của PKI.



Sơ đồ cơ sở hạ tầng khóa công khai

2.1. Trả lời các câu hỏi

1. PKI là viết tắt của từ gì? Nó là gì?
2. Những thành phần nào được tích hợp cho một PKI giải pháp điển hình để bảo vệ việc truyền và nhận thông tin an toàn?
3. Việc triển khai PKI phổ biến bao gồm những gì?
4. Sức mạnh của hệ thống mật mã dựa vào điều gì?
5. Chứng thư số là gì?
6. Điều gì là quan trọng để sử dụng thành công mã hóa và chống chối bỏ các dịch vụ trong phạm vi tin cậy của PKI.10?
7. Hệ thống cơ sở hạ tầng khóa công khai dựa trên cái gì?
8. Giải pháp PKI có thể cung cấp những cơ chế nào để hạn chế quyền truy cập và khả năng lộ các khóa riêng tư ?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI).

Sửa Sai (F)

1. Mục đích của chứng thư số là thiết lập danh tính của người dùng bên trong hệ sinh thái.
 A. Đúng B. Sai C. NI
2. Một thực thể phải được nhận dạng duy nhất trong mỗi miền CA trên cơ sở thông tin về thực thể đó. Cơ quan xác thực bên thứ ba có thể cung cấp thông tin thực thể này thay mặt cho CA.
 A. Đúng B. Sai C. NI
3. Độ phức tạp của khóa và chất lượng tổng thể của khóa quản lý là những yếu tố cơ bản không quan trọng đối với bảo vệ an ninh thông tin.
 A. Đúng B. Sai C. NI
4. CA cung cấp danh sách thu hồi chứng chỉ cho người dùng của mình, như ng không mất khóa của họ khi khóa riêng được đồng ý hoặc khi họ có đặc quyền sử dụng chìa khóa trong khu vực quyền hạn bị mất.
 A. Đúng B. Sai C. NI

5. Mục đích của PKI là tạo điều kiện thuận lợi cho việc chuyển giao điện tử an toàn thông tin cho một loạt các hoạt động mạng như thư ờng mại điện tử, internet ngân hàng và email bí mật.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1. CA có thể làm gì khi người dùng mất đặc quyền sử dụng các khóa trong phạm vi quyền hạn?

- A. CA có thể rút khóa của người dùng.
- B. CA có thể thu hồi khóa của người dùng.
- C. A & B đều đúng
- D. CA có thể hủy khóa của người dùng.

2. Chức năng của hệ thống trung tâm do CA điều hành là gì?

- A. Nó tạo ra các khóa mật mã mạnh được tất cả mọi người coi là người dùng trở nên đáng tin cậy một cách độc lập.
- B. Nó cung cấp sao lưu khóa riêng, khôi phục khóa và thu hồi khóa.
- C. A & B đều đúng
- D. Nó xác minh bất kỳ người dùng nào dựa trên danh sách thu hồi chứng chỉ hiện tại.

3. Người dùng PKI nên lựa chọn cơ chế nào trong chứng thực số?

- A. Cơ chế bảo mật khóa cung cấp mức độ bảo vệ khóa phù hợp với nhu cầu của họ.
- B. Các cơ chế thuận tiện giúp chúng trao đổi thông tin liên lạc nhanh.
- C. Cơ chế giao dịch tốt cho phép họ làm những gì họ cần
- D. A&C đều đúng

4.bởi CA cho phép kinh doanh điện tử an toàn, được mã hóa, không thể chối cãi giao dịch.

A. chính sách cấp giấy chứng nhận

B. cấp giấy chứng nhận

C. cơ chế chứng chỉ

D. thủ tục cấp giấy chứng nhận

5. CA có thư ờng xuyên phân phối danh sách thu hồi chứng chỉ cho tất cả người dùng không?

- A. Hàng năm
- B. Thư ờng xuyên
- C. Hai lần một năm
- D. Hàng tháng

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?
2. Trình bày quy trình thực hiện chứng thư số.
3. Trình bày ưu điểm của PKI.

ĐỌC VÀ NÓI 5

1. Thảo luận các câu hỏi

1. Từ tấn công mạng có nghĩa là gì?
2. Tấn công mạng là gì?
3. Bạn biết những kiểu tấn công mạng nào?
4. Bạn biết những kiểu tấn công nào trong mật mã?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Các cuộc tấn công vào hệ thống mật mã

Trong lịch sử, các nỗ lực để giành được quyền truy cập trái phép vào thông tin liên lạc an toàn đã sử dụng các cuộc tấn công vũ phu, trong đó bản mã được tìm kiếm nhiều lần để tìm manh mối có thể dẫn đến cấu trúc của thuật toán. Các cuộc tấn công bản mã này liên quan đến việc tin tặc tìm kiếm cấu trúc văn bản, từ ngữ hoặc cú pháp phổ biến trong tin nhắn được mã hóa có thể cho phép anh ta hoặc cô ta tính toán số lượng của từng loại chữ cái được sử dụng trong tin nhắn. Quá trình này, được gọi là phân tích tần suất, được sử dụng cùng với tần suất xuất hiện của các mẫu ngôn ngữ khác nhau và có thể cho phép kẻ tấn công có kinh nghiệm bẻ khóa nhanh chóng hầu hết mọi mã với một mẫu văn bản được mã hóa đủ lớn. Để chống lại điều này, các thuật toán hiện đại cố gắng loại bỏ các chuỗi ký tự lặp đi lặp lại và có thể dự đoán được khỏi bản mã.

Đôi khi, kẻ tấn công có thể lấy được các văn bản trùng lặp, một ở dạng bản mã và một ở dạng bản rõ, và do đó thiết kế nguy hiểm của thuật toán mã hóa trong sơ đồ tấn công bằng bản rõ đã biết. Ngoài ra, những kẻ tấn công có thể tiến hành một cuộc tấn công văn bản rõ được chọn bằng cách gửi cho nạn nhân tiềm năng một văn bản cụ thể mà họ chắc chắn rằng nạn nhân sẽ chuyển tiếp cho người khác. Khi nạn nhân mã hóa và chuyển tiếp tin nhắn, nó có thể được sử dụng trong cuộc tấn công nếu kẻ tấn công có được phiên bản mã hóa gửi đi. Ít nhất, kỹ thuật đảo ngược thư ờng có thể khiến kẻ tấn công phát hiện ra hệ thống mật mã nào đang được sử dụng.

Hầu hết các phương pháp mã hóa có sẵn công khai thư ờng được phát hành cho các cộng đồng bảo mật thông tin và máy tính để kiểm tra khả năng chống bẻ khóa của thuật toán mã hóa. Ngoài ra, những kẻ tấn công được thông báo về phương pháp tấn công nào đã thất bại. Mặc dù mục đích của việc chia sẻ thông tin này là để phát triển một thuật toán an toàn hơn, như ngay nó ngăn cản những kẻ tấn công lãng phí thời gian của họ,

giải phóng họ để tìm ra những điểm yếu mới trong hệ thống mật mã hoặc các phương tiện mới, khó khăn hơn để lấy khóa mã hóa.

Nói chung, các cuộc tấn công vào hệ thống mật mã rơi vào bốn loại chung: người ở giữa, tưƠng quan, từ điển và thời gian.

Người ở đài ông giữa cuộc chiến

Một cuộc tấn công trung gian có gắng chặn khóa chung hoặc thậm chí chèn cấu trúc khóa đã biết thay cho khóa chung được yêu cầu. Do đó, những kẻ tấn công cố gắng tự đặt mình vào giữa người gửi và người nhận và sau khi chặn được yêu cầu trao đổi khóa, chúng sẽ gửi cho mỗi người tham gia một khóa công khai hợp lệ, khóa này chỉ có họ biết. Đối với nạn nhân của các cuộc tấn công như vậy, giao tiếp được mã hóa thường như diễn ra bình thường, nhưng trên thực tế, kẻ tấn công đang nhận từng tin nhắn được mã hóa và giải mã nó (với khóa được trao cho bên gửi), sau đó mã hóa và gửi nó đến người nhận dự kiến. Việc thiết lập các khóa công khai bằng chữ ký số có thể ngăn chặn cuộc tấn công trung gian truyền thống, vì kẻ tấn công không thể sao chép chữ ký.

Tấn công tưƠng quan

Khi độ phức tạp của các phương pháp mã hóa tăng lên, các công cụ và phương pháp của các nhà phân tích mật mã cũng tăng theo. Các cuộc tấn công tưƠng quan là một tập hợp các phương pháp brute-force cố gắng suy ra các mối quan hệ thống kê giữa cấu trúc của khóa không xác định và bản mã do hệ thống mật mã tạo ra. Phân tích mật mã vi sai và tuyến tính, là các phương pháp phá mã tiên tiến nằm ngoài phạm vi của văn bản này, đã được sử dụng để thực hiện các cuộc tấn công thành công vào mã hóa khỏi mật mã như DES. Nếu những cách tiếp cận nâng cao này có thể tính toán giá trị của khóa công khai trong một khoảng thời gian hợp lý, thì tất cả các thông báo được viết bằng khóa đó đều có thể được giải mã. Biện pháp phòng thủ duy nhất chống lại cuộc tấn công này là lựa chọn các hệ thống mật mã mạnh mẽ vượt qua thử thách của thời gian, quản lý khóa kỹ lưỡng và tuân thủ nghiêm ngặt các phương pháp mã hóa tốt nhất về tần suất thay đổi khóa.

Tấn công từ điển

Trong một cuộc tấn công từ điển, kẻ tấn công mã hóa mọi từ trong từ điển bằng cách sử dụng cùng một hệ thống mật mã mà mục tiêu sử dụng nhằm cố gắng xác định sự trùng khớp giữa bản mã mục tiêu và danh sách các từ được mã hóa. Các cuộc tấn công từ điển có thể thành công khi bản mã bao gồm tưƠng đối ít ký tự, chẳng hạn như

các tệp chứa tên ngư ời dùng và mật khẩu đư ợc mã hóa. Kẻ tấn công lấy đư ợc tệp mật khẩu hệ thống có thể chạy hàng trăm nghìn mật khẩu tiềm năng từ từ điển mà kẻ đó đã chuẩn bị dựa trên danh sách bị đánh cắp. Hầu hết các hệ thống máy tính sử dụng hàm băm một chiều nổi tiếng để lưu trữ mật khẩu trong các tệp như vậy, nhưng kẻ tấn công hầu như luôn có thể tìm thấy ít nhất một vài kết quả trùng khớp trong bất kỳ tệp mật khẩu bị đánh cắp nào.

Sau khi tìm thấy kết quả phù hợp, kẻ tấn công về cơ bản đã xác định đư ợc một mật khẩu hợp lệ tiềm năng cho hệ thống.

Thời gian tấn công

Trong một cuộc tấn công theo thời gian, kẻ tấn công nghe lén phiên của nạn nhân và sử dụng phân tích thống kê các mẫu và thời gian nhấn phím giữa các lần nhấn để phân biệt thông tin phiên nhạy cảm. Mặc dù phân tích thời gian có thể không trực tiếp dẫn đến việc giải mã dữ liệu nhạy cảm, như ng nó có thể đư ợc sử dụng để thu thập thông tin về khóa mã hóa và có lẽ cả hệ thống mật mã. Nó cũng có thể loại bỏ một số thuật toán, do đó thu hẹp phạm vi tìm kiếm của kẻ tấn công và tăng tỷ lệ thành công cuối cùng. Sau khi phá vỡ mã hóa, kẻ tấn công có thể khởi chạy một cuộc tấn công phát lại, đây là nỗ lực gửi lại bản ghi thực đã giải mã để giành quyền truy cập vào một nguồn an toàn.

Bảo vệ chống lại các cuộc tấn công

Mã hóa là một công cụ rất hữu ích trong việc bảo vệ tính bảo mật của thông tin đư ợc lưu trữ hoặc truyền tải. Tuy nhiên, đó chỉ là một công cụ khác trong kho vũ khí của quản trị viên bảo mật thông tin chống lại các mối đe dọa đối với bảo mật thông tin.

Thông thường, những ngư ời không hiểu rõ chỉ mô tả bảo mật thông tin dưới dạng mã hóa (và có thể cả tư ờng lửa và phần mềm chống vi-rút). Như ng mã hóa chỉ đơn giản là quá trình che giấu ý nghĩa thực sự của thông tin.

Trải qua hàng thiên niên kỷ, nhân loại đã phát triển các phương tiện phức tạp hơn đáng kể để che giấu thông tin khỏi những ngư ời không nhìn thấy nó, nhưng cho dù các hệ thống mã hóa và mật mã có trở nên tinh vi đến đâu, chúng vẫn giữ lại lỗ hổng đã có trong hệ thống đầu tiên như vậy: Nếu bạn phát hiện ra key, nghĩa là phương pháp đư ợc sử dụng để thực hiện mã hóa, bạn có thể đọc tin nhắn. Vì vậy, quản lý then chốt không phải là quản lý công nghệ mà là quản lý con ngư ời.

2.1. Trả lời các câu hỏi

1. Tấn công tư ơ ng quan là gì?
2. Phư ơ ng pháp nào có thể ngăn chặn các cuộc tấn công tư ơ ng quan?
3. Tấn công trung gian là gì?
4. Phư ơ ng pháp nào có thể ngăn chặn kiểu tấn công xen giữa truyền thông?
5. Khi nào tấn công từ điển có thể thành công?
6. Khi nào kẻ tấn công có thể khởi động một cuộc tấn công lặp lại trong cuộc tấn công định thời?
7. Phư ơ ng pháp nào đã được sử dụng để truy cập trái phép vào bảo mật thông tin liên lạc?
8. Loại tấn công nào được đề cập trong văn bản?

2.2. Quyết định xem những câu sau đây là đúng (T), sai (F) hay không có thông tin (NI). Sửa Sai (F)

1. Một cuộc tấn công trong đó kẻ tấn công bí mật chuyển tiếp và có thể thay đổi thông tin liên lạc giữa hai bên tin rằng họ đang trực tiếp giao tiếp với nhau được gọi là tấn công man-in-the-middle.
A. Đúng B. Sai C. NI
2. Mặc dù phân tích tần suất có thể cho phép kẻ tấn công thiếu kinh nghiệm để bẻ khóa hầu hết mọi mã một cách nhanh chóng, các thuật toán hiện đại có thể phá vỡ nó.
A. Đúng B. Sai C. NI
3. Hàm băm một chiều nổi tiếng được sử dụng để lưu trữ mật khẩu, vì vậy kẻ tấn công không thể bẻ khóa nó và thông tin không bao giờ bị đánh cắp.
A. Đúng B. Sai C. NI
4. Các phư ơ ng tiện tinh vi hơn để che giấu thông tin với những người không nên thấy nó ngày càng phát triển nên việc bảo mật thông tin luôn được an toàn.
A. Đúng B. Sai C. NI
5. Một cuộc tấn công từ điển dựa trên việc thử tất cả các chuỗi được sắp xếp trước liệt kê, thường bắt nguồn từ một danh sách các từ như trong từ điển.
A. Đúng B. Sai C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu và câu hỏi sau

1. Những cuộc tấn công nào đã được sử dụng để giành quyền truy cập trái phép vào hệ thống an toàn thông tin liên lạc?
 - A. Tấn công vũ phu
 - B. các cuộc tấn công bằng văn bản đã biết
 - C. các cuộc tấn công -plaintext đã chọn
 - D. Tất cả đều đúng

2. Những kẻ tấn công có thể tiến hành bằng cách gửi cho các nạn nhân tiềm năng một văn bản cụ thể mà họ chắc chắn rằng các nạn nhân sẽ chuyển tiếp cho những người khác.
 - A. tấn công bằng văn bản đã biết
 - B. tấn công bản rõ đã chọn
 - C. Tấn công vũ phu
 - D. A & C đều đúng

3.đã được sử dụng để thực hiện tấn công thành công vào mật mã khôi phục như DES.
 - A. Thám mã vi sai và tuyển tính
 - B. Thám mã vi sai
 - C. Phân tích tần số
 - D. Giải mã tuyển tính

4. Kẻ tấn công nghe trộm phiên làm việc của nạn nhân trong cuộc tấn công nào?
 - A. Trong một cuộc tấn công từ điển
 - B. Trong một cuộc tấn công tư ơng quan
 - C. Trong một cuộc tấn công trung gian
 - D. Trong một cuộc tấn công thời gian

5. Từ “these” trong đoạn 4 đề cập đến điều nào sau đây?
 - A. Tấn công tư ơng quan
 - B. Phư ơng pháp bạo lực
 - C. Thám mã vi sai và tuyển tính
 - D. Phư ơng pháp nâng cao

3. Nói

1. Qua văn bản em rút ra được những nội dung chính nào? bạn biết gì về họ?

2. Trình bày các cuộc tấn công vào hệ thống mật mã.

4. Lắng nghe

1. <https://www.youtube.com/watch?v=cqgtdkURzTE>
2. <https://www.youtube.com/watch?v=c5rHvmJwF0M>

3. <https://www.youtube.com/watch?v=2BldESGZKB8>
4. https://www.youtube.com/watch?v=JR4_RBb8A9Q
5. https://www.youtube.com/watch?v=Rnn_HLtgJ2M
6. <https://www.youtube.com/watch?v=AQDCe585Lnc>

VIẾT VÀ NÓI

1. Viết khoảng 400 từ về một trong những chủ đề sau theo cách của riêng bạn từ ngữ.

- Hàm băm
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Tấn công vào hệ thống mật mã

2. Trình bày các nội dung sau:

- Hàm băm
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Tấn công vào hệ thống mật mã

ĐỌC THÊM

Chữ ký số

Chữ ký số được tạo ra để đáp ứng nhu cầu ngày càng tăng để xác minh thông tin được truyền qua hệ thống điện tử. Các quy trình mã hóa bắt đầu xứng được sử dụng để tạo chữ ký số. Khi một quy trình mã hóa bắt đầu xứng sử dụng khóa riêng của người gửi để mã hóa tin nhắn, thì khóa chung của người gửi phải được sử dụng để giải mã tin nhắn. Khi quá trình giải mã thành công, quá trình xác minh rằng thông báo đã được gửi bởi người gửi và do đó không thể bắc bối. Quá trình này được gọi là không từ chối và là nguyên tắc của mật mã làm nền tảng cho cơ chế xác thực được gọi chung là chữ ký số.

Do đó, chữ ký số là các thông điệp được mã hóa có thể được chứng minh là xác thực về mặt toán học.

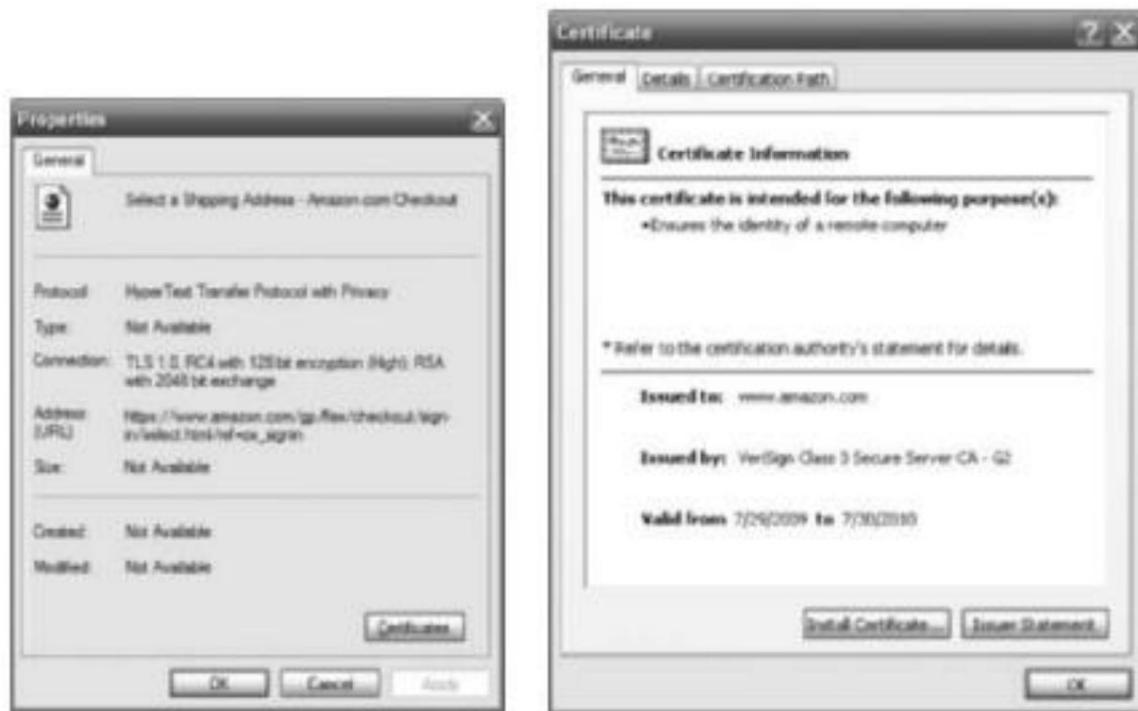
Việc quản lý chữ ký điện tử được tích hợp trong hầu hết các trình duyệt Web. Nói chung, chữ ký số nên được tạo bằng cách sử dụng các quy trình và sản phẩm dựa trên Tiêu chuẩn Chữ ký số (DSS). Khi các quy trình và sản phẩm được chứng nhận là tuân thủ DSS, chúng đã được chính phủ tiểu bang và liên bang Hoa Kỳ cũng như nhiều chính phủ nước ngoài phê duyệt và chứng thực như một phương tiện xác thực tác giả của tài liệu điện tử. NIST đã phê duyệt một số thuật toán có thể được sử dụng để tạo và xác minh chữ ký số.

Các thuật toán này có thể được sử dụng cùng với khóa công khai và khóa riêng của người gửi, khóa chung của người nhận và Tiêu chuẩn băm toàn (được mô tả trước đó trong chương này) để nhanh chóng tạo ra các thông báo được mã hóa và không thể chối bỏ. Quá trình này trước tiên tạo ra một bản tóm tắt thông báo bằng cách sử dụng thuật toán băm, sau đó được nhập vào thuật toán chữ ký số cùng với một số ngẫu nhiên để tạo chữ ký số. Chức năng chữ ký điện tử cũng phụ thuộc vào khóa riêng của người gửi và các thông tin khác do CA cung cấp. Thông báo được mã hóa kết quả chứa chữ ký số, chữ ký này có thể được xác minh bởi người nhận bằng khóa công khai của người gửi.

Chứng chỉ kỹ thuật

số Chứng chỉ kỹ thuật số là một tài liệu điện tử hoặc tệp vùng chứa chứa giá trị khóa và thông tin nhận dạng về thực thể kiểm soát khóa. Chứng chỉ thư ờng được cấp và chứng nhận bởi bên thứ ba, thư ờng là chứng chỉ. Một

chữ ký điện tử đư ợc đính kèm với tệp chứa chứng chỉ xác nhận nguồn gốc và tính toàn vẹn của tệp. Quá trình xác minh này thường xảy ra khi bạn tải xuống hoặc cập nhật phần mềm qua Internet. Ví dụ, cửa sổ trong **Hình 6-3** cho thấy rằng các tệp đã tải xuống thực tế đến từ cơ quan có nguồn gốc rõ ràng là Amazon.com và do đó có thể đư ợc tin cậy.



Hình 6-3 Chứng thư số

Không giống như chữ ký số, giúp xác thực nguồn gốc của tin nhắn, chứng chỉ số xác thực khóa mật mã đư ợc nhúng trong chứng chỉ.

Khi đư ợc sử dụng đúng cách, các chứng chỉ này cho phép người dùng siêng năng xác minh tính xác thực của bất kỳ chứng chỉ nào của tổ chức. Điều này rất giống với những gì xảy ra khi Tổng công ty Bảo hiểm Tiền gửi Liên bang cấp logo FDIC cho các ngân hàng để đảm bảo với khách hàng rằng ngân hàng của họ là xác thực. Các ứng dụng máy khách-máy chủ khác nhau sử dụng các loại chứng chỉ kỹ thuật số khác nhau để thực hiện các chức năng đư ợc giao, như sau

- Bộ ứng dụng CA phát hành và sử dụng các chứng chỉ (khóa) xác định và thiết lập mối quan hệ tin cậy với CA để xác định chứng chỉ (khóa) bổ sung nào có thể đư ợc xác thực.

- Các ứng dụng thư sử dụng các chứng chỉ Phần mở rộng Thư Internet Bảo mật/Đa mục đích (S/MIME) để ký và mã hóa e-mail cũng như để ký các biểu mẫu.
- Các ứng dụng phát triển sử dụng chứng chỉ ký đôi tư ợng để xác định người gửi ký mã và tập lệnh hứa hẹn ký đôi tư ợng.
- Máy chủ web và máy chủ ứng dụng Web sử dụng chứng chỉ Lớp cổng bảo mật (SSL) để xác thực máy chủ thông qua giao thức SSL (được mô tả ngắn gọn) nhằm thiết lập phiên SSL được mã hóa.
- Máy khách web sử dụng chứng chỉ SSL máy khách để xác thực người dùng, ký biểu mẫu và tham gia các giải pháp đăng nhập một lần qua SSL.

BÀI 7: AN NINH VẬT LÝ

Giới thiệu

Bảo mật thông tin yêu cầu bảo vệ cả dữ liệu và tài sản vật chất. Bạn đã tìm hiểu về nhiều cơ chế được sử dụng để bảo vệ dữ liệu, bao gồm tia lửa, hệ thống phát hiện xâm nhập và phần mềm giám sát.

An ninh vật lý bao gồm việc thiết kế, triển khai và duy trì các biện pháp đối phó nhằm bảo vệ các nguồn lực vật chất của một tổ chức, bao gồm con người, phần cứng và các phần tử hệ thống hỗ trợ cũng như các nguồn lực kiểm soát thông tin ở tất cả các trạng thái của nó (truyền, lưu trữ và xử lý). Hầu hết các biện pháp kiểm soát dựa trên công nghệ đều có thể bị phá vỡ nếu kẻ tấn công giành được quyền truy cập vật lý vào các thiết bị đang được kiểm soát. Nói cách khác, nếu có thể dễ dàng đánh cắp các ổ cứng từ hệ thống máy tính, thì thông tin trên các ổ cứng đó không an toàn.

Do đó, bảo mật vật lý cũng quan trọng như bảo mật logic đối với chương trình bảo mật thông tin.

Trong các bài trước, bạn gặp phải một số mối đe dọa đối với bảo mật thông tin có thể được phân loại là các mối đe dọa đối với bảo mật vật lý. Ví dụ: một nhân viên vô tình làm đổ cà phê lên máy tính xách tay sẽ đe dọa đến tính bảo mật vật lý của thông tin trong máy tính-trong trường hợp này, mối đe dọa là do lỗi hoặc lỗi của con người. Một sự thỏa hiệp đối với quyền sở hữu trí tuệ có thể bao gồm việc một nhân viên không có giấy phép bảo mật thích hợp sao chép một kế hoạch tiếp thị đã được phân loại. Một hành động gián điệp hoặc xâm phạm có chủ ý có thể là một đối thủ cạnh tranh lén vào cơ sở bằng máy ảnh. Các hành vi phá hoại hoặc phá hoại có chủ ý có thể là các cuộc tấn công vật lý vào cá nhân hoặc tài sản. Hành vi cố ý trộm cắp bao gồm nhân viên ăn cắp thiết bị máy tính, thông tin xác thực, mật khẩu và máy tính xách tay. Chất lượng dịch vụ sai lệch so với các nhà cung cấp dịch vụ, đặc biệt là điện và nước, cũng thể hiện các mối đe dọa an ninh vật lý, cũng như các bất thường về môi trường khác nhau. Trong cuốn sách của mình, Chống tội phạm máy tính, Donn B. Parker liệt kê "Bảy nguồn tổn thất vật chất chính" sau đây:

- Nhiệt độ cực cao: nóng, lạnh •

Khí: khí chiến tranh, hơi thở mặn, không khí ẩm hoặc khô, các hạt lơ lửng

- Chất lỏng: nước, hóa chất • Sinh vật sống: vi rút, vi khuẩn, con người, động vật, côn trùng • Đạn: các vật thể hữu hình đang chuyển động, vật thể được cấp điện • Chuyển động: sụp đổ, cắt, lắc, rung, hóa lỏng, sóng chảy, tách, trượt •

Dị thư ờng về năng lượng: xung điện hoặc hồng hót, từ tính, tĩnh điện, mạch điện bị lão hóa; bức xạ: âm thanh, ánh sáng, radio, lò vi sóng, điện từ, nguyên tử

Như với tất cả các lĩnh vực an ninh khác, việc thực hiện an ninh vật lý

biện pháp đòi hỏi chính sách tổ chức hợp lý. Các chính sách bảo mật vật lý hư hỏng dẫn nguy hiểm dùng cách sử dụng hợp lý tài nguyên máy tính và tài sản thông tin, cũng như bảo vệ an toàn cá nhân của chính họ trong các hoạt động hàng ngày. Bảo mật vật lý được thiết kế và thực hiện trong một số lớp. Mỗi cộng đồng quan tâm của tổ chức chịu trách nhiệm về các thành phần trong các lớp này, như sau:

- Quản lý chung chịu trách nhiệm về an ninh của cơ sở mà tổ chức đặt trụ sở và các chính sách cũng như tiêu chuẩn cho hoạt động an toàn. Điều này bao gồm an ninh bên ngoài, phòng cháy chữa cháy và lối vào tòa nhà, cũng như các biện pháp kiểm soát khác như chó bảo vệ và khóa cửa. • Các chuyên gia và quản lý CNTT chịu trách nhiệm về an ninh môi trường và truy cập tại các địa điểm đặt thiết bị công nghệ, cũng như các chính sách và tiêu chuẩn chi phối hoạt động của thiết bị an toàn. Điều này bao gồm quyền truy cập vào các phòng máy chủ, điều hòa điện và kiểm soát nhiệt độ và độ ẩm của phòng máy chủ, cũng như các biện pháp kiểm soát chuyên dụng hơn như thiết bị nhiệt tinh điện và bụi.

Các chuyên gia và quản lý bảo mật thông tin chịu trách nhiệm đánh giá rủi ro và xem xét các biện pháp kiểm soát bảo mật vật lý được thực hiện bởi hai nhóm còn lại.

ĐỌC VÀ NÓI 1

1. Thảo luận các câu hỏi:

1. An ninh vật lý là gì?
 2. Các mối đe dọa chính đối với an ninh vật lý là gì?
 3. Kiểm soát truy cập vật lý khác với truy cập logic như thế nào
điều khiển? Nó giống như thế nào?
 4. Bạn có thể xác định các biện pháp kiểm soát truy cập vật lý nào trong Học viện của chúng tôi?
 5. Ai chịu trách nhiệm kiểm soát truy cập vật lý trong Học viện của chúng tôi?
2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Kiểm soát truy cập vật lý

Một số biện pháp kiểm soát truy cập vật lý đặc biệt phù hợp để quản lý hoạt động di chuyển của mọi người trong các cơ sở của tổ chức-cụ thể là kiểm soát quyền truy cập vật lý của họ vào các tài nguyên của công ty. Trong khi truy cập hợp lý vào các hệ thống, trong thời đại Internet này, là một chủ đề rất quan trọng, thì việc kiểm soát truy cập vật lý vào tài sản của tổ chức cũng có tầm quan trọng đặc biệt. Một số công nghệ

đư ợc sử dụng để kiểm soát truy cập vật lý cũng đư ợc sử dụng để kiểm soát truy cập logic, bao gồm sinh trắc học, thẻ thông minh và thẻ chìa khóa kích hoạt không dây.

Trư ớc khi tìm hiểu thêm về kiểm soát truy cập vật lý, bạn cần hiểu điều gì làm cho cơ sở an toàn. Quản lý chung của một tổ chức giám sát an ninh vật lý của nó. Thông thường, các biện pháp kiểm soát truy cập của tòa nhà đư ợc vận hành bởi một nhóm có tên là quản lý cơ sở vật chất. Các tổ chức lớn hơn có thể có toàn bộ nhân viên chuyên quản lý cơ sở vật chất, trong khi các tổ chức nhỏ hơn thường thuê ngoài các nhiệm vụ này.

Trong quản lý cơ sở, cơ sở an toàn là một vị trí thực tế có các biện pháp kiểm soát tại chỗ để giảm thiểu rủi ro bị tấn công từ các mối đe dọa vật lý. Thuật ngữ cơ sở an toàn có thể gợi nhớ đến các căn cứ quân sự, nhà tù an ninh tối đa và nhà máy điện hạt nhân, nhưng trong khi việc đảm bảo an toàn cho cơ sở đòi hỏi phải tuân thủ một số quy tắc và thủ tục, thì môi trường không nhất thiết phải bị hạn chế như vậy. Cũng không nhất thiết cơ sở phải giống pháo đài để giảm thiểu rủi ro từ các cuộc tấn công vật lý. Trên thực tế, một cơ sở an toàn đôi khi có thể sử dụng địa hình tự nhiên, luồng giao thông địa phương và sự phát triển xung quanh để tăng cường an ninh vật lý, cùng với các cơ chế bảo vệ như hàng rào, cổng, tường, bảo vệ và hệ thống báo động.

Kiểm soát an ninh vật lý

Có một số biện pháp kiểm soát an ninh vật lý mà các cộng đồng quan tâm của tổ chức nên xem xét khi triển khai an ninh vật lý bên trong và bên ngoài cơ sở. Một số điều khiển chính là:

- Tư ờng, hàng rào và cổng • Bảo vệ
- Chó •
- Thẻ ID và huy hiệu • Ô khóa
- và chìa khóa • Thần chú •
- Giám sát điện tử • Báo động
- và hệ thống báo động • Phòng
- máy tính và tủ đấu dây • Tư ờng và
- cửa bên trong

Tư ờng, Hàng rào và Cổng Một số yếu tố lâu đời nhất và đáng tin cậy nhất của an ninh vật lý là tư ờng, hàng rào và cổng. Mặc dù không phải mọi tổ chức đều cần triển khai các biện pháp kiểm soát vành đai bên ngoài, nhưng tư ờng và hàng rào có cổng phù hợp là điểm khởi đầu cần thiết cho các tổ chức có nhân viên yêu cầu quyền truy cập vào các vị trí thực tế mà tổ chức sở hữu hoặc kiểm soát. Các loại kiểm soát này rất khác nhau về hình thức và chức năng, từ liên kết chuỗi hoặc hàng rào riêng tư kiểm soát nơi mỗi người nén đỗ xe hoặc đi bộ, cho đến xây dựng các rào chắn bằng bê tông hoặc gạch xây đư ợc thiết kế để chịu đư ợc sức nổ của bom xe. Mỗi biện pháp kiểm soát chủ yếu bên ngoài yêu cầu lập kế hoạch chuyên nghiệp để đảm bảo rằng nó đáp ứng các mục tiêu an ninh và

nó thể hiện một hình ảnh phù hợp với tổ chức.

Bảo vệ Các biện pháp kiểm soát như hàng rào và tư ờng có công là tinh và do đó không phản hồi với các hành động, trừ khi chúng được lập trình để phản hồi bằng các hành động cụ thể đối với các kích thích cụ thể, chẳng hạn như mở cửa cho người có chìa khóa chính xác.

Mặt khác, lính canh có thể đánh giá từng tình huống khi nó phát sinh và đưa ra những phản ứng hợp lý. Hầu hết các nhân viên bảo vệ đều có các quy trình vận hành tiêu chuẩn (SOP) rõ ràng giúp họ hành động dứt khoát trong các tình huống không quen thuộc. Ví dụ, trong quân đội, các lính canh được đưa ra các mệnh lệnh chung (xem Ngoại tuyến về nhiệm vụ canh gác), cũng như các mệnh lệnh đặc biệt dành riêng cho vị trí của họ.

Chó Nếu một tổ chức đang bảo vệ các nguồn tài nguyên có giá trị, chó có thể là một phần có giá trị của an ninh vật lý nếu chúng được tích hợp vào kế hoạch và được quản lý đúng cách.

Chó bảo vệ rất hữu ích vì khứu giác và thính giác nhạy bén của chúng có thể phát hiện ra những sự xâm nhập mà những người bảo vệ con người không thể, và chúng có thể bị tổn hại khi cần thiết để tránh gây nguy hiểm đến tính mạng của một người.

Thẻ ID và Phù hiệu Thẻ nhận dạng (ID) thường được che giấu, trong khi huy hiệu tên có thể nhìn thấy được. Cả hai thiết bị có thể phục vụ một số mục đích.

Đầu tiên, chúng đóng vai trò là các dạng sinh trắc học đơn giản ở chỗ chúng sử dụng ảnh của chủ thẻ để xác thực quyền truy cập của họ vào cơ sở. Các thẻ có thể được mã hóa rõ ràng để chỉ định tòa nhà hoặc khu vực nào có thẻ được truy cập. Thứ hai, thẻ ID có dải từ tính hoặc chip radio có thể được đọc bởi các thiết bị điều khiển tự động cho phép tổ chức hạn chế quyền truy cập vào các khu vực nhạy cảm trong cơ sở. Tuy nhiên, thẻ ID và huy hiệu tên không phải là hoàn hảo; và ngay cả những thẻ được thiết kế để giao tiếp với ổ khóa cũng có thể dễ dàng bị sao chép, đánh cắp hoặc sửa đổi. Do điểm yếu này, các thiết bị như vậy không nên là phương tiện duy nhất của tổ chức để kiểm soát quyền truy cập vào các khu vực hạn chế.

Một điểm yếu có hữu khác của loại công nghệ kiểm soát truy cập vật lý này là yếu tố con người. Bám sát xảy ra khi một người được ủy quyền xuất trình chìa khóa để mở cửa và những người khác, có thể hoặc không được ủy quyền, cũng bức ợc vào. Khởi động một chiến dịch để làm cho nhân viên nhận thức được việc theo dõi là một cách để chống lại vấn đề này. Ngoài ra còn có các phương tiện công nghệ làm nản lòng việc theo dõi, chẳng hạn như bẫy (sẽ được thảo luận trong phần sau) hoặc cửa quay. Các cấp độ kiểm soát bổ sung này thường đặt ở chỗ chúng yêu cầu không gian sàn và/hoặc xây dựng, đồng thời gây bất tiện cho những người được yêu cầu sử dụng chúng. Do đó, các biện pháp kiểm soát chống nỗi đau chỉ được sử dụng khi có rủi ro bảo mật đáng kể do xâm nhập trái phép.

Khóa và Chìa khóa Có hai loại cơ cấu khóa: cơ khí và cơ điện. Khóa cơ có thể dựa vào chìa khóa là một miếng kim loại được tạo hình cẩn thận, được xoay để xoay các lẫy nhả ra các vòng thép, nhôm hoặc đồng thau được bảo đảm (chẳng hạn như ổ khóa bằng đồng thau). Ngoài ra, một khóa cơ học có thể có một mặt số xoay các đĩa có rãnh cho đến khi các rãnh trên nhiều đĩa được căn chỉnh, sau đó rút chốt giữ (như trong khóa kết hợp và khóa an toàn).

khóa). Mặc dù khóa cơ về mặt khái niệm là đơn giản, nhưng một số công nghệ đi vào quá trình phát triển của chúng lại khá phức tạp. Một số cải tiến hiện đại này đã dẫn đến việc tạo ra khóa cơ điện.

Khóa điện cơ có thể chấp nhận nhiều loại đầu vào dưới dạng chìa khóa, bao gồm dải từ tính trên thẻ ID, tín hiệu vô tuyến từ huy hiệu tên, số nhận dạng cá nhân (PIN) được nhập vào bàn phím hoặc một số kết hợp của những thứ này để kích hoạt cơ chế khóa chạy bằng điện.

Khóa cũng có thể được chia thành bốn loại dựa trên quy trình kích hoạt: thủ công, có thể lập trình, điện tử và sinh trắc học. Khóa thủ công như khóa móc và khóa kết hợp, là phổ biến và được hiểu rõ. Nếu bạn có chìa khóa (hoặc tổ hợp), bạn có thể mở khóa. Các ổ khóa này thường có mặt của nhà sản xuất và do đó không thể thay đổi. Nói cách khác, một khi khóa thủ công được lắp vào cửa, chúng chỉ có thể được thay đổi bởi thợ khóa được đào tạo bài bản.

Khóa có thể lập trình có thể được thay đổi sau khi chúng được đưa vào sử dụng, cho phép thay đổi tổ hợp hoặc chìa khóa mà không cần thợ khóa và thậm chí cho phép chủ sở hữu thay đổi phuơng thức truy cập khác (khóa hoặc tổ hợp) để nâng cấp bảo mật. Nhiều ví dụ về các loại khóa này được hiển thị trong Hình 7-1. Khóa bấm cơ khí, được hiển thị trong ảnh ngoài cùng bên trái trong Hình 7-1, phổ biến để bảo vệ phòng máy tính và tủ nối dây, vì chúng có mã có thể đặt lại và không cần điện để hoạt động.

Khóa điện tử có thể tích hợp vào hệ thống báo động và kết hợp với các hệ thống quản lý tòa nhà khác. Ngoài ra, những ổ khóa này có thể được tích hợp với các cảm biến để tạo ra nhiều cách kết hợp hành vi khóa khác nhau. Một sự kết hợp như vậy là một hệ thống điều phối việc sử dụng chuông báo cháy và khóa để cải thiện độ an toàn trong các điều kiện báo động (ví dụ: hỏa hoạn). Một hệ thống như vậy sẽ thay đổi mức ủy quyền truy cập bắt buộc của một vị trí khi vị trí đó ở trong tình trạng báo động. Một ví dụ khác là một hệ thống kết hợp trong đó một ổ khóa được gắn một cảm biến để thông báo cho các trạm bảo vệ khi ổ khóa đó đã được kích hoạt. Một dạng khóa điện tử phổ biến khác là khóa điện tử, loại khóa này thường yêu cầu mọi người phải thông báo trước khi bị "bù" qua một cánh cửa bị khóa. Nói chung, khóa điện tử phù hợp để sử dụng khi chúng có thể được kích hoạt hoặc hủy kích hoạt bằng một công tắc được điều khiển bởi một nhân viên, thường là thư ký hoặc bảo vệ. Khóa nút bấm điện tử, giống như những người anh em họ cơ khí của chúng, có bàn phím số phía trên num, yêu cầu người dùng nhập mã cá nhân và mở cửa. Những ổ khóa này thường sử dụng pin dự phòng để cấp nguồn cho bàn phím trong trường hợp mất



Lập trình/cơ khí

điện tử

Hình 7-1 Khóa

Một số ổ khóa sử dụng thẻ thông minh, như đã mô tả trước đây-chìa khóa có chứa chip máy tính. Những thẻ thông minh này có thể mang thông tin quan trọng, cung cấp khả năng xác thực mạnh mẽ và cung cấp một số tính năng khác. Đầu đọc thẻ khóa dựa trên thẻ thông minh thường được sử dụng để bảo vệ phòng máy tính, tủ thông tin liên lạc và các khu vực hạn chế khác. Đầu đọc thẻ có thể theo dõi mục nhập và cung cấp trách nhiệm giải trình. Trong một hệ thống khóa sử dụng thẻ thông minh, cấp độ truy cập của các cá nhân có thẻ được điều chỉnh theo trạng thái hiện tại của họ (tức là nhân viên hiện tại, vừa nghỉ việc) và do đó thay đổi nhân sự không yêu cầu thay thế khóa. Một loại đầu đọc thẻ khóa chuyên dụng là đầu đọc gần, thay vì yêu cầu các cá nhân đưa thẻ vào, cho phép họ chỉ cần đặt thẻ của mình trong phạm vi của đầu đọc. Một số đầu đọc này có thể nhận ra thẻ ngay cả khi nó ở trong túi.

Các khóa phức tạp nhất là khóa sinh trắc học. Đầu đọc ngón tay, lòng bàn tay và bàn tay, máy quét mống mắt và võng mạc, đầu đọc giọng nói và chữ ký thuộc loại này.

Việc quản lý chìa khóa và ổ khóa là cơ bản để hoàn thành trách nhiệm của ban quản lý chung nhằm đảm bảo môi trường vật chất của tổ chức.

Khi mọi người được tuyển dụng, sa thải, sa thải hoặc thuyên chuyển, các biện pháp kiểm soát truy cập của họ, dù là vật lý hay logic, đều phải được điều chỉnh phù hợp. Nếu không làm như vậy có thể dẫn đến việc nhân viên dọn dẹp văn phòng của họ và lấy đi nhiều hơn những vật dụng cá nhân của họ. Ngoài ra, khi thuê thợ khóa, họ phải được sàng lọc và theo dõi cẩn thận, vì có khả năng họ có toàn quyền tiếp cận cơ sở.

Đôi khi khóa không thành công, và do đó các cơ sở cần phải có các quy trình thay thế để kiểm soát truy cập. Các quy trình này phải tính đến trường hợp ổ khóa bị hỏng theo một trong hai cách: khóa cửa bị hỏng và cửa không khóa được-một ổ khóa an toàn bị hỏng; hoặc khóa cửa không thành công và cửa vẫn khóa-một khóa không an toàn.

Trong thực tế, lý do phổ biến nhất khiến các khóa phức tạp về mặt kỹ thuật bị lỗi là

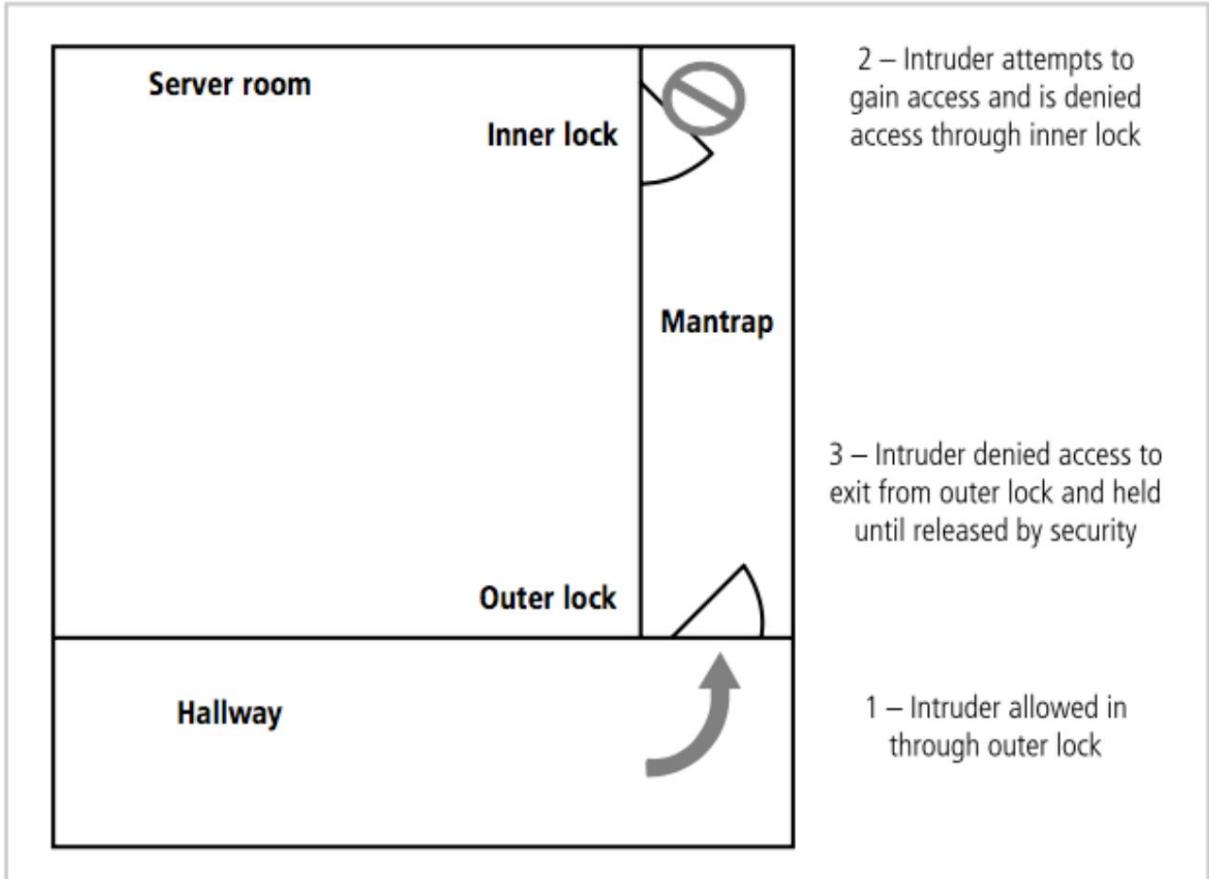
mắt điện và kích hoạt thông qua hệ thống điều khiển hỏa lực. Khóa không an toàn thư ờng được sử dụng để đảm bảo lôi ra, trong đó điều cần thiết là trong trư ờng hợp chẳng hạn như hỏa hoạn, cửa phải được mở khóa. Khóa không an toàn được sử dụng khi sự an toàn của con người trong khu vực được kiểm soát không phải là yếu tố chi phối. Một ví dụ về điều này là tình huống cần phải kiểm soát an ninh vũ khí hạt nhân hoặc sinh học; ở đây, ngăn chặn việc mắt kiểm soát những vũ khí này quan trọng hơn đối với an ninh (có nghĩa đây là vấn đề an ninh có tầm quan trọng lớn hơn) hơn là bảo vệ tính mạng của nhân viên bảo vệ vũ khí.

Hiểu cơ chế khóa là rất quan trọng, bởi vì kẻ xâm nhập có thể khai thác khóa để có quyền truy cập vào vị trí được bảo mật. Nếu khóa điện tử bị đoán mạo, nó có thể trở nên không an toàn và cho phép kẻ đột nhập vượt qua bộ điều khiển và vào phòng.

Mantraps Một cải tiến phổ biến cho các ổ khóa trong khu vực an ninh cao là mantrap. Một mantrap là một bao vây nhỏ có các điểm vào và ra riêng biệt. Để có quyền truy cập vào cơ sở, khu vực hoặc phòng, một người vào bẫy, yêu cầu quyền truy cập thông qua một số dạng khóa và chìa khóa điện tử hoặc sinh trắc học, và nếu được xác nhận, sẽ thoát khỏi bẫy vào cơ sở. Một khác, người đó không thể rời khỏi chiếc bẫy cho đến khi một quan chức an ninh ghi đè các khóa tự động của vỏ bọc. **Hình 7-2** cung cấp một ví dụ về cách bố trí mantrap điển hình.

Giám sát Điện tử Thiết bị giám sát có thể được sử dụng để ghi lại các sự kiện trong một khu vực cụ thể mà lính canh và chó có thể bỏ sót, hoặc ở những khu vực mà các loại kiểm soát vật lý khác không thực tế. Mặc dù bạn có thể không biết điều đó, nhưng nhiều người trong số các bạn, nhờ các quả cầu bạc gắn trên trần của nhiều cửa hàng bán lẻ, đã là đối tượng của các camera quan sát bạn từ các góc kỳ lạ-tức là giám sát video. Kèm theo những máy ảnh này là máy ghi băng video (VCR) và các máy móc liên quan để ghi lại nguồn cấp dữ liệu video. Giám sát điện tử bao gồm các hệ thống truyền hình mạch kín (CCT). Một số hệ thống CCT thu thập nguồn cấp dữ liệu video liên tục, trong khi những hệ thống khác xoay vòng đầu vào từ một số camera, lần lượt lấy mẫu từng khu vực.

Các hệ thống giám sát video này có như ợc điểm: phần lớn chúng bị động và không ngăn chặn truy cập hoặc hoạt động bị cấm. Một như ợc điểm khác của các hệ thống này là mọi người phải xem đầu ra video vì không có hệ thống thông minh nào có khả năng đánh giá nguồn cấp dữ liệu video một cách đáng tin cậy. Để xác định xem các hoạt động trái phép có xảy ra hay không, nhân viên an ninh phải liên tục xem xét thông tin theo thời gian thực hoặc xem xét thông tin thu thập được trong các bản ghi video. Vì lý do này, CCT thư ờng được sử dụng như một thiết bị thu thập bằng chứng sau khi một khu vực bị đột nhập hơn là một công cụ phát hiện. Tuy nhiên, ở những khu vực có mức độ an ninh cao (chẳng hạn như ngân hàng, sòng bạc và trung tâm mua sắm), nhân viên an ninh liên tục giám sát các hệ thống CCT, tìm kiếm hoạt động đáng ngờ.



Hình 7-2 Thàn chú

Nguồn: Course Technology/Cengage Learning

Báo động và Hệ thống báo động Liên quan chặt chẽ đến giám sát là các hệ thống báo động thông báo cho mọi người hoặc hệ thống khi một sự kiện hoặc hoạt động được xác định trước xảy ra. Báo động có thể phát hiện sự xâm nhập vật lý hoặc sự kiện không mong muốn khác. Đây có thể là hỏa hoạn, đột nhập, xáo trộn môi trường như lũ lụt hoặc gián đoạn dịch vụ như mất điện. Một ví dụ về hệ thống báo động là báo trộm thường thấy trong môi trường dân cư và thương mại. Báo động chống trộm phát hiện sự xâm nhập vào các khu vực trái phép và thông báo cho cơ quan an ninh địa phương hoặc từ xa để phản ứng. Để phát hiện sự xâm nhập, các hệ thống này dựa vào một số loại cảm biến khác nhau: máy dò chuyển động, máy dò nhiệt, máy dò kính vỡ, cảm biến trọng lực và cảm biến tiếp xúc. Máy dò chuyển động phát hiện chuyển động trong một không gian hạn chế và hoạt động hoặc thụ động. Một số cảm biến chuyển động phát ra chùm năng lượng, thường ở dạng tia hồng ngoại hoặc ánh sáng laser, âm thanh siêu âm hoặc sóng âm thanh hoặc một số dạng bức xạ điện tử. Nếu năng lượng từ chùm tia chiếu vào khu vực đang được giám sát bị gián đoạn, báo động sẽ được kích hoạt.

Các loại cảm biến chuyển động khác là thụ động ở chỗ chúng liên tục đo năng lượng (hồng ngoại hoặc siêu âm) từ không gian được giám sát và phát hiện những thay đổi nhanh chóng của năng lượng này. Phép đo thụ động của những năng lượng này có thể bị chặn hoặc ngụy trang và do đó có thể sai sót. Máy dò nhiệt đo tốc độ thay đổi nhiệt độ xung quanh trong phòng. Ví dụ, chúng có thể phát hiện khi một người

với nhiệt độ cơ thể là 98,6 độ F bơ ớc vào phòng có nhiệt độ 65 độ F, bởi vì sự hiện diện của ngư ời đó làm thay đổi nhiệt độ xung quanh phòng. Máy dò nhiệt cũng được sử dụng trong phát hiện cháy (như được mô tả trong các phần sau). Cảm biến tiếp xúc và trọng lư ợng hoạt động khi hai tiếp điểm được kết nối, chẳng hạn như khi một bàn chân giẫm lên miếng đệm nhẹ cảm với áp suất dưới tấm thảm hoặc cửa sổ được mở, kích hoạt cảm biến chốt và lò xo. Cảm biến rung cũng thuộc loại này, ngoại trừ việc chúng phát hiện chuyển động của cảm biến hơn là chuyển động trong môi trường.

Phòng máy tính và tủ đấu dây Phòng máy tính và tủ đấu dây và thông tin liên lạc cần được chú ý đặc biệt để đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin. Để biết rõ hơn về các biện pháp kiểm soát vật lý và môi trường cần thiết cho phòng máy tính, hãy đọc hộp Chi tiết kỹ thuật có tiêu đề "Kiểm soát vật lý và môi trường cho phòng máy tính".

Kiểm soát truy cập logic dễ dàng bị đánh bại nếu kẻ tấn công giành được quyền truy cập vật lý vào thiết bị máy tính. Các nhân viên giám sát thường là những nhân viên (hoặc những người không phải là nhân viên) ít được xem xét kỹ lưỡng nhất, những người có quyền truy cập vào các văn phòng của tổ chức. Tuy nhiên, người giám sát được cấp quyền truy cập không giám sát ở mức độ lớn nhất. Họ thường được giao chìa khóa chính cho toàn bộ tòa nhà và sau đó bị phớt lờ, mặc dù họ thu thập giấy tờ từ mọi văn phòng, lau bụi nhiều bàn và di chuyển các thùng chứa lớn từ mọi khu vực. Do đó, không khó để loại công nhân này thu thập thông tin quan trọng và phuơng tiện máy tính hoặc sao chép thông tin độc quyền và thông tin mật.

Tất cả điều này không có nghĩa là nhân viên giám sát của một tổ chức phải thường xuyên bị nghi ngờ là gián điệp, nhưng cần lưu ý rằng quyền truy cập rộng rãi mà người giám sát có thể là một lỗ hổng mà những kẻ tấn công khai thác để lấy thông tin trái phép.

Các tài khoản thực tế tồn tại của các đại lý được đào tạo kỹ thuật làm việc với tư cách là người giám sát trong văn phòng của đối thủ cạnh tranh của họ. Vì vậy, nhân viên lưu ký nên được quản lý cẩn thận không chỉ bởi quản lý chung của tổ chức mà còn bởi quản lý CNTT.

Tư ờng và cửa bên trong Tính bảo mật của tài sản thông tin đôi khi có thể bị ảnh hưởng bởi bản chất của việc xây dựng tư ờng và cửa của cơ sở. Các bức tư ờng trong một cơ sở thường có hai loại: nội thất tiêu chuẩn và tư ờng lửa. Quy tắc xây dựng yêu cầu mỗi tầng phải có một số tư ờng lửa hoặc tư ờng hạn chế thiệt hại lan rộng nếu hỏa hoạn bùng phát trong văn phòng. Trong khi tư ờng lửa mạng được thảo luận trong chương trược cô lập các mạng con hợp lý của tổ chức, thì tư ờng lửa vật lý cô lập không gian vật lý của các văn phòng của tổ chức. Giữa các tư ờng lửa, các bức tư ờng bên trong tiêu chuẩn ngăn cách các văn phòng riêng lẻ. Không giống như tư ờng lửa, những bức tư ờng bên trong này chỉ đến được một phần của tầng tiếp theo, để lại một khoảng trống phía trên trần nhà như bên dưới sàn của tầng tiếp theo. Không gian này được gọi là hội nghị toàn thể, và thư ờng rộng từ 1 đến 3 feet để cho phép lắp đặt các hệ thống thông gió có thể thu hồi không khí từ tất cả các văn phòng trên sàn với chi phí thấp. Tuy nhiên, để đảm bảo an ninh, thiết kế này không lý tưởng, vì nó có nghĩa là một cá nhân có thể trèo qua tư ờng từ văn phòng này sang văn phòng khác. Do đó, tất cả các khu vực có tính bảo mật cao, chẳng hạn như phòng máy tính và tủ nối dây, phải có tư ờng cấp tư ờng lửa bao quanh chúng. Điều này cung cấp bảo mật vật lý không chỉ

từ những kẻ xâm nhập tiềm ẩn, mà còn từ các đám cháy.

Các cửa cho phép vào các phòng có mức độ an ninh cao cũng cần được đánh giá.

Cửa cấp văn phòng tiêu chuẩn cung cấp ít hoặc không có bảo mật. Ví dụ, một trong những tác giả của cuốn sách giáo khoa này đã từng tự khóa mình ở ngoài văn phòng của mình do vô tình làm gãy chìa khóa trong ổ khóa. Khi người thợ khóa đến, anh ta mang theo một cỗ máy lật lùng. Thay vì tháo ổ khóa hoặc triển khai các bí quyết thợ khóa khác, anh ta mang theo một đoạn dây dài chịu lực, uốn cong thành hình cánh cung, với một sợi dây buộc ở mỗi đầu. Anh luồn một đầu của dây cung này qua khe hở một inch dưới cửa, dựng nó lên một đầu và giật mạnh sợi dây. Chiếc nơ dây trượt qua tay nắm cửa và sợi dây quấn quanh nó. Khi người thợ khóa giật mạnh sợi dây, cánh cửa bật mở. (Lưu ý: để xem hoạt động của thiết bị này, hãy truy cập <http://gizmodo.com/5477600/hotel-locks-defeated-by-piece-of-wire-secured-by-knife-or-tire-with-cum>) Thông tin này không nhằm hướng dẫn bạn cách vào các văn phòng bên trong mà để cảnh báo bạn rằng không có văn phòng nào là hoàn toàn an toàn. Làm thế nào bạn có thể tránh được vấn đề này? Trong hầu hết các văn phòng nội thất, bạn không thể. Thay vào đó, các chuyên gia bảo mật CNTT phải giáo dục nhân viên của tổ chức về cách bảo mật thông tin và hệ thống trong văn phòng của họ.

Để có định cửa ra vào, hãy lắp các thanh dây hoặc va chạm vào phòng máy tính và tủ quần áo. Những thanh này khó mở từ bên ngoài hơn nhiều so với tay nắm kéo cửa tiêu chuẩn và do đó cung cấp mức độ bảo mật cao hơn nhiều, như chúng cũng cho phép ra vào an toàn trong trường hợp khẩn cấp.

2.1. Trả lời các câu hỏi: 1. Làm

- thế nào bạn có thể xác định một cơ sở an toàn?
- Tại sao bảo vệ đư ợc coi là hình thức kiểm soát hiệu quả nhất đối với những tình huống đòi hỏi hành động quyết đoán khi đối mặt với những kích thích không quen thuộc?
- Khi nào nên sử dụng chó để bảo vệ thân thể?
- Thẻ căn cước và bảng tên có như ợc điểm gì?
- Tailgating là gì?
- Các biện pháp để ngăn chặn bám đuôi là gì?
- Liệt kê hai loại cơ chế khóa. sự khác biệt giữa chúng là gì?
- Liệt kê và mô tả bốn loại khóa. mỗi người trong hoàn cảnh nào loại khóa ưa thích?
- Hai chế độ khả thi mà khóa sử dụng khi chúng bị lỗi là gì? Gi ý nghĩa của các chế độ này đối với sự an toàn của con người? Trong hoàn cảnh nào mỗi chế độ ưa thích?

10. Bấy giờ chú là gì? Nó nên được sử dụng lúc nào?

11. Như ý điểm của hệ thống giám sát video là gì?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Các biện pháp kiểm soát chống điều chỉnh theo đuôi là các biện pháp phổ biến và hợp lý để triển khai.

A. Đúng

B. Sai

C. NI

2. Chỉ có thể sử dụng chìa khóa là một miếng kim loại được tạo hình cẩn thận để mở một khóa cơ.

A. Đúng

B. Sai

C. NI

3. Khóa thủ công rất phổ biến.

A. Đúng

B. Sai

C. NI

4. Cần có điện để vận hành khóa nút nhấn cơ học.

A. Đúng

B. Sai

C. NI

5. Khóa không an toàn có thể gây ra nhiều nguy hiểm cho mọi người hơn là khóa không an toàn Khóa.

A. Đúng

B. Sai

C. NI

6. CCT là thiết bị giám sát điện tử thư ờng được sử dụng nhất.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1. Thông tin nào KHÔNG được cung cấp trên thẻ căn cước hoặc bảng tên?

A. Địa chỉ của chủ thẻ

B. Hình chủ thẻ

C. Tên chủ thẻ

D. Tòa nhà và khu vực mà chủ thẻ có thể ra vào

2. Loại khóa nào được coi là phức tạp nhất?

A. Khóa cơ điện

B. Khóa sinh trắc học

C. Thẻ thông minh

D. Khóa lập trình được

3. Điều gì KHÔNG được coi là khóa sinh trắc học?

A. Máy quét mống mắt

B. Đầu đọc cọ

C. Đầu đọc giọng nói

D. Đầu đọc tiệm cận

4. Thiết bị báo trộm KHÔNG được tìm thấy ở nơi nào?

A. Trung tâm mua sắm

B. Cửa hàng trang sức

C. Trường đại học

D. Nhà

5. Từ "họ" trong đoạn văn cuối cùng đề cập đến điều gì?

A. thanh đẩy hoặc va

chạm B. phòng máy tính và tủ

quần áo C. tay nắm kéo cửa D.

mức độ an ninh

3. Nói

1. Trình bày hiểu biết của em về các hình thức báo động và nêu ví dụ từ cuộc sống hàng ngày của bạn.

2. Nói về kiểm soát truy cập vật lý mà bạn có thể thêm hoặc cải thiện trong Học viện.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi: 1. Bạn

có thể xác định hệ thống chữa cháy nào trong môi trường xung quanh mình?

2. Liệt kê tất cả các hệ thống phát hiện cháy mà bạn biết.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

An ninh và An toàn Phòng cháy chữa cháy

Mỗi quan tâm bảo mật quan trọng nhất là sự an toàn của những người có mặt trong không gian vật lý của tổ chức-nhân viên, khách hàng, khách hàng và những người khác. Mỗi đe dọa nghiêm trọng nhất đối với sự an toàn đó là hỏa hoạn. Hỏa hoạn gây ra nhiều thiệt hại về tài sản, thươn tích cá nhân và tử vong hơn bất kỳ mối đe dọa nào khác đối với an ninh vật chất. Do đó, điều cấp thiết là các kế hoạch an ninh vật lý phải kiểm tra và thực hiện các biện pháp mạnh mẽ để phát hiện và ứng phó với hỏa hoạn và các nguy cơ hỏa hoạn.

Phát hiện và ứng phó với hỏa hoạn

Hệ thống chữa cháy là các thiết bị được lắp đặt và bảo trì để phát hiện và ứng phó với hỏa hoạn, hỏa hoạn tiềm ẩn hoặc tình huống nguy hiểm do cháy. Các hệ thống này thường hoạt động bằng cách từ chối môi trường một trong ba yếu cầu để ngọn lửa bùng cháy: nhiệt độ (nguồn đánh lửa), nhiên liệu và oxy.

Mặc dù nhiệt độ bắt lửa, hoặc điểm ngọn lửa, phụ thuộc vào vật liệu, nhưng nó có thể thấp tới vài trăm độ. Giấy, chất dễ cháy phổ biến nhất trong văn phòng, có điểm bắt lửa là 451 độ F (một thực tế được sử dụng để tạo hiệu ứng ấn tượng trong tiểu thuyết 451 độ F của Ray Bradbury). Giấy có thể đạt đến nhiệt độ đó khi nó tiếp xúc với một điều thuốc bắt cản làm rơi i, thiết bị điện bị短路 hoặc các hành vi sai trái vô tình hoặc cố ý khác.

Hệ thống nưỚc và sú̄ ơ̄ng mù̄ nưỚc, được mô tả chi tiết trong các đoạn tiếp theo, hoạt động để giảm nhiệt độ của ngọn lửa để dập tắt nó và làm bão hòa một số loại nhiên liệu (chẳng hạn như giấy) để ngăn chặn sự bắt lửa. Hệ thống carbon dioxide (CO₂) cung cấp oxy của lửa. Hệ thống axit soda ngăn chặn ngọn lửa đốt cháy nhiên liệu của nó, ngăn chặn đám cháy lan rộng. Các hệ thống dựa trên khí đốt, chẳng hạn như Halon và các hệ thống thay thế được Cơ quan Bảo vệ Môi trường phê duyệt, làm gián đoạn phản ứng hóa học của đám cháy như ngẫu cung cấp đủ oxy cho mọi người để tồn tại trong một thời gian ngắn.

Tuy nhiên, truỚc khi đám cháy có thể được dập tắt, nó phải được phát hiện.

Phát hiện cháy Các hệ thống phát hiện cháy được chia thành hai loại chung: thủ công và tự động. Các hệ thống phát hiện cháy thủ công bao gồm phản ứng của con người, chẳng hạn như gọi cho sở cứu hỏa, cũng như các báo động được kích hoạt thủ công, chẳng hạn như vòi phun nưỚc

và hệ thống khí. Các tổ chức phải cẩn thận khi báo động đư ợc kích hoạt thủ công đư ợc gắn trực tiếp với hệ thống triệt tiêu, vì báo động sai không phải là hiêm.

Các tổ chức cũng nên đảm bảo rằng an ninh thích hợp vẫn đư ợc duy trì cho đến khi tất cả nhân viên và khách đã rời khỏi tòa nhà và việc sơ tán của họ đã đư ợc xác minh. Trong lúc hỗn loạn của một cuộc sơ tán hỏa hoạn, kẻ tấn công có thể dễ dàng lén vào văn phòng và lấy đư ợc thông tin nhạy cảm. Để giúp ngăn chặn những sự xâm nhập như vậy, các chương trình an toàn phòng cháy chữa cháy thường chỉ định một cá nhân từ mỗi khu vực văn phòng làm nhiệm vụ giám sát sàn.

Có ba loại hệ thống phát hiện cháy cơ bản: phát hiện nhiệt, phát hiện khói và phát hiện ngọn lửa. Các hệ thống phát hiện nhiệt chứa một cảm biến nhiệt tinh vi hoạt động theo một trong hai cách. Cảm biến nhiệt độ cố định phát hiện khi nhiệt độ xung quanh trong một khu vực đạt đến mức định trước, thường là từ 135 độ F đến 165 độ F, hoặc 57 độ C đến 74 độ C. Cảm biến tốc độ tăng phát hiện nhiệt độ khu vực tăng nhanh bất thường trong một khoảng thời gian tương đối ngắn. Trong cả hai trường hợp, nếu các tiêu chí đư ợc đáp ứng, hệ thống báo động và triệt tiêu sẽ đư ợc kích hoạt.

Hệ thống phát hiện nhiệt không tốt kém và dễ bảo trì. Thật không may, máy dò nhiệt thường không bắt đư ợc sự cố cho đến khi nó đang diễn ra, chẳng hạn như trong một đám cháy lớn. Do đó, các hệ thống phát hiện nhiệt không phải là phương tiện phòng cháy chữa cháy đầy đủ ở những khu vực mà sự an toàn của con người có thể gặp rủi ro. Chúng cũng không đư ợc khuyến nghị cho những khu vực có các mặt hàng có giá trị cao hoặc các mặt hàng có thể dễ dàng bị hư hỏng do nhiệt độ cao.

Hệ thống phát hiện khói có lẽ là phương tiện phổ biến nhất để phát hiện đám cháy nguy hiểm tiềm ẩn và chúng đư ợc yêu cầu bởi các quy tắc xây dựng trong hầu hết các khu dân cư và tòa nhà thương mại. Máy dò khói hoạt động theo một trong ba cách. Cảm biến quang điện chiếu và phát hiện chùm tia hồng ngoại trên một khu vực. Nếu chùm tia bị gián đoạn (có lẽ là do khói), hệ thống báo động hoặc triệt tiêu sẽ đư ợc kích hoạt. Cảm biến ion hóa chứa một lưỡng nhỏ chất phóng xạ vô hại trong buồng phát hiện. Khi một số sản phẩm phụ của quá trình đốt cháy đi vào buồng, chúng sẽ thay đổi mức độ dẫn điện trong buồng và kích hoạt máy dò. Các hệ thống cảm biến ion hóa phức tạp hơn nhiều so với cảm biến quang điện và có thể phát hiện đám cháy sớm hơn nhiều, vì các sản phẩm phụ vô hình có thể đư ợc phát hiện từ lâu trước khi đủ vật chất nhìn thấy đư ợc đi vào cảm biến quang điện để kích hoạt phản ứng. Máy dò khí hút là hệ thống tinh vi và đư ợc sử dụng trong các khu vực có độ nhạy cao. Chúng hoạt động bằng cách lấy không khí vào, lọc và di chuyển nó qua một buồng chứa chùm tia laze. Nếu chùm tia laze bị chuyển hướng hoặc khúc xạ bởi các hạt khói, hệ thống sẽ đư ợc kích hoạt.

Các loại hệ thống này thường đắt hơn nhiều so với các hệ thống sử dụng cảm biến quang điện hoặc ion hóa; tuy nhiên, chúng tốt hơn nhiều trong việc phát hiện sớm và thường đư ợc sử dụng ở những khu vực lưu trữ các tài liệu cực kỳ có giá trị.

Loại chính thứ ba của hệ thống phát hiện cháy là đầu báo ngọn lửa. Đầu báo ngọn lửa là một cảm biến phát hiện tia hồng ngoại hoặc tia cực tím đư ợc tạo ra bởi một

ngọn lửa mở. Các hệ thống này so sánh chữ ký ánh sáng của khu vực được quét với cơ sở dữ liệu về chữ ký ánh sáng ngọn lửa đã biết để xác định xem có kích hoạt hệ thống báo động và triệt tiêu hay không. Mặc dù có độ nhạy cao, các hệ thống phát hiện ngọn lửa đắt tiền và phải được lắp đặt ở nơi chúng có thể quét tất cả các khu vực của không gian được bảo vệ. Chúng thường không được sử dụng ở những khu vực có tính mạng con người bị đe dọa; tuy nhiên, chúng khá phù hợp với các khu vực lưu trữ hóa chất, nơi khí thải hóa chất thông thường có thể kích hoạt thiết bị báo khói.

Hệ thống chữa cháy Hệ thống chữa cháy có thể bao gồm các thiết bị di động, thủ công hoặc tự động. Bình chữa cháy xách tay được sử dụng trong nhiều tình huống trong đó ưu tiên ứng dụng dập tắt trực tiếp hoặc thiết bị cố định là không thực tế. Bình chữa cháy xách tay hiệu quả hơn nhiều đối với các đám cháy nhỏ hơn, bởi vì việc kích hoạt hệ thống phun nước của toàn bộ tòa nhà có thể gây ra nhiều thiệt hại.

Bình chữa cháy xách tay được đánh giá theo loại đám cháy mà chúng có thể chống lại, như sau:

- Đám cháy loại A: Những đám cháy liên quan đến nhiên liệu dễ cháy thông thường như gỗ, giấy, hàng dệt, cao su, vải và rác. Đám cháy loại A được dập tắt bởi các tác nhân làm gián đoạn khả năng bắt lửa của nhiên liệu. Bình chữa cháy hóa chất khô đa năng và nước là lý tưởng cho các loại đám cháy này.
- Đám cháy loại B: Những đám cháy gây ra bởi chất lỏng hoặc khí dễ cháy, chẳng hạn như dung môi, xăng, sơn, sơn mài và dầu. Đám cháy loại B được dập tắt bằng các chất loại bỏ oxy khỏi đám cháy. Bình chữa cháy carbon dioxide, hóa chất khô đa năng và Halon là lý tưởng cho các loại đám cháy này.
- Đám cháy loại C: Những đám cháy với thiết bị hoặc dụng cụ điện có điện.

Đám cháy loại C chỉ được dập tắt bằng các chất không dẫn điện. Bình chữa cháy carbon dioxide, hóa chất khô đa năng và Halon là lý tưởng cho các loại đám cháy này. Không bao giờ sử dụng bình chữa cháy bằng nước cho đám cháy loại C.

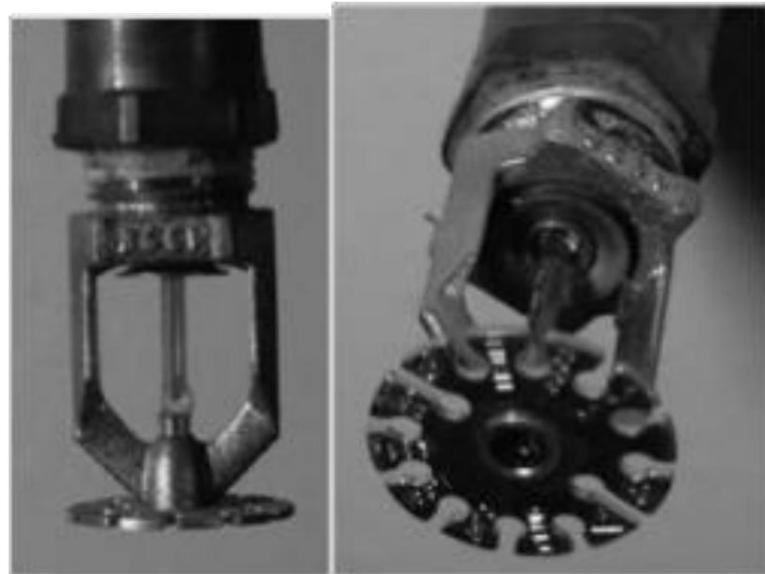
- Đám cháy loại D: Những đám cháy do kim loại dễ cháy, chẳng hạn như magiê, lithium và natri. Đám cháy loại D yêu cầu các chất và kỹ thuật chữa cháy đặc biệt.

Các hệ thống chữa cháy thủ công và tự động bao gồm những hệ thống được thiết kế để áp dụng các chất ức chế. Đây thường là hệ thống phun nước hoặc khí. Tất cả các hệ thống phun nước đều được thiết kế để phun chất lỏng, thường là nước, vào tất cả các khu vực phát hiện đám cháy, như ngỗng chức có thể chọn một trong ba cách triển khai: hệ thống ống ưỚt, ống khô hoặc hệ thống tác động trưỚc. Một hệ thống được ống ưỚt có áp lực nước trong tất cả các đường ống và có một số dạng van ở mỗi khu vực được bảo vệ.

Khi hệ thống được kích hoạt, các van sẽ mở ra, rắc khu vực này. Điều này là tốt nhất cho những khu vực mà hỏa hoạn gây rủi ro nghiêm trọng cho con người, như thiệt hại về tài sản không phải là mối quan tâm lớn. Hạn chế rõ ràng nhất đối với loại hệ thống này là nước làm hư hỏng các thiết bị và vật liệu văn phòng. Hệ thống được ống ưỚt thường không thích hợp trong phòng máy tính, tủ nội dây hoặc bất kỳ nơi nào sử dụng hoặc cất giữ thiết bị điện. Ngoài ra còn có nguy cơ vô tình hoặc kích hoạt trái phép. Hình 8-3 cho thấy một hệ thống phun nước được ống ưỚt được kích hoạt

khi nhiệt độ môi trường đạt từ 140 độ F đến 150 độ F, làm sôi chất lỏng đặc biệt trong ống thủy tinh, làm cho ống bị vỡ và mở van. Khi van mở, nưỚc sẽ chảy qua bộ khuếch tán, giúp phân tán nưỚc ra khắp khu vực.

Hệ thống đưỜng ống khô đưỢc thiết kế để hoạt động ở những khu vực sử dụng thiết bị điện. Thay vì nưỚc, hệ thống chứa không khí điều áp. Không khí giữ các van đóng lại, giữ cho nưỚc tránh xa các khu vực mục tiêu. Khi phát hiện có cháy, các đầu phun Sprinkler đưỢc kích hoạt, khí điều áp thoát ra ngoài, nưỚc lắp đầy các đưỜng ống và thoát ra ngoài qua các đầu Sprinkler. Điều này làm giảm nguy cơ rò rỉ ngẫu nhiên từ hệ thống. Một số hệ thống phun nưỚc, đưỢc gọi là hệ thống xả lũ, luôn mở tất cả các đầu phun nưỚc riêng lẻ và ngay sau khi hệ thống đưỢc kích hoạt, nưỚc sẽ ngay lập tức đưỢc cung cấp cho tất cả các khu vực. Tuy nhiên, đây không phải là giải pháp tối ưu cho môi trường máy tính, vì có những hệ thống khác tinh vi hơn có thể dễ dàng tắt đám cháy mà không làm hỏng thiết bị máy tính.



Hình 7-3 Hệ thống phun nưỚc Nguồn: Course Technology/Cengage Learning

Một biến thể của hệ thống ống khô là hệ thống tác động trực tiếp. Cách tiếp cận này có phản ứng hai giai đoạn đối với đám cháy. Trong điều kiện bình thường, hệ thống không có gì trong các đưỜng ống phân phối. Khi phát hiện đám cháy, giai đoạn đầu tiên đưỢc bắt đầu và các van cho phép nưỚc đi vào hệ thống. Tại thời điểm đó, hệ thống giống như một hệ thống đưỜng ống ướt. Hệ thống xử lý trực tiếp không đưa nưỚc vào không gian đưỢc bảo vệ cho đến khi các đầu phun riêng lẻ đưỢc kích hoạt, lúc đó nưỚc chỉ chảy vào khu vực của đầu phun đưỢc kích hoạt.

Vòi phun sương nưỚc là hình thức mới nhất của hệ thống phun nưỚc và dựa vào sương siêu mịn thay vì hệ thống kiểu vòi hoa sen truyền thống. Hệ thống phun sương nưỚc hoạt động giống như hệ thống nưỚc truyền thống bằng cách giảm nhiệt độ môi trường xung quanh

ngọn lửa, do đó giảm thiểu khả năng duy trì nhiệt độ cần thiết để duy trì sự cháy. Tuy nhiên, không giống như các hệ thống phun nước truyền thống, các hệ thống này tạo ra sự ống mù giống như sự ống mù, vì các giọt nước ít nhạy cảm hơn với trọng lực nên sẽ nổi (trong không khí) lâu hơn nhiều. Kết quả là, một lượng nước nhỏ hơn nhiều được yêu cầu; Ngoài ra, đám cháy được dập tắt nhanh hơn, ít gây ra thiệt hại về tài sản thế chấp hơn. So với các hệ thống khí (sẽ được thảo luận ngay sau đây), các hệ thống gốc nước có chi phí thấp, không độc hại và thường có thể được tạo ra bằng cách sử dụng hệ thống phun nước hiện có có thể đã có trong quá trình xây dựng trước đó.

Kế hoạch an ninh vật lý yêu cầu mọi tòa nhà phải có lối thoát hiểm được đánh dấu rõ ràng và bản đồ được dán khắp cơ sở. Điều quan trọng là phải có các cuộc diễn tập để diễn tập các phản ứng khi có báo cháy và chỉ định các cá nhân chịu trách nhiệm hộ tống mọi người ra khỏi địa điểm và đảm bảo rằng không ai bị bỏ lại phía sau. Điều quan trọng nữa là phải có các hệ thống chữa cháy cả thủ công và tự động, và được kiểm tra và thử nghiệm thường xuyên.

2.1. Trả lời các câu hỏi:

1. Điều gì được coi là mối đe dọa nghiêm trọng nhất trong lĩnh vực thể chất

Bảo vệ? Tại sao nó hợp lệ để coi mối đe dọa này là nghiêm trọng nhất?

2. Làm thế nào để các hệ thống chữa cháy vận dụng ba yếu tố để chữa cháy
để dốt cháy?

3. Điểm ngọn lửa là gì? Trong trường hợp nào giấy có thể đạt đến điểm cháy của nó?

4. Vai trò của giám sát sàn là gì?

5. Liệt kê và mô tả ba công nghệ phát hiện cháy được đề cập trong chương này.

Cái nào hiện nay được sử dụng phổ biến nhất?

6. Liệt kê ba cách thức hoạt động của máy dò khói. Loại nào nhiều nhất
đắt tiền?

7. Liệt kê và mô tả bốn loại lửa được mô tả trong văn bản. Liệu

lớp của một đám cháy ra lệnh làm thế nào để kiểm soát đám cháy?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không thông tin (NI)

1. Hỏa hoạn là mối nguy hiểm phổ biến nhất đối với sự an toàn của con người trong không
gian vật lý của tổ chức.

A. Đúng

B. Sai

C. NI

2. Cảm biến ion hóa thường được tìm thấy ở những nơi có giá trị cao
vật liệu được lưu trữ.

A. Đúng B. Sai C. NI

3. Đầu báo lửa thư ờng đư ợc lắp đặt ở những khu vực đông dân cư .

A. Đúng B. Sai C. NI

4. Phư ơng tiện chữa cháy phù hợp với các đám cháy nhỏ là bình chữa cháy xách tay.

A. Đúng B. Sai C. NI

5. Hệ thống chữa cháy trong mọi tòa nhà cần đư ợc kiểm tra, thử nghiệm mỗi năm.

A. Đúng B. Sai C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1. Điều gì KHÔNG phải là một trong các yếu tố phải có để ngọn lửa bùng cháy và tiếp tục cháy?

- A. oxi
- B. khí cacbonic
- C. nhiệt độ

D. nhiên liệu

2. Cái nào sau đây KHÔNG phải là hệ thống chữa cháy?

- A. Hệ thống axit xút
- B. Hệ thống chạy bằng khí
- C. Hệ thống phun sương nư ớc
- D. Hệ thống phát hiện thủ công

3. Cái nào sau đây KHÔNG phải là hệ thống phát hiện cháy thủ công?

- A. phản ứng của con ngư ời
- B. hệ thống tự động
- C. vòi phun nư ớc
- D. hệ thống khí

4. Trong ba hệ thống phát hiện khói này, hệ thống nào phát hiện cháy sớm tốt nhất phát hiện?

- A. Máy dò khí hút
- B. Cảm biến ion hóa

- C. Cảm biến quang điện
 - D. Chúng giống nhau
5. Từ "it" ở dòng 11, đoạn 3 ám chỉ điều gì?
- A. nhiệt độ đánh lửa
 - B. giấy
 - C. vật liệu
 - D. Không câu nào đúng

3. Nói

1. Trình bày về hệ thống chữa cháy đang được sử dụng trong các tòa nhà mà bạn biết. Tại sao hệ thống cụ thể đó được chọn cho điều đó

định nghĩa bài văn?

ĐỌC VÀ NÓI 3

1. Thảo luận các câu hỏi: 1.

Bạn có nghĩ rằng các tiện ích hỗ trợ như sưởi ấm, thông gió, điều hòa không khí và hệ thống điện có thể ảnh hưởng đến an ninh vật chất của một tổ chức không?

2. Làm thế nào nó có thể xảy ra? Đưa ra những ví dụ thực tế mà bạn biết.

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Sự thất bại của các tiện ích hỗ trợ và sự sụp đổ về cấu trúc Các tiện ích hỗ trợ, chẳng hạn như sưởi ấm, thông gió và điều hòa không khí, điện, nước và các tiện ích khác, có tác động đáng kể đến hoạt động an toàn của một cơ sở. Nhiệt độ và độ ẩm quá cao, biến động điện và gián đoạn dịch vụ nước, nước thải và rác thải có thể tạo ra các điều kiện gây ra các lỗ hổng trong các hệ thống được thiết kế để bảo vệ thông tin. Do đó, mỗi tiện ích này phải được quản lý đúng cách để ngăn ngừa thiệt hại cho thông tin và hệ thống thông tin.

Hệ thống sưởi, thông gió và điều hòa không khí

Mặc dù theo truyền thống là trách nhiệm quản lý cơ sở, hoạt động của hệ thống sưởi ấm, thông gió và điều hòa không khí (HVAC) có thể có tác động đáng kể đến hoạt động và bảo vệ hệ thống thông tin và thông tin.

Cụ thể, các biện pháp kiểm soát nhiệt độ, lọc, độ ẩm và tinh điện phải được theo dõi và điều chỉnh để giảm thiểu rủi ro đối với hệ thống thông tin.

Nhiệt độ và Lọc Các hệ thống máy tính là điện tử, và do đó có thể bị hư hại do nhiệt độ quá cao và ô nhiễm dạng hạt.

Nhiệt độ thấp tới 100 độ F có thể làm hỏng phuơng tiện máy tính và ở nhiệt độ 175 độ F, phần cứng máy tính có thể bị hỏng hoặc phá hủy. Khi nhiệt độ lên tới 32 độ F, phuơng tiện dễ bị nứt và các thành phần máy tính thực sự có thể đóng băng cùng nhau. Những thay đổi nhanh về nhiệt độ, từ nóng sang lạnh hoặc từ lạnh sang nóng, có thể tạo ra sự ngưng tụ, có thể tạo ra đoán mạch hoặc làm hỏng các hệ thống và linh kiện. Nhiệt độ tối ưu cho môi trường máy tính (và cho con người) là từ 70 đến 74 độ F. Các hệ thống được lắp đặt và bảo trì đúng cách sẽ giữ cho môi trường trong phạm vi nhiệt độ do nhà sản xuất khuyến nghị. Trước đây, người ta cho rằng cần phải lọc hoàn toàn tất cả các hạt từ luồng không khí từ hệ thống HVAC. Thiết bị máy tính hiện đại được thiết kế để hoạt động tốt hơn trong môi trường văn phòng điển hình, và do đó, nhu cầu cung cấp hệ thống lọc rộng rãi cho điều hòa không khí hiện chỉ giới hạn ở những môi trường đặc biệt nhạy cảm như khu vực chế tạo chip và lắp ráp linh kiện. Nói cách khác, lọc không còn là một yếu tố quan trọng như trước đây đối với hầu hết các cơ sở xử lý dữ liệu thương mại.

Độ ẩm và tĩnh điện Độ ẩm là lượng ẩm trong không khí.

Độ ẩm cao tạo ra các ván đề nguy hiểm và độ ẩm thấp có thể làm tăng lượng tĩnh điện trong môi trường. Cùng với sự nguy hiểm hơn mức, thiết bị điện sẽ bị ngắn mạch và có khả năng bị mốc và thối trong kho lưu trữ thông tin trên giấy. Tĩnh điện được gây ra bởi một quá trình gọi là điện hóa ma sát, xảy ra khi hai vật liệu tiếp xúc và trao đổi electron, dẫn đến một vật trở nên tích điện dương hơn và vật kia tích điện âm hơn. Khi gặp một vật thứ ba có điện tích trái dấu hoặc chạm đất, các electron lại chảy và tia lửa điện được tạo ra.

Một trong những nguyên nhân hàng đầu gây hư hỏng mạch điện nhạy cảm là hiện tượng phóng tĩnh điện (ESD). Các mạch tích hợp trong máy tính được thiết kế để sử dụng điện từ hai đến năm volt; bất kỳ mức điện áp nào trên phạm vi này đều có nguy cơ làm hỏng vi mạch. Con người thậm chí không nhận thấy tĩnh điện cho đến khi đạt mức 1.500 volt và không thể nhìn thấy tia lửa cho đến khi mức đạt gần 4.000 volt. Hơn nữa, một người có thể tạo ra dòng điện tĩnh lên tới 12.000 volt chỉ bằng cách đi ngang qua một tấm thảm.

Nói chung, thiệt hại ESD đối với chip tạo ra hai loại lỗi. Lỗi tức thời, còn được gọi là lỗi nghiêm trọng, xảy ra ngay lập tức, thường phá hủy hoàn toàn và yêu cầu thay thế chip. Lỗi tiềm ẩn hoặc lỗi chậm có thể xảy ra vài tuần hoặc thậm chí vài tháng sau khi hư hỏng xảy ra. Thiệt hại có thể không đáng chú ý, như ng chip có thể gặp sự cố không liên tục. (Tuy nhiên, người ta đã quan sát thấy rằng với chất lượng tổng thể kém của một số hệ điều hành phổ biến hiện nay, loại hư hỏng này có thể khó nhận thấy.) Do đó, bắt buộc phải duy trì mức độ ẩm tối ưu, trong đó là từ 40 phần trăm đến 60 phần trăm, trong môi trường điện toán.

Volts	Results
40	High probability of damage to sensitive circuits and transistors
1,000	Scrambles monitor display
1,500	Can cause disk drive data loss
2,000	High probability of system shutdown
4,000	May jam printers
17,000	Causes certain and permanent damage to almost all microcircuitry

Bảng 7-1 Hư hỏng tĩnh điện trong máy tính

Các mức độ âm dư ới phạm vi này tạo ra tĩnh và các mức trên tạo ra sự ngưng tụ. Hệ thống làm ấm hoặc hút ấm có thể điều chỉnh mức độ ấm.

Trục thông gió Trong khi hệ thống ống gió trong các tòa nhà dân cư khá nhỏ, thì trong các tòa nhà thương mại lớn, nó có thể đủ lớn để một người trèo qua.

Đây là một trong những phương pháp yêu thích của Hollywood để nhân vật phản diện hoặc anh hùng xâm nhập vào các tòa nhà, nhưng những trục thông gió này không hoàn toàn dễ thương lừa lọc như trong phim mà bạn vẫn tin. Trên thực tế, với các biện pháp phòng ngừa bảo mật vừa phải, các trục này có thể được loại bỏ hoàn toàn dư ới dạng lỗ hỏng bảo mật. Trong hầu hết các tòa nhà mới, các ống dẫn đến các phòng riêng lẻ có đường kính không lớn hơn 12 inch và là các ống mềm dẻo, cách nhiệt. Kích thước và tính chất của các ống dẫn ngăn cản hầu hết mọi người sử dụng chúng, nhưng có thể truy cập thông qua hội nghị toàn thể. Nếu các ống dẫn lớn hơn nhiều, nhóm an ninh có thể lắp đặt lư ới thép tại các điểm khác nhau để phân chia các đường chạy.

Quản lý và điều hòa năng lượng Năng lượng điện là một khía cạnh khác của môi trường vật chất của tổ chức thương mại xem xét trong lĩnh vực an ninh vật lý. Điều quan trọng là các hệ thống điện được sử dụng bởi thiết bị xử lý thông tin phải được lắp đặt đúng cách và nối đất chính xác. Sự can thiệp vào mô hình bình thường của dòng điện được gọi là tiếng ồn. Bởi vì máy tính đôi khi sử dụng chu kỳ 60 Hertz bình thường của điện trong dòng điện xoay chiều để đồng bộ hóa đồng hồ của chúng, tiếng ồn cảm trở chu kỳ này có thể dẫn đến đồng hồ thời gian không chính xác hoặc thậm chí tệ hơn là đồng hồ nội bộ không đáng tin cậy bên trong CPU.

Nối đất và cương độ dòng điện Nối đất đảm bảo rằng dòng điện quay trở lại được xả đúng cách xuống đất. Nếu các bộ phận tiếp đất của hệ thống điện không được lắp đặt đúng cách, bất kỳ ai chạm vào máy tính hoặc thiết bị điện khác đều có thể trở thành nguồn tiếp đất, điều này sẽ gây hư hỏng cho thiết bị và gây thương tích hoặc tử vong cho người đó. Máy tính và các thiết bị điện khác ở những khu vực có thể tích tụ nư ớc phải được nối đất riêng, sử dụng thiết bị ngắt mạch sự cố nối đất (GFCI). GFCI có khả năng xác định và ngắt nhanh chóng sự cố chạm đất-tức là tình huống trong đó một người tiếp xúc với nư ớc và tiếp đất tốt hơn so với nguồn hiện tại của mạch điện.

Nguồn điện cũng cần được cung cấp đủ cương độ để hỗ trợ các hoạt động cần thiết. Không có gì khó chịu hơn là cắm vào hàng loạt máy tính, chỉ để ngắt cầu dao. Tham khảo ý kiến của thợ điện có trình độ khi thiết kế hoặc tu sửa phòng máy tính để đảm bảo có sẵn các mạch cương độ dòng điện đủ cao để cung cấp nguồn điện cần thiết. Việc làm quá tải một mạch điện không chỉ làm ngắt cầu dao mà còn có thể tạo ra tải trọng trên cáp điện vươn quá tải trọng mà cáp được định mức chịu được, do đó làm tăng nguy cơ quá nhiệt và gây cháy.

Nguồn cung cấp điện liên tục (UPS) Nguồn điện chính cho một

thiết bị máy tính của tổ chức thư ờng là tiện ích điện phục vụ khu vực có các tòa nhà của tổ chức. Nguồn năng lượng này có thể bị gián đoạn. Do đó, các tổ chức nên xác định các hệ thống máy tính quan trọng đối với hoạt động của họ (nói cách khác, các hệ thống phải tiếp tục hoạt động trong thời gian bị gián đoạn) và đảm bảo rằng các hệ thống đó được kết nối với một thiết bị đảm bảo cung cấp điện mà không bị gián đoạn—rằng là, một nguồn cung cấp điện liên tục (UPS).

Công suất của các thiết bị UPS được đo bằng cách sử dụng định mức công suất đầu ra volt-ampere (hoặc VA). Các thiết bị UPS thư ờng chạy tới 1.000 VA và có thể được thiết kế để vượt quá 10.000 VA. Một PC thông thường có thể sử dụng 200 VA và một máy chủ trong phòng máy tính có thể cần 2.000 đến 5.000 VA, tùy thuộc vào thời gian chạy cần thiết. [Hình 7-4](#) cho thấy một số loại UPS. Phần này mô tả các cấu hình cơ bản sau: chế độ chờ, tương tác trực tuyến, chế độ chờ kết hợp trực tuyến, chế độ chờ-ferro, chuyển đổi kép trực tuyến (còn được gọi là trực tuyến thực) và chuyển đổi delta trực tuyến.

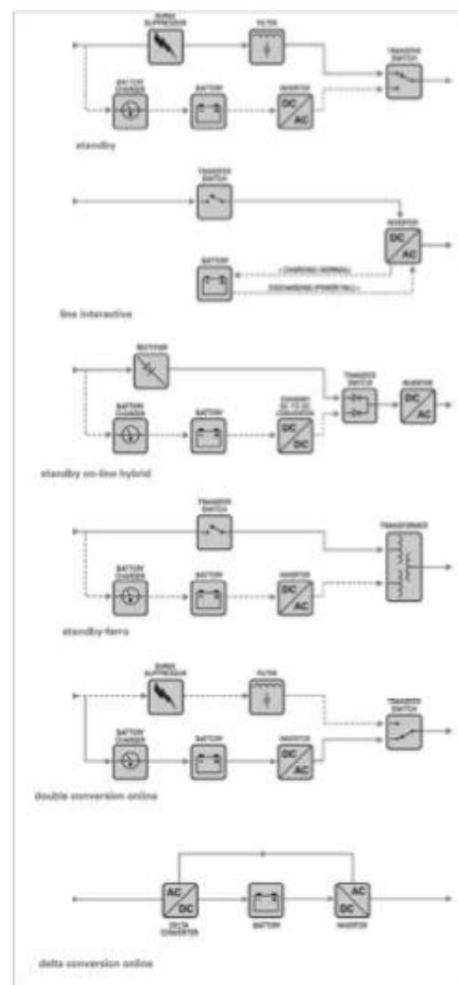
UPS dự phòng hoặc ngoại tuyến là một pin dự phòng ngoại tuyến giúp phát hiện sự gián đoạn nguồn điện cho thiết bị và kích hoạt công tắc chuyển cung cấp nguồn điện từắc quy, thông qua bộ chuyển đổi DC sang AC, cho đến khi nguồn điện được khôi phục hoặc máy tính bị tắt. Bởi vì loại UPS này không thực sự liên tục nên nó thư ờng được gọi là nguồn điện dự phòng (SPS). Ưu điểm của SPS là đây là loại UPS tiết kiệm chi phí nhất. Tuy nhiên, những hạn chế đáng kể, chẳng hạn như thời gian chạy hạn chế và lượng thời gian cần thiết để chuyển từ chế độ chờ sang hoạt động, có thể lớn hơn khoản tiết kiệm chi phí. Thời gian chuyển đổi cũng có thể trở thành một vấn đề vì thiết bị điện toán rất nhạy cảm có thể không xử lý được độ trễ chuyển và có thể đặt lại và bị mất hoặc hỏng dữ liệu. Ngoài ra, các hệ thống SPS không cung cấp khả năng điều hòa năng lượng, một tính năng của các UPS tinh vi hơn (thảo luận bên dưới). Do đó, SPS hiếm khi được sử dụng trong các ứng dụng điện toán quan trọng và phù hợp nhất cho việc sử dụng tại nhà và văn phòng nhẹ.

UPS dự phòng cộng hưởng ferro cải tiến dựa trên thiết kế của UPS dự phòng. Nó vẫn là một UPS ngoại tuyến, với dịch vụ điện cung cấp nguồn điện chính và UPS đóng vai trò là pin dự phòng. Sự khác biệt chính là một máy biến áp cộng hưởng sắt thay thế công tắc chuyển UPS. Máy biến áp cung cấp khả năng lọc đường dây cho nguồn điện chính, giảm ảnh hưởng của một số sự cố về điện và giảm tiếng ồn có thể có trong nguồn điện khi nó được cung cấp.

Máy biến áp này cũng lưu trữ năng lượng trong các cuộn dây của nó, do đó cung cấp một bộ đệm để lấp đầy khoảng trống giữa việc gián đoạn dịch vụ và kích hoạt nguồn điện thay thế (thư ờng là pin dự phòng). Điều này làm giảm đáng kể khả năng thiết lập lại hệ thống và mất dữ liệu. Các hệ thống UPS dự phòng cộng hưởng Ferro phù hợp hơn với các cài đặt yêu cầu công suất lớn của nguồn điện điều hòa và đáng tin cậy, vì chúng có sẵn để sử dụng lên đến 14.000 VA. Tuy nhiên, với sự cải tiến trong các thiết kế UPS khác, nhiều nhà sản xuất đã từ bỏ thiết kế này để chuyển sang các cấu hình khác.

UPS tư ơng tác trực tuyến có thiết kế khác biệt đáng kể so với các mẫu UPS đã đề cập trước đó. Trong các UPS tư ơng tác trực tuyến, các thành phần bên trong của các kiểu dự phòng được thay thế bằng một cặp bộ biến tần và bộ chuyển đổi. Nguồn năng lượng chính, như trong cả SPS và UPS cộng hưởng sắt, vẫn là của công ty điện lực, với pin đóng vai trò dự phòng. Tuy nhiên, bộ biến tần và bộ chuyển đổi đều sạc pin và cung cấp năng lượng khi cần thiết. Khi nguồn điện bị gián đoạn, bộ chuyển đổi bắt đầu cung cấp điện cho hệ thống. Bởi vì thiết bị này luôn được kết nối với đầu ra thay vì phụ thuộc vào công tắc, kiểu máy này có thời gian phản hồi nhanh hơn nhiều, đồng thời cũng tích hợp điều hòa nguồn và lọc dòng.

Trong một UPS trực tuyến thực sự, nguồn năng lượng chính là ắc quy và nguồn cấp điện từ tiện ích liên tục sạc lại ắc quy này. Mô hình này cho phép sử dụng hệ thống liên tục, đồng thời loại bỏ hoàn toàn dao động điện năng. UPS trực tuyến thực sự có thể cung cấp dòng điện liên tục, trơn tru, có điều kiện cho các hệ thống máy tính. Nếu nguồn điện do tiện ích cung cấp bị hỏng, hệ thống máy tính sẽ không bị ảnh hưởng miễn là hết pin. UPS trực tuyến được coi là tùy chọn hàng đầu và đắt nhất. Hạn chế lớn duy nhất, ngoài chi phí, là quá trình



Hình 7-4 Các loại nguồn điện liên tục

Nguồn: Courtesy of American Power Conversion Corporation

liên tục chuyển đổi từ nguồn cấp AC từ tiện ích sang DC đư ợc sử dụng bởi bộ lưu trữ pin và sau đó chuyển đổi ngược lại thành AC để hệ thống sử dụng sẽ tạo ra rất nhiều nhiệt. Một mô hình cải tiến giải quyết vấn đề này bằng cách kết hợp một thiết bị đư ợc gọi là bộ chuyển đổi delta, cho phép một phần năng lư ợng đầu vào đư ợc cung cấp trực tiếp cho máy tính đích, do đó giảm lư ợng năng lư ợng lãng phí và nhiệt sinh ra. Nếu mất điện, thiết bị delta sẽ tắt và pin sẽ tự động bù cho mức tiêu thụ năng lư ợng tăng lên.

Chọn UPS tốt nhất có thể là một bài học về kỹ thuật điện, bởi vì bạn phải tính toán tải mà hệ thống đư ợc bảo vệ yêu cầu từ UPS. Điều này có thể khá phức tạp và tỏ ra khó khăn trong thực tế. May mắn thay, nhiều nhà cung cấp UPS cung cấp các tình huống mẫu có thể giúp bạn chọn thiết bị tối ưu. Vì một UPS chất lư ợng cao có thể có giá vài nghìn đô la nên bạn nên chọn UPS nhỏ nhất cần thiết để mang lại hiệu quả mong muốn. Để tính toán thủ công xếp hạng cần thiết trong UPS, bạn nên bắt đầu bằng cách xem xét các hệ thống máy tính và tất cả các thiết bị hỗ trợ đư ợc kết nối để đư ợc bảo vệ. Ví dụ: mặt sau của màn hình có thể cho biết màn hình đư ợc định mức ở mức 110 volt và 2 ampe. Vì volt nhân với ampe mang lại nhu cầu năng lư ợng của một thiết bị, nên để tính toán năng lư ợng bạn cần để chạy thiết bị này, bạn nhân 110 với 2; việc tạo ra phuơng trình này là định mức của màn hình, 220 VA. Nay giờ, giả sử máy tính sử dụng 3 ampe ở 110 volt và do đó có định mức là 330 VA. Tổng cộng là 550 VA. Sau khi có thông tin này, bạn có thể chọn một UPS có khả năng hỗ trợ mức công suất này.

Nói chung, các hệ thống UPS cung cấp thông tin về thời gian chúng sẽ chạy ở các mức VA cụ thể. Một số UPS quy mô nhỏ hơn có thể chạy trong khoảng sáu phút ở 600 VA ở điện áp đầy đủ. Bạn nên tìm một UPS cung cấp đủ thời gian để thiết bị máy tính vư ợt qua các dao động điện nhỏ và để người dùng tắt máy tính một cách an toàn nếu cần.

Ngắt khẩn cấp

Một khía cạnh quan trọng của quản lý điện năng trong bất kỳ môi trường nào là khả năng ngắt điện ngay lập tức nếu dòng điện gây rủi ro cho sự an toàn của con người hoặc máy móc. Hầu hết các phòng máy tính và tủ nối dây đều đư ợc trang bị nút ngắt điện khẩn cấp, thường là một nút lớn màu đỏ đư ợc đặt ở vị trí nổi bật để thuận tiện cho việc tiếp cận và có nắp đậy để ngăn việc sử dụng ngoài ý muốn. Các thiết bị này là tuyên phòng thủ cuối cùng chống lại thường tích cá nhân và hư hỏng máy móc trong trường hợp lũ lụt hoặc kích hoạt vòi phun nưỚc. Người cuối cùng ra khỏi phòng máy tính nhấn công tắc để ngăn dòng điện vào phòng, ngăn nưỚc có thể dùng để dập lửa làm chập mạch máy tính. Mặc dù không bao giờ nên để nưỚc tiếp xúc với máy tính, như ng khả năng khôi phục hệ thống sẽ cao hơn nhiều nếu chúng không đư ợc khởi động khi bị ướt. Ở mức tối thiểu, ổ đĩa cứng và các thiết bị niêm phong khác có thể phục hồi đư ợc. Một số công ty khắc phục thảm họa chuyên về khắc phục thiệt hại do nưỚc.

vấn đề về nư ớc

Một yếu tố cơ sở hạ tầng tiện ích quan trọng khác là dịch vụ nư ớc. Một mặt, thiếu nư ớc gây ra các vấn đề cho các hệ thống, bao gồm cả hệ thống chữa cháy và điều hòa không khí. Mặt khác, lư ợng nư ớc dư thừa hoặc áp lực nư ớc đặt ra một mối đe dọa thực sự. Lũ lụt, rò rỉ và sự hiện diện của nư ớc ở những nơi không nên có là thảm họa đối với việc lưu trữ thông tin trên giấy và điện tử. Thiệt hại do nư ớc có thể dẫn đến sự cố hoàn toàn của hệ thống máy tính và cấu trúc chứa chúng. Do đó, điều quan trọng là phải tích hợp các hệ thống phát hiện nư ớc vào các hệ thống báo động để điều chỉnh các hoạt động tổng thể của cơ sở.

sụp đổ cấu trúc

Các yếu tố môi trường không thể tránh khỏi hoặc các lực lư ợng tự nhiên có thể gây ra sự cố trong các cấu trúc chứa đựng tổ chức. Các công trình được thiết kế và xây dựng với các giới hạn tải trọng cụ thể, và việc quá tải các giới hạn thiết kế này chắc chắn sẽ dẫn đến hư hỏng công trình. Thư ơng tích cá nhân và khả năng mất mạng cũng có thể xảy ra. Lập kế hoạch kiểm tra định kỳ bởi các kỹ sư xây dựng có trình độ sẽ cho phép các nhà quản lý xác định các điều kiện cấu trúc nguy hiểm tiềm ẩn trư ớc khi cấu trúc bị hỏng.

Bảo trì hệ thống cơ sở

Cũng giống như bất kỳ giai đoạn nào của quy trình bảo mật, việc triển khai giai đoạn bảo mật vật lý phải được ghi lại, đánh giá và kiểm tra liên tục; một khi an ninh vật lý của một cơ sở được thiết lập, nó phải được duy trì cẩn thận.

Việc bảo trì hệ thống liên tục được yêu cầu như là một phần của hoạt động của hệ thống. Tài liệu về cấu hình, hoạt động và chức năng của cơ sở nên được tích hợp vào kế hoạch khắc phục thảm họa và quy trình vận hành tiêu chuẩn. Thủ nghiệm cung cấp thông tin cần thiết để cải thiện an ninh vật lý trong cơ sở và xác định các điểm yếu.

2.1. Trả lời các câu hỏi:

1. Bốn đặc điểm vật lý nào của môi trường trong nhà là được điều khiển bởi một hệ thống HVAC được thiết kế phù hợp?
2. Phạm vi nhiệt độ và độ ẩm tối ưu cho máy tính là gì hệ thống?
3. Tại sao lọc không khí KHÔNG còn quan trọng như trư ớc đây?
4. Nguyên nhân của vấn đề ngưng tụ là gì? Hậu quả nào có thể kết quả từ chúng?
5. Người ta dùng gì để điều chỉnh độ ẩm?
6. Tại sao việc lắp đặt đúng cách các bộ phận nối đất của hệ thống điện lại quan trọng?

7. Quá tải mạch dẫn đến hậu quả gì?
8. Vai trò của UPS là gì?
9. Tại sao cần phải ngắt điện khẩn cấp, đặc biệt là trong phòng máy tính và tủ nối dây?
10. Hai chức năng quan trọng nào bị suy giảm khi không có nút trong một cơ sở?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Ngày nay, kiểm soát nhiệt độ là yếu tố quan trọng để bảo vệ hầu hết cơ sở xử lý dữ liệu thương mại.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Ngày nay, lọc rỗng rãnh cho điều hòa không khí là điều bắt buộc nếu bạn muốn để duy trì một môi trường tối ưu cho hầu hết các xử lý dữ liệu thương mại cơ sở.

A. Đúng	B. Sai	C. NI
---------	--------	-------
3. Dòng điện mồi vôn có thể gây hại cho vi mạch.

A. Đúng	B. Sai	C. NI
---------	--------	-------
4. Các trực thông gió thường được kẻ tần công sử dụng để đột nhập tòa nhà thương mại ngày nay.

A. Đúng	B. Sai	C. NI
---------	--------	-------
5. Thiếu nút và thừa nút đều có thể làm hỏng máy tính các hệ thống.

A. Đúng	B. Sai	C. NI
---------	--------	-------

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau

1. Nhiệt độ nào sau đây là thích hợp nhất cho máy tính?

A. 30 độ F	B. 73 độ F	C. 170 độ F
------------	------------	-------------
2. UPS nào phù hợp sử dụng cho nhà ở thông thường?

D. 103 độ F

- A. UPS trực tuyến đích thực
- B. UPS ngoại tuyến
- C. UPS dự phòng cộng hưởng Ferro
- D. UPS tư duy tác động trực tuyến

3. Nơi nào sau đây thường KHÔNG có nguồn điện dự phòng

được sử dụng?

- A. các ứng dụng điện toán quan trọng
- B. nhà
- văn phòng C.
- D. trường học

4. Vấn đề nào sau đây KHÔNG phải là vấn đề về nút ớc?

- A. Thiếu nút ớc
- B. Nút ớc bị ô nhiễm
- C. Lũ lụt
- D. Rò rỉ

5. Hệ thống nào sẽ bị ảnh hưởng trực tiếp nếu lưu lượng nút ớc không đủ?

- A. hệ thống báo động
- B. hệ thống phát hiện nút ớc
- C. hệ thống điều hòa không khí
- D. hệ thống điện

3. Nói

1. Trình bày hiểu biết của bạn về 4 loại UPS chính các hệ thống. Cái nào hiệu quả nhất và đắt nhất, và tại sao?

ĐỌC THÊM

Đánh chặn dữ liệu Có

ba phư ơng pháp đánh chặn dữ liệu: quan sát trực tiếp, đánh chặn truyền dữ liệu và đánh chặn điện từ. Phư ơng pháp đầu tiên, quan sát trực tiếp, yêu cầu một cá nhân ở đầu gần thông tin để vi phạm tính bảo mật. Các cơ chế bảo mật vật lý được mô tả trong các phần trước hạn chế khả năng một cá nhân truy cập vào các khu vực trái phép và trực tiếp quan sát thông tin. Tuy nhiên, có rủi ro khi thông tin bị xóa khỏi cơ sở được bảo vệ. Nếu một nhân viên đang duyệt tài liệu trong bữa trưa tại nhà hàng hoặc làm việc về nhà, nguy cơ bị quan sát trực tiếp sẽ tăng lên đáng kể. Một đối thủ cạnh tranh có thể dễ dàng chặn thông tin quan trọng tại nhà của một nhân viên thông thường hơn là tại một văn phòng an toàn. Có thể tránh được các trường hợp bị chặn, chẳng hạn như lười vui, nếu nhân viên bị cấm xóa thông tin nhạy cảm khỏi văn phòng hoặc được yêu cầu thực hiện an ninh chặt chẽ tại nhà của họ.

Phư ơng pháp thứ hai, chặn truyền dữ liệu, đã trở nên dễ dàng hơn trong thời đại Internet. Nếu kẻ tấn công có thể truy cập vào phư ơng tiện truyền dữ liệu, thì chúng không cần phải ở gần nguồn thông tin. Trong một số trường hợp, kẻ tấn công có thể sử dụng phần mềm nghe lén, đã được mô tả trong các chương trước, để thu thập dữ liệu. Các phư ơng tiện đánh chặn khác, chẳng hạn như xâm nhập vào mạng LAN, yêu cầu một số khoảng cách gần với máy tính hoặc mạng của tổ chức. Điều quan trọng là các quản trị viên mạng phải tiến hành kiểm tra thực tế định kỳ tất cả các cổng dữ liệu để đảm bảo rằng không có hành vi xâm nhập trái phép nào xảy ra. Nếu việc nghe lén trực tiếp là mối lo ngại, tổ chức nên cân nhắc sử dụng cáp quang, vì khó nói vào loại cáp này khiến nó có khả năng chống nghe lén cao hơn nhiều. Nếu mạng LAN không dây được sử dụng, tổ chức nên quan tâm đến việc nghe trộm, vì kẻ tấn công có thể rình mò từ một vị trí có thể-tùy thuộc vào độ mạnh của các điểm truy cập không dây (WAP)-cách hàng trăm feet bên ngoài tòa nhà của tổ chức. Do các mạng LAN không dây đặc biệt dễ bị nghe lén và các trình nghe trộm không dây thế hệ hiện tại là những công cụ rất mạnh, nên tất cả các giao tiếp không dây phải được bảo mật thông qua mã hóa. Ngẫu nhiên, bạn có thể quan tâm khi biết rằng luật liên bang của Hoa Kỳ liên quan đến việc nghe lén không bao gồm các liên lạc không dây, ngoại trừ các cuộc gọi điện thoại di động thương mại; tòa án đã phán quyết rằng người dùng không có kỳ vọng về quyền riêng tư với phư ơng tiện liên lạc dựa trên đài phát thanh.

Phư ơng pháp chặn dữ liệu thứ ba, chặn điện từ, nghe có vẻ giống như một tập phim Star Trek . Trong nhiều thập kỷ, các nhà khoa học đã biết rằng dòng điện di chuyển qua dây cáp phát ra tín hiệu điện từ (EM). Có thể nghe lén các tín hiệu này và do đó xác định dữ liệu được truyền trên cáp mà không thực sự chạm vào chúng. Năm 1985, các nhà khoa học đã chứng minh rằng màn hình máy tính cũng phát ra sóng vô tuyến và hình ảnh trên màn hình có thể được tái tạo từ những tín hiệu này. Gần đây hơn, các nhà khoa học đã

đã xác định rằng một số thiết bị nhất định có màn hình LED thực sự phát ra thông tin đư ợc mã hóa dưới dạng ánh sáng phát xung trong các đèn LED này.

Liệu các thiết bị phát ra bức xạ điện từ (EMR) có thực sự đư ợc theo dõi sao cho dữ liệu đang đư ợc xử lý hoặc hiển thị có thể đư ợc tái tạo lại hay không đã là một chủ đề tranh luận (và tin đồn) trong nhiều năm. James Atkinson, một kỹ sư điện tử đư ợc Cơ quan An ninh Quốc gia (NSA) chứng nhận, nói rằng không có cái gọi là giám sát thực tế các bức xạ điện tử và tuyên bố rằng những câu chuyện về giám sát như vậy chỉ là truyền thuyết đô thị. Anh ấy tiếp tục nói rằng hầu hết các máy tính hiện đại đều đư ợc che chắn để tránh gây nhiễu cho các thiết bị gia đình và văn phòng khác–chứ không phải để ngăn chặn việc nghe trộm. Atkinson thừa nhận rằng việc nhận tín hiệu từ màn hình máy tính về mặt lý thuyết là có thể, nhưng lưu ý rằng đó sẽ là một công việc cực kỳ khó khăn, tốn kém và không thực tế.

Truyền thuyết hay không, chính phủ và quân đội đã chi rất nhiều tiền để bảo vệ máy tính khỏi bị nghe lén điện tử từ xa. Trên thực tế, chính phủ Hoa Kỳ đã phát triển một chương trình có tên TEMPEST để giảm rủi ro giám sát EMR. (Để phù hợp với sở thích suy đoán xung quanh chủ đề này, một số người tin rằng từ viết tắt TEMPEST ban đầu là một từ mã do chính phủ Hoa Kỳ tạo ra vào những năm 1960, nhưng sau đó đư ợc định nghĩa là Vật liệu điện tử viễn thông phát xung điện từ thoáng qua đư ợc bảo vệ khỏi truyền dẫn giả.) Nói chung, TEMPEST bao gồm các quy trình sau: đảm bảo rằng các máy tính đư ợc đặt ở một khoảng cách đủ xa từ các thiết bị điện tử khác nhau để tránh làm cơ sở hạ tầng khác mang sóng vô tuyến sóng. Bất kể mối đe dọa từ việc nghe trộm các phát xạ điện tử có thật hay không, nhiều quy trình bảo vệ chống lại các phát xạ cũng bảo vệ chống lại các mối đe dọa đối với an ninh vật lý.

Hệ thống di động và di động

Điện toán di động thậm chí còn đòi hỏi bảo mật cao hơn so với hệ thống nội bộ trung bình. Hầu hết các hệ thống máy tính di động—máy tính xách tay, thiết bị cầm tay và PDA—có thông tin công ty có giá trị đư ợc lưu trữ bên trong chúng và một số đư ợc định cấu hình để tạo điều kiện cho người dùng truy cập vào các cơ sở máy tính an toàn của tổ chức. Các hình thức truy cập bao gồm kết nối VPN, cấu hình quay số và cơ sở dữ liệu mật khẩu. Ngoài ra, nhiều người dùng lưu giữ vị trí của các tệp và manh mồi về việc lưu trữ thông tin trong máy tính xách tay của họ. Nhiều người dùng thích sự tiện lợi của việc cho phép các hệ điều hành cơ sở ghi nhớ tên người dùng và mật khẩu của họ vì nó giúp truy cập dễ dàng hơn và vì họ thường có nhiều tài khoản, với các tên người dùng và mật khẩu khác nhau để quản lý. Mặc dù việc cho phép các hệ điều hành cho phép truy cập dễ dàng hơn vào các tài khoản đư ợc sử dụng thường xuyên rất hấp dẫn, nhưng như ợc điểm của việc thiết lập các sắp xếp này trên một hệ thống di động là rõ ràng: mất hệ thống đồng nghĩa với việc mất các cơ chế kiểm soát truy cập.

Một công nghệ tư ơ ng đổi mới giúp xác định vị trí máy tính xách tay bị mất hoặc bị đánh cắp có thể cung cấp bảo mật bổ sung. Ví dụ, CompuTrace Laptop Security của Absolute Software là phần mềm máy tính được cài đặt trên máy tính xách tay, như minh họa trong **Hình 7-5**. Theo định kỳ, khi máy tính kết nối Internet, phần mềm sẽ tự báo cáo và số sê-ri điện tử của máy tính được cài đặt vào trung tâm giám sát trung tâm. Nếu máy tính xách tay được báo cáo là bị đánh cắp, phần mềm này có thể theo dõi máy tính đến vị trí hiện tại của nó để có thể phục hồi. Phần mềm không thể bị phát hiện trên hệ thống, ngay cả khi kẻ trộm biết phần mềm đã được cài đặt. Ngoài ra, CompuTrace vẫn được cài đặt ngay cả khi ổ cứng của máy tính xách tay được định dạng và hệ điều hành được cài đặt lại.

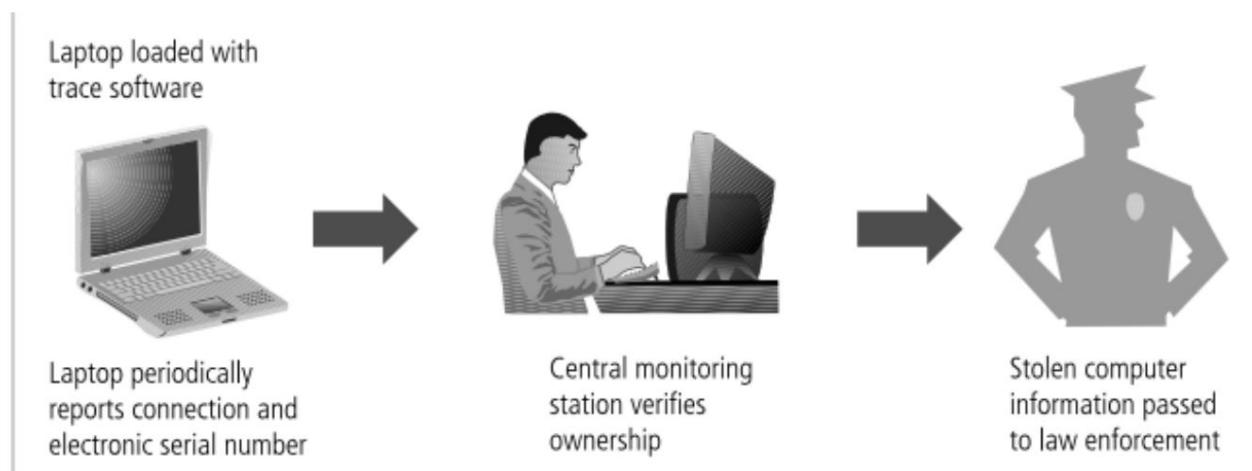
Cũng có sẵn cho máy tính xách tay là thiết bị báo trộm được tạo thành từ thẻ PC hoặc thiết bị khác có chứa bộ phát hiện chuyển động. Nếu thiết bị được trang bị vũ khí và máy tính xách tay được di chuyển nhiều hơn dự kiến, báo thức sẽ kích hoạt còi hoặc còi rất lớn. Hệ thống bảo mật cũng có thể vô hiệu hóa máy tính hoặc sử dụng tùy chọn mã hóa để làm cho thông tin được lưu trữ trong hệ thống không sử dụng được.

Để bảo mật tối đa, máy tính xách tay phải luôn được bảo mật. Nếu bạn đang đi du lịch với một máy tính xách tay, bạn nên sở hữu nó mọi lúc. Cần đặc biệt cẩn thận khi đi máy bay, vì hành vi trộm cắp máy tính xách tay rất phổ biến ở các sân bay. Danh sách sau đây do Cảnh sát Thủ đô của Quận Columbia đưa ra và liệt kê các bước bạn có thể thực hiện để ngăn máy tính xách tay của mình khỏi bị đánh cắp hoặc làm hỏng do bất cẩn:

Không để máy tính xách tay trong xe không khóa, ngay cả khi xe đang ở trên đường lái xe vào nhà hoặc ga ra của bạn, và không bao giờ để nó ở nơi dễ thấy, ngay cả khi xe đã khóa—điều đó chỉ gây ra rắc rối. Nếu bạn phải để máy tính xách tay của mình trong xe, nơi tốt nhất là trong cốp xe có khóa. Nếu bạn không có cốp xe, hãy đậy nắp lại và khóa cửa lại.

Nhà để xe có khả năng là khu vực xảy ra trộm cắp xe cộ, vì chúng cung cấp nhiều sự lựa chọn và che chở cho kẻ trộm. Một lần nữa, đừng bao giờ để máy tính xách tay của bạn ở nơi dễ thấy; đậy lại hoặc cho vào cốp xe.

Hãy nhận thức được những thiệt hại mà nhiệt độ khắc nghiệt có thể gây ra cho máy tính.



□

Hình 7-5 Ngăn chặn trộm cắp máy tính xách tay Nguồn: Course Technology/Cengage Learning

Mang theo máy tính xách tay của bạn trong hộp đựng, cặp hoặc túi không có gì đặc biệt khi di chuyển. Đặt nó trong hộp để ợc thiết kế cho máy tính là một lời cảnh báo ngay lập tức cho những tên trộm rằng bạn có một chiếc máy tính xách tay.

Đi ăn trưa hay nghỉ ngơi? Đừng rời khỏi phòng họp hoặc hội nghị mà không có máy tính xách tay của bạn. Hãy mang nó theo, nếu không bạn sẽ gặp rủi ro là nó sẽ không còn ở đó khi bạn quay lại.

Khóa máy tính xách tay trong văn phòng của bạn trong giờ làm việc. Bạn không có văn phòng riêng? Sử dụng khóa cáp quần quanh chân bàn hoặc ghế hoặc đặt máy tính xách tay trong tủ hoặc tủ có khóa.

Đừng để những người lạ không có người đi kèm đi lang thang trong nơi làm việc của bạn. Cung cấp hỗ trợ và đưa du khách đến các điểm đến của họ.

Áp dụng các dấu sơn đặc biệt để làm cho máy tính xách tay của bạn trở nên độc đáo và dễ nhận biết. Chất tẩy trắng dạng lỏng là một chất tốt để áp dụng.

Cân nhắc mua một trong những hệ thống báo trộm mới ợc sản xuất đặc biệt cho máy tính xách tay.

Xin lưu ý rằng nếu máy tính của bạn bị đánh cắp, đăng nhập tự động có thể giúp kẻ trộm dễ dàng gửi thư không phù hợp bằng tài khoản của bạn.

Sao lưu thông tin của bạn trên đĩa ngay hôm nay và lưu trữ đĩa ở nhà hoặc văn phòng.

Bảo mật máy tính từ xa

Tính toán địa điểm từ xa, ngày càng trở nên phổ biến, bao gồm nhiều địa điểm điện toán khác nhau cách xa cơ sở tổ chức cơ sở và bao gồm tất cả các hình thức làm việc từ xa. Làm việc từ xa là máy tính bên ngoài sử dụng các kết nối Internet, kết nối quay số, kết nối qua các liên kết điểm-điểm thuê giữa các văn phòng và các cơ chế kết nối khác.

Viễn thông từ nhà của người dùng đáng ợc quan tâm đặc biệt. Một trong những điểm hấp dẫn của việc làm việc từ xa đối với cả nhân viên và người sử dụng lao động là bằng cách tránh phải đi lại nhiều lần, nhân viên làm việc từ xa có nhiều thời gian hơn để tập trung vào công việc họ làm. Nhưng khi nhiều người trở thành những người làm việc từ xa, rủi ro đối với thông tin truyền qua các kết nối thư ờng không an toàn mà những người làm việc từ xa sử dụng là rất lớn. Vấn đề là không đủ các tổ chức cung cấp các kết nối an toàn cho mạng văn phòng của họ và thậm chí còn ít tổ chức hơn cung cấp các hệ thống an toàn nếu máy tính ở nhà của nhân viên bị xâm phạm. Để bảo mật toàn bộ mạng, tổ chức phải dành tài nguyên bảo mật để bảo vệ các kết nối gia đình này. Mặc dù việc cài đặt VPN có thể giúp bảo vệ dữ liệu trong

đư ờng truyền, những ngư ời làm việc từ xa thư ờng xuyên lư u trữ dữ liệu văn phòng trên hệ thống tại nhà của họ, trong tủ hồ sơ gia đình và trên các phư ơng tiện truyền thông bên ngoài. Để đảm bảo một quy trình an toàn, các máy tính mà những ngư ời làm việc từ xa sử dụng phải đư ợc đảm bảo an toàn hơn các hệ thống của tổ chức, vì chúng nằm ngoài phạm vi bảo mật. Kẻ tấn công đột nhập vào nhà của ai đó có thể sẽ thấy mức độ bảo mật thấp hơn nhiều so với tại văn phòng. Hầu hết các hệ thống văn phòng đều yêu cầu ngư ời dùng đăng nhập, như ng máy tính ở nhà của ngư ời làm việc từ xa có thể là máy cá nhân của nhân viên và do đó có thể có hệ điều hành kém an toàn hơn nhiều và có thể không sử dụng mật khẩu. Những ngư ời làm việc từ xa phải sử dụng hệ điều hành an toàn yêu cầu xác thực mật khẩu, chẳng hạn như Windows XP/Vista/7 hoặc Server 2003/2008. Họ phải lưu trữ tất cả dữ liệu lỏng lẻo trong tủ hồ sơ có khóa và phư ơng tiện lỏng lẻo trong két sắt có khóa. Họ phải xử lý dữ liệu ở nhà cẩn thận hơn so với ở văn phòng, vì mức độ bảo mật chung cho một ngôi nhà trung bình thấp hơn so với một tòa nhà thư ờng mại.

Điều tự ơng tự cũng áp dụng cho những ngư ời lao động sử dụng máy tính di động trên đư ờng. Nhân viên sử dụng sổ ghi chép trong phòng khách sạn nên cho rằng các đư ờng truyền không đư ợc mã hóa của họ đang bị theo dõi và bất kỳ máy tính xách tay không bảo mật nào cũng có thể bị đánh cắp. Nhân viên bên ngoài cơ sở sử dụng các cơ sở thuê không biết ai khác đư ợc kết nối vật lý với mạng và do đó ai có thể đang nghe các cuộc hội thoại dữ liệu của họ. VPN là điều bắt buộc trong tất cả các giao tiếp từ bên ngoài đến bên trong và việc sử dụng các hệ thống xác thực nâng cao có liên quan đư ợc khuyến khích mạnh mẽ.

Mặc dù có thể bảo mật các trang web từ xa, như ng các tổ chức không thể cho rằng nhân viên sẽ đầu tư tiền của họ để bảo mật. Nhiều tổ chức hầu như không chấp nhận làm việc từ xa vì một số lý do, bao gồm cả việc nhân viên làm việc từ xa thư ờng yêu cầu hai bộ thiết bị máy tính, một cho văn phòng và một cho gia đình. Khoản chi phí tăng thêm này rất khó để biện minh, đặc biệt khi nhân viên là ngư ời duy nhất đư ợc hưởng lợi từ việc làm việc từ xa. Trong những trường hợp hiếm hoi mà việc cho phép nhân viên hoặc chuyên gia tư vấn làm việc từ xa là cách duy nhất để đạt đư ợc những kỹ năng cực kỳ có giá trị, tổ chức thường sẵn sàng làm những gì cần thiết để bảo mật hệ thống của mình. Chỉ khi nghiên cứu bổ sung về làm việc từ xa cho thấy rõ ràng lợi thế cuối cùng thì các tổ chức mới bắt đầu đầu tư đủ nguồn lực vào việc đảm bảo an toàn cho thiết bị của những ngư ời làm việc từ xa của họ. Tuy nhiên, có một số tổ chức hỗ trợ làm việc từ xa và các tổ chức này thư ờng rơi vào một trong ba nhóm. Đầu tiên là tổ chức thành và do đó lành mạnh về mặt tài chính với đủ ngân sách để hỗ trợ làm việc từ xa và do đó nâng cao vị thế của tổ chức với nhân viên và hình ảnh của tổ chức. Trong những năm gần đây, tùy chọn làm việc từ xa đã trở thành một yếu tố trong bảng xếp hạng tổ chức do nhiều tạp chí thực hiện. Một số tổ chức tìm cách cải thiện điều kiện làm việc của nhân viên và cũng cải thiện vị trí của họ trong bảng xếp hạng những nơi làm việc tốt nhất bằng cách thêm tùy chọn làm việc từ xa cho nhân viên. Nhóm thứ hai là công ty công nghệ cao mới, với một số lư ợng lớn nhân viên đa dạng về mặt địa lý, hầu như chỉ làm việc từ xa. Các công ty này sử dụng công nghệ một cách rộng rãi và quyết tâm biến việc áp dụng và sử dụng công nghệ thành

nền tảng của các tổ chức của họ. Nhóm thứ ba trùng lặp với nhóm thứ hai và được gọi là tổ chức ảo. Tổ chức ảo là một nhóm các cá nhân được tập hợp lại để thực hiện một nhiệm vụ cụ thể, thường là từ các tổ chức, bộ phận hoặc phòng ban khác nhau. Những cá nhân này thành lập một công ty ảo, trong các cơ sở cho thuê hoặc thông qua các thỏa thuận làm việc từ xa 100%. Khi công việc được hoàn thành, tổ chức sẽ được chuyển hướng hoặc giải thể. Các tổ chức này hầu như chỉ dựa vào điện toán từ xa và làm việc từ xa, nhưng chúng cực kỳ hiếm và do đó không được ghi chép hoặc nghiên cứu kỹ càng.

Cân nhắc đặc biệt cho an ninh vật lý

Có một số cân nhắc đặc biệt cần tính đến khi phát triển một chương trình bảo mật vật lý. Đầu tiên trong số này là câu hỏi nên xử lý bảo mật vật lý trong nhà hay thuê bên ngoài. Như với bất kỳ khía cạnh nào của bảo mật thông tin, không nên đưa ra quyết định mua hay bán một cách hời hợt. Có một số cơ quan đủ năng lực và chuyên nghiệp cung cấp các dịch vụ và tư vấn về an ninh vật lý. Lợi ích của việc thuê ngoài an ninh vật lý bao gồm thu được kinh nghiệm và kiến thức của các cơ quan này, nhiều cơ quan trong số đó đã hoạt động trong lĩnh vực này hàng thập kỷ. Thuê ngoài các hoạt động không quen thuộc luôn giải phóng một tổ chức để tập trung vào các mục tiêu chính của nó, thay vì hỗ trợ các hoạt động. Như điểm bao gồm chi phí, mất kiểm soát đối với các thành phần riêng lẻ của giải pháp bảo mật vật lý và nhu cầu tin tưởng vào một công ty khác để thực hiện một chức năng kinh doanh thiết yếu. Một tổ chức không chỉ phải tin tưởng vào các quy trình được sử dụng bởi công ty ký hợp đồng mà còn phải có khả năng thuê và giữ chân những nhân viên đáng tin cậy, những người tôn trọng sự an toàn của công ty ký hợp đồng mặc dù họ không có lòng trung thành với nó. Mức độ tin cậy này thường là khía cạnh khó khăn nhất trong quyết định thuê ngoài, bởi vì thực tế của việc thuê ngoài an ninh vật lý là những người không phải là nhân viên sẽ cung cấp một biện pháp bảo vệ mà tổ chức chỉ quản lý một chút.

Một xem xét an ninh vật lý khác là kỹ thuật xã hội. Như bạn đã học trong các chương trình, kỹ thuật xã hội liên quan đến việc sử dụng các kỹ năng của con người để thu thập thông tin bí mật từ nhân viên. Trong khi hầu hết các kỹ sư xã hội thích sử dụng điện thoại hoặc máy tính để thu thập thông tin, một số cố gắng truy cập thông tin trực tiếp hơn. Như trong các trường hợp đã đề cập trước đó, trong đó các đại lý thành thạo về kỹ thuật được bố trí vào các vị trí lao động tại văn phòng của đối thủ cạnh tranh, có một số cách mà người bên ngoài có thể tiếp cận với các nguồn lực của tổ chức. Ví dụ, hầu hết các tổ chức không có các quy trình kỹ lưỡng để xác thực và kiểm soát những người không phải là nhân viên truy cập vào cơ sở của họ. Khi không có thủ tục, không ai để ý đến người thợ sửa chữa lang thang, công nhân dịch vụ hay quan chức thành phố. Không khó để ăn mặc như thợ sửa điện thoại, công nhân xây dựng hoặc thanh tra tòa nhà và di chuyển tự do trong tòa nhà. Một số thậm chí có thể nói rằng để đi đến hầu hết mọi nơi trong bất kỳ tòa nhà nào, tất cả những gì người ta thực sự cần là một bằng tạm và một thái độ. Nếu bạn trông như thế bạn có sứ mệnh và tỏ ra có năng lực, hầu hết người sẽ để bạn yên. Làm thế nào các tổ chức có thể chống lại kiểu tấn công này? Bằng cách yêu cầu tất cả các

hiển thị phù hiệu du khách phù hợp và được hộ tống khi họ ở trong khu vực hạn chế.

Quản lý hàng tồn kho

Giống như các nguồn lực tổ chức khác, thiết bị máy tính nên được kiểm kê và kiểm tra thường xuyên. Việc quản lý hàng tồn kho máy tính là một phần quan trọng của an ninh vật lý. Làm cách nào khác để bộ phận an ninh của công ty biết được liệu một nhân viên đã ăn cắp vật tư máy tính hay một nhân viên cũ đã mang thiết bị của tổ chức về nhà? Tự ứng tự, thông tin mật cũng cần được kiểm kê và quản lý. Trong quân đội, bất cứ khi nào cần sao chép tài liệu mật, người ta sẽ dán tem lên bản gốc trước khi sao chép. Điều này cho biết mức độ phân loại của tài liệu và dấu văn bản "của" để người sao chụp có thể đánh dấu số thứ tự của từng bản sao cũng như tổng số bản sao được sao chụp. Ví dụ, nếu cần tạo 25 bản sao, người chịu trách nhiệm sao chép tài liệu sẽ viết "26" vào ô trống bên phải, tạo các bản sao và sau đó đánh số thứ tự. Tại sao 26 mà không phải 25? Bản gốc luôn là tài liệu số một. Sau khi đánh số, từng bản mật được cấp cho người được phân công ký nhận. Mặc dù thủ tục này có thể là quá mức cần thiết đối với hầu hết các tổ chức, nhưng nó đảm bảo rằng việc quản lý hàng tồn kho các tài liệu được phân loại luôn được an toàn. Ngoài ra, hình thức phải ký vào một tài liệu cũng có giá trị của nó trong tâm trí người nhận.

1. Trả lời câu hỏi

1. Liệt kê và mô tả ba cách cơ bản mà dữ liệu có thể bị chặn.

Làm thế nào để một chương trình bảo mật vật lý bảo vệ chống lại từng phương pháp chặn dữ liệu này?

2. Bạn có thể làm gì để giảm nguy cơ bị đánh cắp máy tính xách tay?

3. Ưu và nhược điểm của việc thuê ngoài bảo mật vật lý là gì?

4. Mọi người nên làm gì để kiểm soát những người không phải là nhân viên ra vào cơ sở của họ?

2. Phát biểu (Làm việc theo nhóm). Nghiên cứu một trường hợp thực tế về tấn công bảo mật vật lý. Chuyện gì đã xảy ra thế? Hệ thống an ninh vật lý nào có liên quan? Kết quả là gì? Trình bày về chúng trước lớp.

BÀI 8: THỰC HIỆN BẢO MẬT THÔNG TIN

Giới thiệu

Đầu tiên và quan trọng nhất, người quản lý dự án bảo mật thông tin phải nhận ra rằng việc triển khai một dự án bảo mật thông tin cần có thời gian, nỗ lực cũng như rất nhiều sự giao tiếp và phối hợp. Chuỗi này và chuỗi tiếp theo thảo luận về hai giai đoạn của giai đoạn triển khai vòng đời phát triển hệ thống bảo mật (SecSDLC) và mô tả cách thực hiện thành công kế hoạch chi tiết bảo mật thông tin. Nói chung, giai đoạn triển khai được hoàn thành bằng cách thay đổi cấu hình và hoạt động của các hệ thống thông tin của tổ chức để làm cho chúng an toàn hơn. Nó bao gồm các thay đổi sau:

Thủ tục (ví dụ, thông qua chính sách)

Con người (ví dụ, thông qua đào tạo)

Phần cứng (ví dụ: thông qua tư ờng lửa)

Phần mềm (ví dụ: thông qua mã hóa)

Dữ liệu (ví dụ: thông qua phân loại)

Như bạn có thể nhớ lại từ các chương trứớc, SecSDLC liên quan đến việc thu thập thông tin về các mục tiêu, kiến trúc kỹ thuật và môi trường bảo mật thông tin của tổ chức. Các yếu tố này được sử dụng để tạo thành kế hoạch chi tiết bảo mật thông tin, là nền tảng để bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin của tổ chức.

Trong giai đoạn triển khai, tổ chức chuyển kế hoạch chi tiết về bảo mật thông tin thành một kế hoạch dự án. Kế hoạch dự án hướng dẫn các cá nhân đang thực hiện giai đoạn thực hiện. Các hướng dẫn này tập trung vào các thay đổi kiểm soát bảo mật cần thiết để cải thiện tính bảo mật của phần cứng, phần mềm, quy trình, dữ liệu và con người tạo nên hệ thống thông tin của tổ chức. Toàn bộ kế hoạch dự án phải mô tả cách thu thập và triển khai các biện pháp kiểm soát bảo mật cần thiết, đồng thời tạo ra một môi trường để các biện pháp kiểm soát đó đạt được kết quả mong muốn.

Tuy nhiên, trứớc khi phát triển một kế hoạch dự án, ban quản lý nên điều phối tầm nhìn và mục tiêu bảo mật thông tin của tổ chức với các cộng đồng có lợi ích liên quan đến việc thực hiện kế hoạch. Kiểu phối hợp này đảm bảo rằng chỉ những biện pháp kiểm soát làm tăng thêm giá trị cho chương trình bảo mật thông tin của tổ chức mới được đưa vào kế hoạch dự án. Nếu không có tuyên bố về tầm nhìn và mục tiêu cho chương trình an ninh của tổ chức thì phải phát triển và đưa vào kế hoạch dự án. Tuyên bố tầm nhìn nên ngắn gọn. Nó nên nêu nhiệm vụ của chương trình bảo mật thông tin và các mục tiêu của nó. Nói cách khác, kế hoạch dự án được xây dựng dựa trên tuyên bố về tầm nhìn, đóng vai trò như một

la bàn để hướng dẫn những thay đổi cần thiết cho giai đoạn thực hiện. Các thành phần của kế hoạch dự án không bao giờ được xung đột với tầm nhìn và mục tiêu của tổ chức.

ĐỌC VÀ NÓI 1

1. Thảo luận các câu hỏi:

1. Bạn đã bao giờ tham gia lập kế hoạch cho một dự án chưa? Nó thế nào
Thực thi?

2. Bạn nghĩ những đặc điểm của một kế hoạch tốt là gì?

2. Đọc văn bản và thực hiện các yêu cầu bên dưới

Quản lý dự án bảo mật thông tin Thay đổi tổ chức

không dễ thực hiện. Các phần sau thảo luận về các vấn đề mà một kế hoạch dự án phải giải quyết, bao gồm lãnh đạo dự án; cân nhắc về quản lý, kỹ thuật và ngân sách; và sự phản kháng của tổ chức đối với sự thay đổi.

Các bước chính trong việc thực hiện kế hoạch dự án như sau:

- Lập kế hoạch dự án •
- Giám sát các nhiệm vụ và các bước hành động • Kết thúc

Kế hoạch dự án có thể được phát triển theo nhiều cách. Mỗi tổ chức phải xác định phuơng pháp quản lý dự án riêng cho các dự án CNTT và bảo mật thông tin. Bất cứ khi nào có thể, các dự án bảo mật thông tin nên tuân theo các thông lệ quản lý dự án của tổ chức.

Phát triển kế hoạch dự án

Lập kế hoạch cho giai đoạn thực hiện đòi hỏi phải tạo ra một kế hoạch dự án chi tiết. Nhiệm vụ tạo ra một kế hoạch dự án như vậy thường được giao cho người quản lý dự án hoặc người phụ trách dự án. Cá nhân này quản lý dự án và ủy thác các phần của nó cho những người ra quyết định khác. Thường thì người quản lý dự án đến từ cộng đồng CNTT quan tâm, bởi vì hầu hết các nhân viên khác đều thiếu nền tảng bảo mật thông tin cần thiết và quyền quản lý phù hợp và/hoặc kiến thức kỹ thuật.

Kế hoạch dự án có thể được tạo bằng cách sử dụng một công cụ lập kế hoạch đơn giản như cấu trúc phân chia công việc (WBS). Để sử dụng phuơng pháp WBS, trước tiên bạn chia nhỏ kế hoạch dự án thành các nhiệm vụ chính của nó. Các nhiệm vụ chính của dự án được đặt vào WBS, cùng với các thuộc tính sau cho từng nhiệm vụ:

- Công việc cần hoàn thành (các hoạt động và sản phẩm) • Các cá nhân (hoặc nhóm kỹ năng) được chỉ định thực hiện nhiệm vụ • Ngày bắt đầu và ngày kết thúc của nhiệm vụ (khi biết) • Lực lượng nỗ lực cần thiết để hoàn thành tính bằng giờ hoặc ngày làm việc • Chi phí vốn ước tính cho nhiệm vụ
- Chi phí phi vốn ước tính cho nhiệm vụ • Xác định sự phụ thuộc giữa các nhiệm vụ

Mỗi nhiệm vụ chính trên WBS sau đó được chia thành các nhiệm vụ nhỏ hơn (nhiệm vụ con) hoặc các bước hành động cụ thể. Với sự đa dạng của các dự án khả thi, có rất ít hướng dẫn chính thức để quyết định mức độ chi tiết nào-tức là, ở mức độ nào một nhiệm vụ hoặc nhiệm vụ con sẽ trở thành một bước hành động-là phù hợp. Tuy nhiên, có một quy tắc khó và nhanh mà bạn có thể sử dụng để đưa ra quyết định này: một nhiệm vụ hoặc nhiệm vụ con trở thành một bước hành động khi nó có thể được hoàn thành bởi một cá nhân hoặc bộ kỹ năng và có một sản phẩm duy nhất.

WBS có thể được chuẩn bị bằng một chương trình bảng tính máy tính để bàn đơn giản. Việc sử dụng các công cụ phần mềm quản lý dự án phức tạp hơn thường dẫn đến tình trạng kích động, trong đó người quản lý dự án dành nhiều thời gian hơn để ghi lại các nhiệm vụ dự án, thu thập các phép đo hiệu suất, ghi lại thông tin nhiệm vụ dự án và cập nhật dự báo hoàn thành dự án hơn là hoàn thành công việc dự án có ý nghĩa.

Công việc cần hoàn thành Công việc cần hoàn thành bao gồm cả các hoạt động và sản phẩm bàn giao. Sản phẩm có thể bàn giao là một tài liệu hoặc mô-đun chương trình đã hoàn thành, có thể đóng vai trò là điểm bắt đầu cho một nhiệm vụ sau này hoặc trở thành một thành phần trong dự án đã hoàn thành. Lý tưởng nhất là người lập kế hoạch dự án cung cấp nhãn và mô tả kỹ lưỡng cho nhiệm vụ. Mô tả phải đủ đầy đủ để tránh sự mơ hồ trong quá trình theo dõi sau này, nhưng không quá chi tiết để làm cho WBS trở nên khó sử dụng. Ví dụ: nếu nhiệm vụ là viết thông số kỹ thuật tư ờng lửa để chuẩn bị yêu cầu đề xuất (RFP), người lập kế hoạch cần lưu ý rằng tài liệu có thể chuyển giao là tài liệu đặc tả phù hợp để phân phối cho nhà cung cấp.

Người được giao Người lập kế hoạch dự án nên mô tả bộ kỹ năng hoặc người, thư ờng được gọi là nguồn lực, cần thiết để hoàn thành nhiệm vụ. Nên tránh đặt tên cho các cá nhân trong các nỗ lực lập kế hoạch ban đầu. Thay vì chỉ định cá nhân, kế hoạch dự án nên tập trung vào vai trò tổ chức hoặc bộ kỹ năng đã biết. Ví dụ: nếu bắt kỳ kỹ sư nào trong nhóm mạng có thể viết thông số kỹ thuật cho bộ định tuyến, tài nguyên được chỉ định sẽ được ghi chú là "kỹ sư mạng" trên WBS. Tuy nhiên, khi tiến hành lập kế hoạch, các nhiệm vụ cụ thể và các bước hành động có thể và nên được giao cho các cá nhân. Ví dụ: khi chỉ người quản lý của nhóm mạng mới có thể đánh giá phản hồi đối với RFP và đưa ra giải thư ờng cho hợp đồng, người lập kế hoạch dự án nên xác định người quản lý mạng là tài nguyên được chỉ định cho nhiệm vụ này.

Ngày bắt đầu và ngày kết thúc Trong giai đoạn đầu của việc lập kế hoạch, người lập kế hoạch dự án nên

cố gắng chỉ định ngày hoàn thành chỉ cho các mốc quan trọng của dự án. Cột mốc quan trọng là một điểm cụ thể trong kế hoạch dự án khi một nhiệm vụ có tác động đáng chú ý đến tiến độ của kế hoạch dự án đư ợc hoàn thành. Ví dụ: ngày gửi RFP cuối cùng cho nhà cung cấp là một cột mốc quan trọng, bởi vì nó báo hiệu rằng tất cả công việc chuẩn bị RFP đã hoàn tất. Việc ấn định quá nhiều ngày cho quá nhiều nhiệm vụ sớm trong quá trình lập kế hoạch sẽ làm trầm trọng thêm tình trạng viêm trực tràng. Người lập kế hoạch có thể tránh cạm bẫy này bằng cách chỉ ấn định ngày bắt đầu và ngày kết thúc quan trọng hoặc mốc quan trọng trong quá trình. Sau này trong quá trình lập kế hoạch, người lập kế hoạch có thể thêm ngày bắt đầu và ngày kết thúc nếu cần.

Lực lượng nỗ lực Người lập kế hoạch cần ước tính nỗ lực cần thiết để hoàn thành từng nhiệm vụ, nhiệm vụ con hoặc bước hành động. Ước tính số giờ nỗ lực cho công việc kỹ thuật là một quá trình phức tạp. Ngay cả khi một tổ chức có quản trị chính thức, quy trình xem xét kỹ thuật và quy trình kiểm soát thay đổi, thì việc yêu cầu những người quen thuộc nhất với các nhiệm vụ hoặc các nhiệm vụ tương tự thực hiện các ước tính này luôn là một thông lệ tốt. Sau khi các ước tính này đư ợc thực hiện, tất cả những người đư ợc chỉ định cho các bước hành động nên xem lại số giờ nỗ lực ước tính, hiểu các nhiệm vụ và đồng ý với các ước tính.

Ước tính chi phí vốn Người lập kế hoạch cần ước tính chi phí vốn cần thiết để hoàn thành từng nhiệm vụ, nhiệm vụ con hoặc mục hành động. Trong khi mỗi tổ chức lập ngân sách và chi tiêu vốn theo các thủ tục đư ợc thiết lập riêng, hầu hết đều phân biệt giữa chi tiêu vốn cho tài sản lâu bền và chi phí cho các mục đích khác. Ví dụ: một thiết bị tư ờng lửa có giá 5.000 đô la có thể là chi phí vốn cho một tổ chức, nhưng cùng một tổ chức có thể không coi gói phần mềm trị giá 5.000 đô la là chi phí vốn vì các quy tắc kế toán của nó phân loại tất cả phần mềm là khoản mục chi phí, bắt kể chi phí.

Chi phí phi vốn ước tính Người lập kế hoạch cần ước tính chi phí phi vốn để hoàn thành từng nhiệm vụ, nhiệm vụ con hoặc mục hành động. Một số tổ chức yêu cầu chi phí này bao gồm phí thu hồi thời gian của nhân viên, trong khi những tổ chức khác loại trừ thời gian của nhân viên và chỉ hợp đồng dự án hoặc thời gian tư vấn là chi phí phi vốn. Như đã đề cập trước đó, điều quan trọng là phải xác định các thông lệ của tổ chức mà kế hoạch sẽ đư ợc sử dụng. Ví dụ: tại một số công ty, một dự án triển khai tư ờng lửa có thể chỉ tính chi phí của phần cứng tư ờng lửa là vốn và coi tất cả các chi phí cho lao động và phần mềm là chi phí, coi yếu tố phần cứng là hàng hóa lâu bền có tuổi thọ nhiều năm. Một tổ chức khác có thể sử dụng tổng tất cả các dòng tiền ra liên quan đến việc thực hiện làm phí vốn và không tính phí cho loại chi phí. Lý do đằng sau việc sử dụng tổng hợp này, có thể bao gồm chi phí cho các mặt hàng tương tự như phần cứng, nhân công và vận chuyển hàng hóa, là khả năng mới đư ợc triển khai dự kiến sẽ tồn tại trong nhiều năm và là một cải tiến đối với cơ sở hạ tầng của tổ chức. Một công ty thứ ba có thể tính toàn bộ dự án là chi phí nếu tổng số tiền giảm xuống dưới một ngưỡng nhất định, theo lý thuyết rằng các dự án nhỏ là chi phí của các hoạt động đang diễn ra.

Nhiệm vụ phụ thuộc Người lập kế hoạch nên lưu ý bắt cứ khi nào có thể các phụ thuộc của

các nhiệm vụ hoặc bút ớc hành động khác trong nhiệm vụ hoặc bút ớc hành động hiện tại. Các nhiệm vụ hoặc bút ớc hành động xuất hiện trước nhiệm vụ cụ thể hiện tại được gọi là nhiệm vụ tiền nhiệm và những nhiệm vụ xuất hiện sau nhiệm vụ hiện tại được gọi là nhiệm vụ kế nhiệm. Có thể có nhiều hơn một loại phụ thuộc, nhưng những chi tiết như vậy thường được đề cập trong các khóa học về quản lý dự án và nằm ngoài phạm vi của văn bản này.

2.1. Trả lời các câu hỏi:

1. Liệt kê và mô tả ba bút ớc chính trong việc thực hiện kế hoạch dự án.
2. Cấu trúc phân chia công việc (WBS) là gì? Đó có phải là cách duy nhất để tổ chức một kế hoạch dự án?
3. Liệt kê và định nghĩa các thuộc tính chung của các nhiệm vụ của một WBS.
4. Làm thế nào để một người lập kế hoạch biết khi nào một nhiệm vụ đã được chia nhỏ thành một mức độ và có thể được phân loại như một bút ớc hành động?
5. Sản phẩm bàn giao là gì? Kể tên hai cách sử dụng cho sản phẩm bàn giao.
6. Làm cách nào bạn có thể xác định liệu một nhiệm vụ hoặc nhiệm vụ con có thể trở thành một hành động hay không bút ớc?
7. Tài nguyên là gì? Hai loại là gì?
8. Cột mốc là gì? và tại sao nó lại quan trọng đối với việc lập kế hoạch dự án?
9. Ai là người đánh giá tốt nhất các ước tính nỗ lực cho các nhiệm vụ và các bút ớc hành động của dự án?
Tại sao?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không có thông tin (NI)

1. Một chương trình bảng tính trên máy tính để bàn đơn giản là một công cụ kém hiệu quả để chuẩn bị các WBS.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Nếu tên người được giao nhiệm vụ rõ ràng khi bắt đầu nỗ lực lập kế hoạch.

A. Đúng	B. Sai	C. NI
---------	--------	-------
3. Có thể giảm bớt tình trạng trì trệ bằng cách xác định nhiều ngày hơn cho mỗi nhiệm vụ.

A. Đúng	B. Sai	C. NI
---------	--------	-------

4. Cách phù hợp nhất cho các nhà hoạch định và quản lý là ước tính nỗ lực giờ cho công việc kỹ thuật.

A. Đúng

B. Sai

C. NI

5. Các công ty khác nhau có cách tính phí khác nhau khi nói đến vốn và

chi phí.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau.

1. Điều nào sau đây cần được xem xét khi lập kế hoạch dự án?

A. Ngân sách

B. Lãnh đạo dự án

C. Tổ chức chống lại sự thay đổi.

D. Tất cả đều đúng.

2. Ai thường chịu trách nhiệm lập kế hoạch dự án chi tiết?

A. giám đốc

B. kỹ sư mạng

C. người quản lý mạng

D. người quản lý dự án

3. Thuộc tính nào sau đây KHÔNG có trong WBS?

A. người được giao

B. kiến thức kỹ thuật

C. ngày bắt đầu và ngày kết thúc

D. chi phí ước tính

4. Từ "determination" ở dòng 34 có nghĩa gần nhất với từ nào?

A. sức chịu đựng

B. quyết định

C. kiên trì

D. khám phá

5. Từ “those” trong đoạn cuối đề cập đến điều gì?

- A. Người tiền nhiệm
- B. Nhiệm vụ hoặc các bước hành động
- C. Các nhà quy hoạch
- D. Chi tiết

2. Nói

- 1. Trình bày về đặc điểm chung của các nhiệm vụ của một WBS.
- 2. (Làm việc theo nhóm) Tạo WBS của một kế hoạch dự án trong lớp của bạn.

ĐỌC VÀ NÓI 2

1. Thảo luận các câu hỏi: 1.

Bạn đã từng làm dự án nào chưa?

2. Điều gì thường được xem xét khi làm việc trong một dự án?

2. Đọc văn bản và thực hiện các yêu cầu sau:

Cân nhắc lập kế hoạch dự án

Khi kế hoạch dự án được phát triển, việc thêm chi tiết không phải lúc nào cũng đơn giản. Các phần sau đây thảo luận về các yếu tố mà người lập kế hoạch dự án phải xem xét khi họ quyết định những gì cần đưa vào kế hoạch làm việc, cách chia nhiệm vụ thành các nhiệm vụ con và các bước hành động cũng như cách hoàn thành các mục tiêu của dự án.

Cân nhắc về tài chính Bất kể nhu cầu bảo mật thông tin của tổ chức là gì, số lượng nỗ lực có thể được sử dụng tùy thuộc vào nguồn vốn hiện có. Phân tích lợi ích chi phí (CBA), thường được chuẩn bị trong giai đoạn phân tích của SecSDLC, phải được xem xét và xác minh trước khi phát triển kế hoạch dự án. CBA xác định tác động mà một công nghệ hoặc cách tiếp cận cụ thể có thể có đối với tài sản thông tin của tổ chức và chi phí của nó.

Mỗi tổ chức có cách tiếp cận riêng để tạo và quản lý ngân sách và chi phí. Trong nhiều tổ chức, ngân sách bảo mật thông tin là một phần phụ của ngân sách CNTT tổng thể. Ở những nơi khác, bảo mật thông tin là một danh mục ngân sách riêng biệt có thể có cùng mức độ hiển thị và mức độ ưu tiên như ngân sách CNTT. Bất kể các hạng mục bảo mật thông tin nằm ở đâu trong ngân sách, các hạn chế về tiền tệ sẽ xác định những gì có thể (và không thể) được hoàn thành.

Các tổ chức công có xu hướng dễ dự đoán hơn trong các quy trình ngân sách của họ so với các tổ chức tư nhân, bởi vì ngân sách của các tổ chức công thường là sản phẩm của luật pháp hoặc các cuộc họp công khai. Điều này gây khó khăn cho việc huy động vốn bổ sung sau khi ngân sách được xác định. Ngoài ra, một số tổ chức công dựa vào các khoản trợ cấp tạm thời hoặc tái tạo cho ngân sách của họ và phải quy định các khoản chi tiêu theo kế hoạch khi viết đơn xin trợ cấp. Nếu phát sinh chi phí mới, tiền phải được yêu cầu thông qua các ứng dụng tài trợ mới. Ngoài ra, các khoản chi trợ cấp thường được kiểm toán và không thể bỏ sót. Tuy nhiên, nhiều tổ chức công cộng phải chi tiêu tất cả các khoản ngân sách trong năm tài chính-nếu không, ngân sách của năm tiếp theo sẽ bị giảm số tiền chưa chi tiêu. Do đó, các tổ chức này thường tiến hành chi tiêu nhiều lần vào cuối năm tài chính. Ví dụ, đây thường là thời điểm tốt nhất để mua phần công nghệ còn lại cần thiết để hoàn thiện kiến trúc bảo mật thông tin.

Các tổ chức tư nhân (vì lợi nhuận) có những hạn chế về ngân sách do thị trường quyết định. Khi một tổ chức vì lợi nhuận bắt đầu một dự án để cải thiện an ninh, nguồn tài trợ đến từ ngân sách vốn và chi phí của công ty. Mỗi tổ chức vì lợi nhuận xác định ngân sách vốn và các quy tắc quản lý chi tiêu và chi tiêu vốn khác nhau. Tuy nhiên, trong hầu hết các trường hợp, hạn chế về ngân sách ảnh hưởng đến việc lập kế hoạch và chi tiêu thực tế cho bảo mật thông tin.

Ví dụ, một công nghệ hoặc giải pháp ưa thích có thể bị hy sinh để đổi lấy một giải pháp ít đắt hơn mong đợi hơn nhưng giá cả phải chăng hơn. Ngân sách cuối cùng hướng dẫn việc thực hiện bảo mật thông tin.

Để biện minh cho số tiền được lập ngân sách cho một dự án bảo mật tại một tổ chức công cộng hoặc vì lợi nhuận, có thể hữu ích khi định chuẩn chi phí của các tổ chức tương tự.

Hầu hết các tổ chức vì lợi nhuận công bố các thành phần của báo cáo chi phí của họ.

Tương tự như vậy, các tổ chức công cộng phải ghi lại cách sử dụng tiền. Một người quản lý dự án bảo mật thông tin hiểu biết có thể tìm thấy một số tổ chức có quy mô tương tự với chi phí bảo mật lớn hơn để biện minh cho các khoản chi đã lên kế hoạch.

Mặc dù các chiến thuật như vậy có thể không cải thiện ngân sách năm nay, nhưng chúng có thể cải thiện ngân sách trong tương lai. Trớ trêu thay, những kẻ tấn công cũng có thể giúp những người lập kế hoạch dự án bảo mật thông tin biện minh cho ngân sách bảo mật thông tin. Nếu các cuộc tấn công xâm phạm thành công các hệ thống thông tin đắt giá bảo mật, ban quản lý có thể sẵn sàng hỗ trợ ngân sách bảo mật thông tin hơn.

Cân nhắc Ưu tiên Nói chung, các biện pháp kiểm soát bảo mật thông tin quan trọng nhất trong kế hoạch dự án nên đắt hơn lịch trình. Hạn chế về ngân sách có thể ảnh hưởng đến việc phân công các ưu tiên của dự án. Việc thực hiện các biện pháp kiểm soát đắt hơn dẫn bởi mức độ ưu tiên của các mối đe dọa và giá trị của tài sản thông tin bị đe dọa. Một biện pháp kiểm soát ít quan trọng hơn có thể đắt hơn nếu giải quyết một nhóm lỗ hỏng cụ thể và cải thiện tình hình bảo mật của tổ chức ở mức độ cao hơn so với các biện pháp kiểm soát có mức độ ưu tiên cao hơn của từng cá nhân khác.

Cân nhắc về thời gian và lập lịch trình Thời gian và lập lịch trình có thể ảnh hưởng đến kế hoạch dự án ở hàng chục điểm-xem xét thời gian từ khi đặt hàng đến khi nhận đắt hơn kiểm soát an ninh, có thể không có sẵn ngay lập tức; thời gian cài đặt và cấu hình điều khiển; thời gian đào tạo người dùng; và thời gian cần thiết để nhận ra lỗi từ vào quyền kiểm soát. Ví dụ: nếu một biện pháp kiểm soát phải đắt hơn thực hiện trước khi một tổ chức có thể triển khai sản phẩm thương mại điện tử của mình, quá trình lựa chọn có thể bị ảnh hưởng bởi tốc độ thu thập và triển khai các giải pháp thay thế khác nhau.

Cân nhắc về nhân sự Nhu cầu về nhân sự có trình độ, đắt hơn đào tạo và sẵn có cũng hạn chế kế hoạch dự án. Thưòng cần một đội ngũ nhân viên có kinh nghiệm để triển khai công nghệ, phát triển và thực hiện các chính sách và chương trình đào tạo. Nếu không có nhân viên nào đắt hơn đào tạo để định cấu hình tư tưởng mới, nhân viên thích hợp phải đắt hơn hoặc thuê.

Cân nhắc mua sắm Thưòng có những hạn chế về thiết bị và

quy trình lựa chọn dịch vụ-ví dụ: một số tổ chức yêu cầu sử dụng các nhà cung cấp dịch vụ cụ thể hoặc nhà sản xuất và nhà cung cấp. Những ràng buộc này có thể hạn chế những công nghệ nào có thể đạt được. Ví dụ: trong một chu kỳ ngân sách gần đây, quản trị viên phòng thí nghiệm của các tác giả đang cân nhắc lựa chọn gói phần mềm phân tích rủi ro tự động. Ứng cử viên hàng đầu đã đưa ra đề xuất hợp lý như sau, bao gồm quét lỗ hổng, đánh giá rủi ro và lựa chọn kiểm soát. Sau khi nhận được RFP, nhà cung cấp đã đưa ra giá thầu để đáp ứng các yêu cầu mong muốn với mức giá 75.000 đô la khiến người ta thót tim, cộng với 10% phí bảo trì hàng năm. Nếu một tổ chức có ngân sách vốn bảo mật thông tin hàng năm là 30.000 đô la, thì tổ chức đó phải loại bỏ một gói như thế này khỏi sự cân nhắc-bất chấp các tính năng của phần mềm chưa hẹn như thế nào. Ngoài ra, hãy xem xét hiệu ứng lạnh nhạt đối với sự đổi mới khi một tổ chức yêu cầu tài liệu hỗ trợ phức tạp và/hoặc đấu thầu phức tạp cho các giao dịch mua thậm chí ở quy mô nhỏ. Những ràng buộc mua sắm như vậy, được thiết kế để kiểm soát tổn thất do lạm dụng không thường xuyên, thực sự có thể làm tăng chi phí khi tính đến sự thiếu linh hoạt trong hoạt động.

Cân nhắc tính khả thi của tổ chức Bất cứ khi nào có thể, các thay đổi công nghệ liên quan đến bảo mật phải minh bạch đối với người dùng hệ thống, như ngay lập tức khi những thay đổi đó yêu cầu các thủ tục mới, ví dụ như xác thực hoặc xác thực bổ sung. Một dự án thành công đòi hỏi tổ chức phải có khả năng đồng hóa các thay đổi được đề xuất. Các công nghệ mới đôi khi yêu cầu các chính sách mới và cả hai đều yêu cầu đào tạo và giáo dục nhân viên. Việc lên lịch đào tạo sau khi các quy trình mới được áp dụng (nghĩa là sau khi người dùng phải đổi phó với các thay đổi mà không có sự chuẩn bị) có thể tạo ra căng thẳng và phản kháng, đồng thời có thể làm suy yếu các hoạt động bảo mật. Người dùng chưa được đào tạo có thể phát triển các cách để khắc phục các quy trình bảo mật không quen thuộc và việc họ bỏ qua các biện pháp kiểm soát có thể tạo ra các lỗ hổng bổ sung. Người lại, người dùng không nên chuẩn bị trước quá lâu đến nỗi họ quên các kỹ thuật và yêu cầu đào tạo mới. Khung thời gian tối ưu cho đào tạo thường là từ một đến ba tuần trước khi các chính sách và công nghệ mới xuất hiện trực tuyến.

Cân nhắc về đào tạo và truyền bá Quy mô của tổ chức và cách thức kinh doanh bình thường có thể cản trở một chương trình đào tạo lớn duy nhất về các quy trình hoặc công nghệ bảo mật mới. Nếu vậy, tổ chức nên tiến hành triển khai theo từng giai đoạn hoặc thí điểm, chẳng hạn như đào tạo triển khai cho một bộ phận tại một thời điểm. Khi một dự án liên quan đến sự thay đổi về chính sách, có thể chỉ cần tóm tắt cho người giám sát về chính sách mới và giao cho họ nhiệm vụ cập nhật người dùng cuối trong các cuộc họp được lên lịch thường xuyên. Các nhà hoạch định dự án phải đảm bảo rằng các tài liệu tuyên thủ cũng được phân phối và tất cả nhân viên đều phải đọc, hiểu và đồng ý với các chính sách mới.

cân nhắc phạm vi

Phạm vi dự án mô tả lượng thời gian và số giờ nỗ lực cần thiết để cung cấp các tính năng theo kế hoạch và mức chất lượng của các sản phẩm có thể bàn giao của dự án. Phạm vi của bất kỳ kế hoạch dự án nhất định nào cũng cần được xem xét cẩn thận và giữ ở mức nhỏ nhất có thể.

mục tiêu của dự án. Để kiểm soát phạm vi dự án, các tổ chức nên triển khai các dự án bảo mật thông tin lớn theo từng giai đoạn, như trong phuơng pháp tiếp cận hồng tâm được thảo luận sau trong chương này.

Có một số lý do tại sao phạm vi của các dự án an toàn thông tin phải được đánh giá và điều chỉnh một cách thận trọng. Đầu tiên, ngoài thách thức xử lý nhiều tác vụ phức tạp cùng một lúc, việc cài đặt các biện pháp kiểm soát bảo mật thông tin có thể làm gián đoạn hoạt động đang diễn ra của một tổ chức và cũng có thể xung đột với các biện pháp kiểm soát hiện có theo những cách không thể đoán trước. Ví dụ: nếu bạn cài đặt đồng thời bộ định tuyến lọc gói mới và tường lửa proxy ứng dụng mới và kết quả là người dùng bị chặn truy cập Web, công nghệ nào đã gây ra xung đột? Đó có phải là bộ định tuyến, tường lửa hay sự tương tác giữa cả hai?

Giới hạn phạm vi dự án thành một tập hợp các nhiệm vụ có thể quản lý không có nghĩa là dự án chỉ cho phép thay đổi một thành phần tại một thời điểm, nhưng một kế hoạch tốt sẽ xem xét cẩn thận số lượng nhiệm vụ được lên kế hoạch cho cùng một thời điểm trong một bộ phận.

Sự cần thiết của quản lý dự án

Quản lý dự án đòi hỏi một bộ kỹ năng đặc đáo và sự hiểu biết sâu sắc về nhiều kiến thức chuyên ngành. Trên thực tế, hầu hết các dự án bảo mật thông tin đều yêu cầu người quản lý dự án được đào tạo-CISO hoặc người quản lý CNTT lành nghề được đào tạo về kỹ thuật quản lý dự án. Ngay cả các nhà quản lý dự án có kinh nghiệm cũng nên tìm kiếm sự trợ giúp của chuyên gia khi tham gia vào quy trình đấu thầu chính thức để lựa chọn các công nghệ tiên tiến hoặc tích hợp hoặc các dịch vụ thuê ngoài.

Thực hiện có giám sát Mặc dù đây không phải là giải pháp tối ưu, nhưng một số tổ chức chỉ định một người đứng đầu từ cộng đồng quản lý chung có lợi để giám sát việc thực hiện kế hoạch dự án bảo mật thông tin. Trong trường hợp này, các nhóm nhiệm vụ được giao cho các cá nhân hoặc nhóm từ cộng đồng CNTT và bảo mật thông tin quan tâm. Một giải pháp thay thế là chỉ định một người quản lý CNTT cấp cao hoặc CIO của tổ chức để lãnh đạo việc triển khai. Trong trường hợp này, công việc chi tiết được giao cho các nhóm liên chức năng. Giải pháp tối ưu là chỉ định một người phù hợp từ cộng đồng bảo mật thông tin quan tâm. Trong phân tích cuối cùng, mỗi tổ chức phải tìm ra người lãnh đạo dự án phù hợp nhất với nhu cầu cụ thể của mình cũng như tính cách và chính trị của văn hóa tổ chức.

Thực hiện kế hoạch Khi một dự án đang được tiến hành, nó được quản lý bằng một quy trình được gọi là vòng phản hồi tiêu cực hoặc vòng điều khiển học, đảm bảo rằng tiến độ được đo lường định kỳ. Trong vòng phản hồi tiêu cực, kết quả đo được so sánh với kết quả mong đợi. Khi sai lệch đáng kể xảy ra, hành động khắc phục được thực hiện để đưa nhiệm vụ sai lệch trở lại phù hợp với kế hoạch dự án, nếu không thì dự báo sẽ được sửa đổi theo thông tin mới. Xem Hình 8-1 để biết tổng quan về quá trình này.

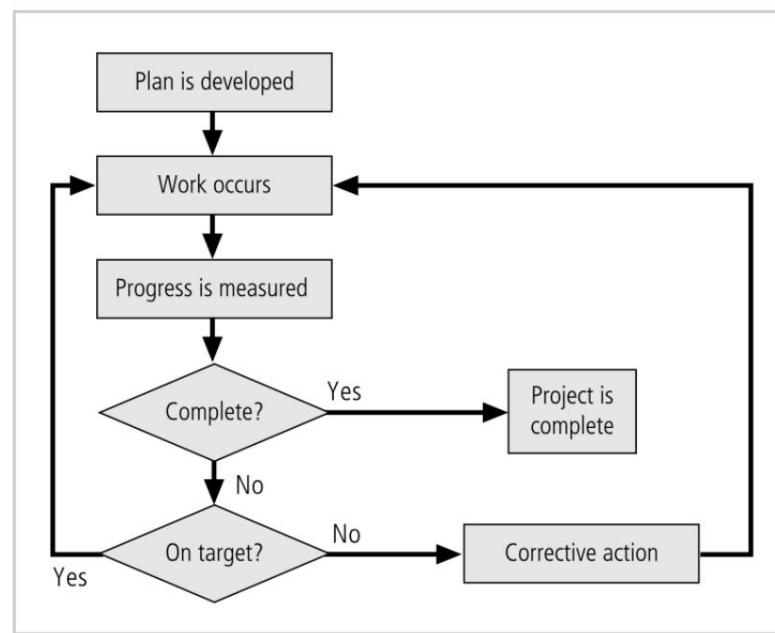
Hành động khắc phục được thực hiện trong hai tình huống cơ bản: ước tính bị sai sót hoặc

hiệu suất đã bị tụt lại. Khi ước tính có sai sót, chẳng hạn như khi số giờ nỗ lực cần thiết bị đánh giá thấp, kế hoạch nên được sửa chữa và các nhiệm vụ tiếp theo được cập nhật để phản ánh sự thay đổi. Khi hiệu suất bị chậm lại, chẳng hạn như do thay thế nhân viên lành nghề cao, hành động khắc phục có thể ở dạng bổ sung nguồn lực, lập lịch trình dài hơn hoặc giảm chất lượng hoặc số lượng của sản phẩm có thể giao được. Quyết định hành động khắc phục thường được thể hiện dưới dạng đánh đổi. Thông thường, người quản lý dự án có thể điều chỉnh một trong ba tham số lập kế hoạch sau cho nhiệm vụ đang được sửa chữa:

Công sức và tiền bạc được phân bổ

Thời gian đã trôi qua hoặc tác động lên lịch trình

Chất lượng hoặc số lượng của sản phẩm có thể giao được



Hình 8-1 Vòng phản hồi tiêu cực

Khi tồn quá nhiều công sức và tiền bạc, bạn có thể quyết định dành nhiều thời gian hơn để hoàn thành các nhiệm vụ của dự án hoặc giảm chất lượng hoặc số lượng có thể giao được. Nếu nhiệm vụ mất quá nhiều thời gian để hoàn thành, có lẽ bạn nên thêm nhiều nguồn lực hơn về thời gian hoặc tiền bạc của nhân viên hoặc chất lượng hoặc số lượng có thể giao thấp hơn. Nếu chất lượng của sản phẩm có thể bàn giao quá thấp, bạn thường phải bổ sung thêm nguồn lực về thời gian hoặc tiền bạc của nhân viên hoặc mất nhiều thời gian hơn để hoàn thành nhiệm vụ. Tuy nhiên, có những động lực phức tạp giữa các biến này và những giải pháp đơn giản này không phù hợp trong mọi trường hợp, nhưng mô hình đánh đổi đơn giản này có thể giúp người quản lý dự án phân tích các tùy chọn có sẵn.

Kết thúc dự án Kết thúc dự án thường được xử lý như một nhiệm vụ thủ tục và được giao cho người quản lý bảo mật thông tin hoặc CNTT cấp trung. Những người quản lý này thu thập tài liệu, hoàn thiện báo cáo trạng thái và gửi báo cáo cuối cùng và

thuyết trình tại cuộc họp tổng kết. Mục tiêu của tổng kết là giải quyết mọi vấn đề đang chờ xử lý, phê bình nỗ lực tổng thể của dự án và đưa ra kết luận về cách cải thiện quy trình cho tương lai.

2.1. Trả lời các câu hỏi:

1. Vai trò của phân tích lợi ích chi phí (CBA) là gì?
2. Tại sao nhiều tổ chức công thường dành một khoản đáng kể tiền cuối năm tài chính?
3. Khi nào người dùng nên được đào tạo trước khi có các chính sách và công nghệ mới trực tuyến?
4. Phạm vi dự án là gì? Tại sao nó phải được đánh giá cẩn thận?
5. Vòng phản hồi âm là gì? Làm thế nào nó được sử dụng để giữ một dự án trong điều khiển?
6. Khi một nhiệm vụ không được hoàn thành theo kế hoạch, hai hoàn cảnh có khả năng được tham gia?
7. Người quản lý dự án có thể điều chỉnh tham số nào để sửa tác vụ khi sai lệch đáng kể xảy ra?
8. Mục tiêu của việc tổng kết dự án là gì?

2.2. Quyết định xem các câu sau đây là đúng (T), sai (F) hay không

thông tin (NI)

1. Nguồn vốn hiện có có vai trò quyết định đến mức độ nỗ lực chi tiêu trong các dự án bảo mật thông tin trong mọi tổ chức.

A. Đúng	B. Sai	C. NI
---------	--------	-------
2. Trong mọi tổ chức, ngân sách bảo mật thông tin là một tiêu mục của ngân sách CNTT tổng thể.

A. Đúng	B. Sai	C. NI
---------	--------	-------
3. Hầu hết các tổ chức thiếu nhân sự có trình độ và được đào tạo để thực hiện dự án an toàn thông tin.

4. Thời gian và lịch trình chỉ ảnh hưởng đến một dự án khi bắt đầu

lập kế hoạch.

B. Sai

C. NI

5. Một vòng phản hồi tiêu cực đảm bảo rằng tiến độ được đo cù sau hai

năm.

A. Đúng

B. Sai

C. NI

2.3. Chọn câu trả lời đúng nhất cho các câu hỏi và câu sau.

1. Từ nào sau đây gần nghĩa nhất với từ “đã hoàn thành” trong

dòng 16, đoạn 3?

A. Kết luận

B. Đạt đư ợc

C. Phân bô

D. Đứ ợc đào tạo

2. Ngân sách bảo mật thông tin của các tổ chức công KHÔNG đến từ đâu từ?

A. Pháp luật

B. Họp công cộng

c. Cấp tái tạo

D. Ngân sách chi tiêu của chính họ

3. Điều nào sau đây có thể KHÔNG ảnh hưởng đến ngân sách cho chứng khoán dự án của một tổ chức vì lợi nhuận?

A. Các cuộc tấn công thành công truy ức đó vào các hệ thống thông tin được bảo mật

B. Chi tiêu chuẩn của các tổ chức tư ơng tự

C. Chương trình đào tạo nhân viên

D. Khu chợ

4. Trong một tổ chức, nên lựa chọn ai để giám sát việc thực hiện

của một kế hoạch dự án bảo mật thông tin?

A. một nhà vô địch từ cộng đồng quản lý chung đư ợc quan tâm

- B. một người phù hợp từ cộng đồng bảo mật thông tin của lão
 - C. CIO của tổ chức
 - D. một nhà quản lý CNTT cấp cao của tổ chức
5. Điều nào sau đây là một trong những mục tiêu của cuộc họp tổng kết?
- A. Thảo luận dự án năm tới
 - B. Đánh giá nỗ lực tổng thể
 - C. Hoàn thành nhiệm vụ cuối cùng của dự án
 - D. Dự toán số ngân sách để lại
4. Phát biểu

Trình bày hiểu biết của anh/chị về mô hình đánh đổi trong các tình huống khi các hành động khắc phục phải được thực hiện. Cho ví dụ.

ĐỌC THÊM

Các khía cạnh kỹ thuật của việc thực hiện

Một số khía cạnh của quy trình triển khai có bản chất kỹ thuật và liên quan đến việc áp dụng công nghệ, trong khi những khía cạnh khác lại liên quan đến giao diện của con người với các hệ thống kỹ thuật. Trong các phần tiếp theo, các chiến lược chuyển đổi, ưu tiên giữa nhiều thành phần, thuê ngoài và quản trị công nghệ sẽ được thảo luận.

Chiến lược chuyển đổi

Khi các thành phần của hệ thống bảo mật mới được lên kế hoạch, các điều khoản phải được thực hiện để chuyển đổi từ phương pháp thực hiện nhiệm vụ trước đó sang phương pháp mới. Cũng giống như hệ thống CNTT, các dự án bảo mật thông tin yêu cầu lập kế hoạch chuyển đổi cẩn thận. Trong cả hai trường hợp, bốn cách tiếp cận cơ bản được sử dụng để thay đổi từ một hệ thống hoặc quy trình cũ sang một quy trình mới là:

- **Chuyển đổi trực tiếp:** Còn được gọi là "gà tây nguội", chuyển đổi trực tiếp liên quan đến việc dừng phương pháp cũ và bắt đầu phương pháp mới. Điều này có thể đơn giản như yêu cầu nhân viên tuân theo quy trình hiện có trong một tuần và sau đó sử dụng quy trình mới vào tuần tiếp theo. Một số trường hợp chuyển đổi trực tiếp rất đơn giản, chẳng hạn như yêu cầu nhân viên sử dụng mật khẩu mới (sử dụng mức độ xác thực mạnh hơn) bắt đầu vào ngày đã thông báo; một số có thể phức tạp hơn, chẳng hạn như yêu cầu toàn bộ công ty thay đổi quy trình khi nhóm mạng tắt tường lửa cũ và kích hoạt tường lửa mới. Hạn chế chính của phương pháp chuyển đổi trực tiếp là nếu hệ thống mới bị lỗi hoặc cần sửa đổi, người dùng có thể không có dịch vụ trong khi các lỗi của hệ thống được xử lý. Thủ nghiệm hoàn chỉnh hệ thống mới trước khi chuyển đổi trực tiếp giúp giảm khả năng xảy ra các sự cố như vậy.

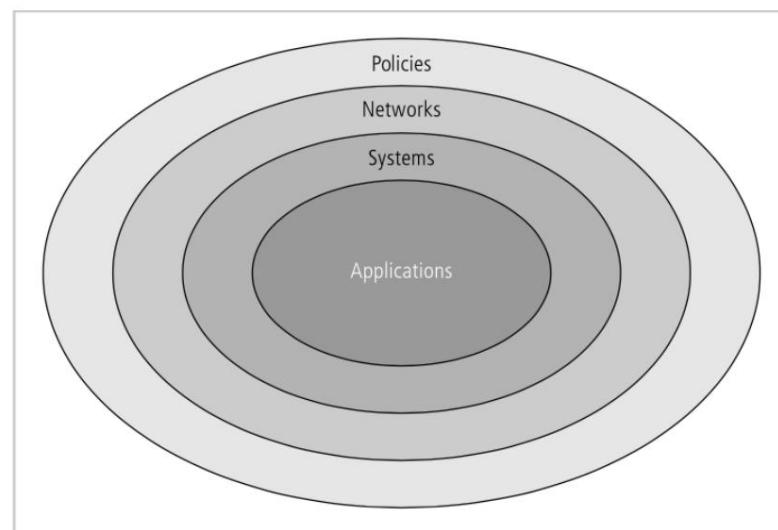
- **Triển khai theo giai đoạn:** Triển khai theo giai đoạn là chiến lược chuyển đổi phổ biến nhất và liên quan đến việc triển khai có đợt lưỡng hệ thống đã hoạch định, với một phần của toàn bộ được triển khai và phổ biến trong toàn tổ chức trước khi phần tiếp theo được triển khai. Điều này có thể có nghĩa là nhóm bảo mật chỉ thực hiện một phần nhỏ của hồ sơ bảo mật mới, giúp người dùng có cơ hội làm quen với nó và giải quyết các vấn đề khi chúng phát sinh. Đây thường là cách tiếp cận tốt nhất để thực hiện dự án bảo mật. Ví dụ: nếu một tổ chức tìm cách cập nhật cả hệ thống VPN và IDPS của mình, thì trước tiên tổ chức đó có thể giới thiệu giải pháp VPN mới mà nhân viên có thể sử dụng để kết nối với mạng của tổ chức khi họ đang di chuyển. Mỗi tuần, một bộ phận khác sẽ được phép sử dụng VPN mới, quá trình này sẽ tiếp tục cho đến khi tất cả các bộ phận đều sử dụng phương pháp mới. Khi VPN mới đã được đưa vào hoạt động theo từng giai đoạn, các bản sửa đổi đối với IDPS của tổ chức có thể bắt đầu.

- Triển khai thí điểm: Trong quá trình triển khai thí điểm, toàn bộ hệ thống bảo mật được đặt tại một văn phòng, phòng ban hoặc bộ phận duy nhất và các vấn đề phát sinh sẽ được xử lý trước khi mở rộng sang phần còn lại của tổ chức. Việc triển khai thí điểm hoạt động tốt khi một nhóm biệt lập có thể đóng vai trò là “chuột bạch”, giúp ngăn chặn bất kỳ sự cố nào với hệ thống mới ảnh hưởng nghiêm trọng đến hiệu suất của toàn bộ tổ chức. Ví dụ: hoạt động của một nhóm nghiên cứu và phát triển có thể không ảnh hưởng đến hoạt động thời gian thực của tổ chức và có thể hỗ trợ bảo mật trong việc giải quyết các vấn đề phát sinh.
- Hoạt động song song: Chiếm lứa ợc hoạt động song song liên quan đến việc chạy các phương pháp mới cùng với các phương pháp cũ. Nói chung, điều này có nghĩa là chạy đồng thời hai hệ thống; về mặt hệ thống thông tin, nó có thể bao gồm, ví dụ, chạy đồng thời hai bức tư ờng lửa. Mặc dù cách tiếp cận này phức tạp như nhau có thể cung cấp bảo mật thông tin của tổ chức bằng cách cho phép (các) hệ thống cũ đóng vai trò dự phòng cho các hệ thống mới nếu chúng bị lỗi hoặc bị xâm phạm. Hạn chế thường bao gồm nhu cầu xử lý cả hai hệ thống và duy trì cả hai bộ thủ tục.

Mô hình Bull's-Eye

Một phương pháp đã được chứng minh để ưu tiên một chương trình thay đổi phức tạp là phương pháp hồng tâm. Phương pháp này, có nhiều tên gọi khác nhau và đã được nhiều tổ chức sử dụng, yêu cầu các vấn đề phải được giải quyết từ tổng thể đến cụ thể và tập trung vào các giải pháp có hệ thống thay vì các vấn đề riêng lẻ. Các khả năng tăng lên-nghĩa là các khoản chi tiêu tăng lên-được sử dụng để cải thiện chương trình bảo mật thông tin một cách có hệ thống và được đo lường. Như được trình bày ở đây và được minh họa trong Hình 8-2, cách tiếp cận dựa trên quá trình đánh giá kế hoạch dự án theo bốn lớp:

1. Các chính sách: Đây là vòng ngoài, hoặc vòng đầu tiên, trong sơ đồ hồng tâm. Tầm quan trọng sống còn của các chính sách đã được nhấn mạnh xuyên suốt cuốn sách giáo khoa này.



Hình 8-2 Mô hình Bull's-Eye

Nền tảng của tất cả các chương trình bảo mật thông tin hiệu quả là chính sách công nghệ thông tin và bảo mật thông tin hợp lý. Vì chính sách thiết lập các quy tắc cơ bản cho việc sử dụng tất cả các hệ thống và mô tả những gì phù hợp và những gì không phù hợp nên nó cho phép tất cả các thành phần bảo mật thông tin khác hoạt động chính xác. Khi quyết định cách triển khai các thay đổi phức tạp và chọn từ các tùy chọn xung đột, bạn có thể sử dụng chính sách để làm rõ những gì tổ chức đang cố gắng đạt được bằng những nỗ lực của mình.

2. Mạng: Trước đây, hầu hết các nỗ lực bảo mật thông tin đều tập trung vào lớp này và vì vậy cho đến gần đây, bảo mật thông tin thường được coi là đồng nghĩa với bảo mật mạng. Trong môi trường máy tính ngày nay, việc triển khai bảo mật thông tin phức tạp hơn vì cơ sở hạ tầng mạng thường tiếp xúc với các mối đe dọa từ mạng công cộng. Những tổ chức mới sử dụng Internet nhận thấy (ngay khi môi trường chính sách của họ xác định cách bảo vệ mạng của họ) rằng việc thiết kế và triển khai DMZ hiệu quả là cách chính để bảo mật mạng của tổ chức. Các nỗ lực thứ cấp trong lớp này bao gồm cung cấp xác thực và ủy quyền cần thiết khi cho phép người dùng kết nối qua mạng công cộng với hệ thống của tổ chức.

3. Hệ thống: Nhiều tổ chức nhận thấy rằng các vấn đề về cấu hình và vận hành hệ thống thông tin theo cách an toàn trở nên khó khăn hơn khi số lượng và độ phức tạp của các hệ thống này tăng lên. Lớp này bao gồm các máy tính được sử dụng làm máy chủ, máy tính để bàn và các hệ thống được sử dụng để kiểm soát quy trình và hệ thống sản xuất.

4. Ứng dụng: Lớp nhận được sự chú ý cuối cùng là lớp xử lý các hệ thống phần mềm ứng dụng được tổ chức sử dụng để hoàn thành công việc của mình. Điều này bao gồm các ứng dụng đóng gói, chẳng hạn như các chương trình e-mail và tự động hóa văn phòng, cũng như các gói hoạch định nguồn lực doanh nghiệp (ERP) cao cấp hơn là mở rộng tổ chức. Phần mềm ứng dụng tùy chỉnh do tổ chức phát triển cho nhu cầu riêng của mình cũng được bao gồm.

Bằng cách xem xét kế hoạch chi tiết bảo mật thông tin và trạng thái hiện tại của các nỗ lực bảo mật thông tin của tổ chức theo bốn lớp này, người lập kế hoạch dự án có thể xác định khu vực nào yêu cầu khả năng bảo mật thông tin mở rộng. Mô hình hồng tâm cũng có thể được sử dụng để đánh giá trình tự các bước được thực hiện nhằm tích hợp các phần của kế hoạch chi tiết bảo mật thông tin vào một kế hoạch dự án. Như được đề xuất bởi hình dạng mắt bò của nó, mô hình này đưa ra những điều sau:

- Cho đến khi các chính sách bảo mật thông tin và CNTT hợp lý và có thể sử dụng được phát triển, truyền đạt và thực thi, không nên sử dụng thêm tài nguyên cho các biện pháp kiểm soát khác.
- Cho đến khi các biện pháp kiểm soát mạng hiệu quả được thiết kế và triển khai, tất cả các nguồn lực sẽ hướng tới việc đạt được mục tiêu này (trừ khi các nguồn lực là cần thiết để xem xét lại nhu cầu chính sách của tổ chức).

- Sau khi triển khai các chính sách và kiểm soát mạng, việc triển khai nên tập trung vào hệ thống thông tin, quy trình và sản xuất của tổ chức. Cho đến khi có sự đảm bảo đầy đủ thông tin rằng tất cả các hệ thống quan trọng đang được định cấu hình và vận hành theo cách an toàn, tất cả các nguồn lực nên được sử dụng để đạt được mục tiêu đó.
- Khi đã có sự đảm bảo rằng các chính sách được áp dụng, mạng được bảo mật và hệ thống được an toàn, cần chú ý đến việc đánh giá và khắc phục tính bảo mật của các ứng dụng của tổ chức. Đây là một lĩnh vực quan tâm phức tạp và rộng lớn đối với nhiều tổ chức. Hầu hết các tổ chức bỏ qua việc phân tích tác động của bảo mật thông tin đối với các hệ thống đã mua và sở hữu riêng của họ. Như trong tất cả các nỗ lực lập kế hoạch, trước tiên cần chú ý đến các ứng dụng quan trọng nhất.

Thuê ngoài hay không

Không phải mọi tổ chức đều cần phát triển một bộ phận hoặc chương trình bảo mật thông tin của riêng mình. Giống như một số tổ chức thuê ngoài một phần hoặc tất cả các hoạt động CNTT của họ, các tổ chức cũng có thể thuê ngoài một phần hoặc tất cả các chương trình bảo mật thông tin của họ. Chi phí và thời gian cần thiết để phát triển một chương trình bảo mật thông tin hiệu quả có thể nằm ngoài khả năng của một số tổ chức và do đó, họ có thể thuê các dịch vụ chuyên nghiệp để giúp bộ phận CNTT của họ triển khai một chương trình như vậy.

Khi một tổ chức thuê ngoài hầu hết hoặc tất cả các dịch vụ CNTT, bảo mật thông tin phải là một phần của thỏa thuận hợp đồng với nhà cung cấp. Các tổ chức xử lý hầu hết các chức năng CNTT của riêng họ có thể chọn thuê ngoài các chức năng bảo mật thông tin chuyên biệt hơn. Các tổ chức vừa và nhỏ thường thuê chuyên gia tư vấn bên ngoài để kiểm tra thâm nhập và kiểm toán chương trình bảo mật thông tin. Các tổ chức thuộc mọi mô hình kinh doanh thuê ngoài các chức năng giám sát mạng để đảm bảo rằng hệ thống của họ được bảo mật đầy đủ và để nhận được hỗ trợ trong việc theo dõi các cuộc tấn công đã cố gắng hoặc thành công.

Quản trị Công nghệ và Kiểm soát Thay đổi

Các yếu tố khác quyết định sự thành công của các chương trình bảo mật thông tin và CNTT của một tổ chức là các quy trình kiểm soát thay đổi và quản trị công nghệ.

Quản trị công nghệ, một quy trình phức tạp mà các tổ chức sử dụng để quản lý tác động và chi phí của việc triển khai, đổi mới và lối đi của công nghệ, hướng dẫn tần suất cập nhật các hệ thống kỹ thuật cũng như cách các bản cập nhật kỹ thuật được phê duyệt và tài trợ. Quản trị công nghệ cũng tạo điều kiện trao đổi thông tin về các tiến bộ kỹ thuật và các vấn đề trong toàn tổ chức.

Các tổ chức vừa và lớn đối phó với tác động của thay đổi kỹ thuật đối với hoạt động của tổ chức thông qua quy trình kiểm soát thay đổi. Bằng cách quản lý quá trình thay đổi, tổ chức có thể thực hiện những việc sau:

- Cải thiện truyền thông về thay đổi trong toàn tổ chức • Tăng cường sự phối hợp giữa các nhóm trong tổ chức khi thay đổi là đã lên kế hoạch và hoàn thành
- Giảm các hậu quả ngoài ý muốn bằng cách có một quy trình giải quyết xung đột và gián đoạn mà sự thay đổi có thể gây ra • Cải thiện chất lượng dịch vụ khi các lỗi tiềm ẩn được loại bỏ và các nhóm làm việc cùng nhau
- Đảm bảo với ban quản lý rằng tất cả các nhóm đều tuân thủ các chính sách của tổ chức về quản trị công nghệ, mua sắm, kế toán và bảo mật thông tin

Kiểm soát thay đổi hiệu quả là một phần thiết yếu của hoạt động CNTT trong tất cả trừ các tổ chức nhỏ nhất. Nhóm bảo mật thông tin cũng có thể sử dụng quy trình kiểm soát thay đổi để đảm bảo rằng các bước quy trình thiết yếu nhằm đảm bảo tính bảo mật, tính toàn vẹn và tính khả dụng được tuân thủ khi các hệ thống được nâng cấp trong toàn tổ chức.

Các khía cạnh phi kỹ thuật của việc thực hiện

Một số khía cạnh của quy trình triển khai bảo mật thông tin không có bản chất kỹ thuật và thay vào đó xử lý giao diện của con người với các hệ thống kỹ thuật. Trong các phần tiếp theo, chủ đề tạo ra văn hóa quản lý thay đổi và những cân nhắc cho các tổ chức đổi mới với thay đổi sẽ được thảo luận.

Văn hóa quản lý thay đổi

Triển vọng thay đổi, từ quen thuộc chuyển sang xa lạ, có thể khiến nhân viên hình thành, một cách vô thức hoặc có ý thức, sự phản kháng đối với sự thay đổi đó. Bất kể những thay đổi được coi là tốt (như trong trường hợp triển khai bảo mật thông tin) hay xấu (chẳng hạn như thu hẹp quy mô hoặc tái cấu trúc quy mô lớn), nhân viên có xu hướng thích cách làm việc cũ hơn. Ngay cả khi nhân viên chấp nhận các thay đổi, thì sự căng thẳng khi thực sự thực hiện các thay đổi và điều chỉnh theo các quy trình mới có thể làm tăng khả năng xảy ra sai sót hoặc tạo ra các lỗ hổng trong hệ thống. Bằng cách hiểu và áp dụng một số nguyên lý cơ bản của quản lý thay đổi, người quản lý dự án có thể giảm bớt sự phản đối của nhân viên trước sự thay đổi và thậm chí có thể xây dựng khả năng phục hồi để thay đổi, do đó làm cho sự thay đổi đang diễn ra trở nên dễ chịu hơn đối với toàn bộ tổ chức.

Nền tảng cơ bản của quản lý thay đổi đòi hỏi những người thực hiện thay đổi phải hiểu rằng các tổ chức thường có văn hóa đại diện cho tâm trạng và triết lý của họ. Sự gián đoạn đối với nền văn hóa này phải được giải quyết đúng đắn và giảm thiểu tác động của chúng. Một trong những mô hình thay đổi lâu đời nhất là mô hình thay đổi Lewin, bao gồm:

- Tháo băng • Di chuyển

- Cấp động lại

Làm tan băng liên quan đến việc làm tan băng những thói quen khó và nhanh và các quy trình đã được thiết lập. Di chuyển là sự chuyển đổi giữa cách cũ và cách mới. Tái định hình là sự tích hợp các phương pháp mới vào văn hóa tổ chức, được thực hiện bằng cách tạo ra một bầu không khí trong đó những thay đổi được chấp nhận như là cách ưu tiên để hoàn thành các nhiệm vụ cần thiết.

Cân nhắc thay đổi tổ chức

Các bước có thể được thực hiện để làm cho một tổ chức dễ thay đổi hơn. Các bước này làm giảm khả năng chống lại sự thay đổi khi bắt đầu quá trình lập kế hoạch và khuyến khích các thành viên của tổ chức linh hoạt hơn khi có những thay đổi.

Giảm khả năng chống lại sự thay đổi ngay từ đầu Mức độ chống lại sự thay đổi ảnh hưởng đến mức độ dễ dàng mà một tổ chức có thể thực hiện các thay đổi về thủ tục và quản lý. Các phương pháp và hành vi hiện tại càng ăn sâu thì việc thay đổi càng khó thực hiện. Do đó, tốt nhất là cải thiện sự tương tác giữa các thành viên bị ảnh hưởng của tổ chức và những người lập kế hoạch dự án trong giai đoạn đầu của dự án cải tiến bảo mật thông tin. Sự tương tác giữa các nhóm này có thể được cải thiện thông qua quy trình ba bước trong đó các nhà quản lý dự án giao tiếp, giáo dục và tham gia.

Giao tiếp là bước đầu tiên và quan trọng nhất. Người quản lý dự án phải giao tiếp với nhân viên để họ biết rằng một quy trình bảo mật mới đang được xem xét và phản hồi của họ là điều cần thiết để làm cho nó hoạt động. Bạn cũng phải liên tục cập nhật cho nhân viên về tiến độ của SecSDLC và cung cấp thông tin về ngày hoàn thành dự kiến. Chuỗi cập nhật đang diễn ra này giữ cho quy trình không bị bất ngờ vào phút cuối và giúp mọi người dễ dàng chấp nhận thay đổi hơn khi nó đến.

Đồng thời, bạn phải cập nhật và giáo dục nhân viên về chính xác những thay đổi được đề xuất sẽ ảnh hưởng đến cá nhân họ và trong tổ chức như thế nào. Mặc dù thông tin chi tiết có thể không có sẵn trong các giai đoạn trước của kế hoạch dự án, nhưng các chi tiết có thể được chia sẻ với nhân viên có thể xuất hiện khi SecSDLC tiến triển. Giáo dục cũng liên quan đến việc dạy nhân viên sử dụng các hệ thống mới khi chúng được đưa vào sử dụng. Điều này, như đã thảo luận trước đó, có nghĩa là cung cấp các chương trình đào tạo chất lượng cao vào những thời điểm thích hợp.

Cuối cùng, các nhà quản lý dự án có thể giảm khả năng chống lại sự thay đổi bằng cách lôi kéo nhân viên tham gia vào kế hoạch dự án. Điều này có nghĩa là mời các đại diện chủ chốt từ các nhóm người dùng làm thành viên của quy trình phát triển SecSDLC. Trong phát triển hệ thống, điều này được gọi là phát triển ứng dụng chung, hoặc JAD. Việc xác định mối liên hệ giữa những người triển khai CNTT và bảo mật thông tin và toàn bộ dân số của tổ chức có thể phục vụ tốt cho nhóm dự án trong các giai đoạn lập kế hoạch ban đầu, khi có thể cần giải quyết các vấn đề không lường trước được về việc chấp nhận dự án.

Phát triển một nền văn hóa hỗ trợ thay đổi Một tổ chức lý tưởng thúc đẩy khả năng phục hồi để thay đổi. Điều này có nghĩa là tổ chức hiểu rằng thay đổi là một phần cần thiết của văn hóa và việc chấp nhận thay đổi sẽ hiệu quả hơn là chống lại nó. Để phát triển một nền văn hóa như vậy, tổ chức phải thực hiện thành công nhiều dự án đòi hỏi sự thay đổi. Một nền văn hóa kiên cường có thể được vun đắp hoặc bị hủy hoại bởi cách tiếp cận của ban quản lý. Sự hỗ trợ mạnh mẽ của ban quản lý đối với sự thay đổi, với người đứng đầu cấp điều hành rõ ràng, cho phép tổ chức nhận ra sự cần thiết và tầm quan trọng chiến lược của sự thay đổi. Sự hỗ trợ quản lý yếu kém, với trách nhiệm được giao quá mức và không có người đứng đầu, khiến dự án gần như chắc chắn thất bại. Trong trường hợp này, nhân viên cảm thấy mức độ ưu tiên thấp đã được dành cho dự án và không liên lạc với đại diện từ nhóm phát triển vì nỗ lực này không như vô ích.

Trả lời các câu hỏi:

1. Liệt kê và mô tả bốn chiến lược chuyển đổi cơ bản (như được mô tả trong chương) được sử dụng khi chuyển đổi sang một hệ thống mới. Theo đó hoàn cảnh là mỗi trong số những cách tiếp cận tốt nhất?
2. Quản trị công nghệ là gì? Kiểm soát thay đổi là gì? Họ thế nào có liên quan?

Danh sách các từ

viết tắt (n): rút gọn

abacus (n): bàn tính.

access control (n): kiểm soát truy cập

hoàn thành (v): thực hiện

add (n): phép cộng

Advanced Encryption Standard (AES): chuẩn hóa dữ liệu mã hóa tiên tiến

Advanced Research Projects Agency Network (ARPANET): mạng cơ quan với các đề tài nghiên cứu tiên tiến.

Advanced Research Projects Agency (ARPA): Cơ quan chỉ đạo các dự án Nghiên cứu Tiên tiến

adversary (n): kẻ thù

thuật toán (n): thuật

toán phân bổ (v): phân phối.

analysis (n): sự phân tích

analog (n, adj): tư duy tự.

American National Standard Institute (ANSI): Viện tiêu chuẩn Quốc gia Mỹ

alphanumeric data (n): dữ liệu chữ số alphabetical catalog (n): mục lục xếp theo

trật tự chữ cái thiết bị (n): thiết bị, máy móc

application (n): ứng dụng

Application-Level Gateway (ALG): cổng cấp ứng dụng

thích hợp (adj): thích hợp

approximation (n): xấp xỉ phát

sinh (v): xuất hiện, nảy sinh

arithmetic (adj): số học

assort (v): chia loại, phân loại

asymmetric-key (n): khóa phi đối xứng

asymmetric algorithm (n): thuật toán phi đối xứng

authentication (n): sự xác thực

Authenticator (n): ký hiệu xác nhận

giao thức xác thực (n): giao thức xác thực

người dùng được ủy quyền (n): người dùng

hợp pháp có sẵn (adj): có sẵn, được sử dụng, có

hiệu lực backdoor (n): tấn công cửa sau nhì phân

(adj/n): thuộc về nhì phân/ số nhì phân.

bijection (n): ánh xạ

binary alphabet (n): bảng nhị phân

bit-string (n): xâu bit

block cipher (n): mã khôi

boot (v): khởi động

phân loại rộng (n): phân loại tổng quát tấn công

vũ phu (n): tấn công vét cạn

Khả năng (n): khả năng

cataloging (n): biên mục công việc

cipher (n): mật mã

ciphertext (n): bản mã

Cổng cấp mạch: kịch bản chỉ có bản mã

của cổng mạch (n): trưòng hợp chỉ biết chế độ phản hồi mã hóa

mã hóa (CFB): chế độ phản hồi mã hóa chế độ chuỗi khôi mã hóa

(CBC): chứng nhận mã hóa liên kết khôi chế độ (n) : giấy chứng nhận

cơ quan chứng nhận (n): cơ quan chứng nhận Circuit

Level Gate (CLG): cổng mạch làm rõ (v): làm dễ hiểu.

cluster controller (n): bộ điều khiển trùm

complex (adj): phức tạp

component (n): thành phần, thiết bị

computerize (v): tin học hóa

computer-control instrumentation (n): dụng cụ điều khiển bằng điện toán

Compromised-Key Attack (n): tấn công phá khóa

command (v/n): ra lệnh/lệnh

compile (v): biên dịch

cookie (n): một tệp nhỏ, được lưu trên máy tính của bạn bằng trình duyệt

tung xu

CIA tam giác (Confidentiality Integrity Availability): tam giác bảo mật che

giấu (v): giấu, che đậy configuration (n): cấu hình

tư ơng thích (adj): tư ơng

thích Consultant (n): vấn đề

convert (v): chuyển đổi

secret (n): tính bí mật

concept (n): khái niệm

cryptanalysis (n): phân tích mật mã

cryptanalyst (n): người làm công việc thám mã

cryptography (n): mật mã

cryptosystem (n): hệ mật

cryptanalytic technique (n): kỹ thuật thám mã

crypto-communication (n): truyền tin bí mật

thuật toán mã hóa (n): thuật toán mật mã

cryptography hash function (n): hash hash code

character-by character (n): từng ký tự

hệ số (n): hệ số columnar transposition

(n): biên đổi cột (v): thay thế, giao đổi

hàng tư ơng ứng (n): hàng tư ơng ứng bản

rõ tư ơng ứng khôi (n): khôi bản rõ tư ơng ứng

hệ thống mật mã (n): hệ mật

data packet (n): gói dữ liệu

datapression function (n): datapression function (hàm nén dữ liệu)

database (n): cơ sở dữ liệu

Data Encryption Standard (DES): chuẩn hóa dữ liệu mã hóa

deal (v): giao dịch

có chủ ý tấn công phần mềm (n): tấn công phần mềm có chủ ý

demagnetize (v): khử từ hóa

device (n): thiết bị

detect (v): sự dò

xét đáng tin cậy (adj): có thể tin cậy đư ợc.

devise (v): phát minh.

decipher (v): giải mã

demand (n): yêu cầu

detail (adj): chi tiết

develop (v): phát triển

Từ chối dịch vụ phân tán: tấn công từ chối dịch vụ phân tán phân phối

thủ công (n): sự phân phối bằng tay

đĩa (n): đĩa

chia (n): phép chia như ợc

điểm (n): trờ nên sợ hãi, hạn chế

decoding technology (n): kỹ thuật giải mã

Defense Advanced Research Projects Agency (DARPA): Cơ quan chỉ đạo các Dự án

án nghiên cứu Quốc phòng Tiên tiến, dial-

in modem (n): modem quay số kết nối quay số (n):

cuộc tấn công quay số vi sai (n): tấn công sai

số kỹ thuật số (adj): thuộc về chữ ký số (n): ký

tự số

Thuật toán chữ ký số (DSA): thuật toán chữ ký số chữ ký số (n):

chữ ký điện tử, chữ ký số

rời rạc (adj): rời rạc

logarit rời rạc (np): logarit rời rời

ư ớc (n): ư ớc số domain name (n): tên miền

Nhiễm độc bộ nhớ cache của Hệ thống tên miền (DNS): tấn công khai thác lỗ hổng trong hệ

thông tên miền

dummy run (n): việc chạy thử

tư ờng lửa lọc gói động (n): tư ờng lửa bộ lọc gói động

nghe lén (v): nghe trộm

hiệu quả (adj): có hiệu lực

hiệu quả (adj): có hiệu suất cao

embed (v): gắn vào, nhúng vào

mã hóa (n): mã hóa

khóa mã hóa (n): khóa mã hóa thiết

bị mã hóa (n): thiết bị mã hóa

encipher (v): mã hóa

mã hóa (n): công việc mã hóa thực

thẻ's Identity (n): danh tính/sự nhận định dạng của đối tượng/đối tượng tác động

elite (adj): ưu tú,

giỏi error-sửa mã số (n): mã sửa các sai số

gián điệp (n): do thám

chuyên môn (v): thành thạo, tinh thông

thạo key (n): khóa tìm kiếm bằng phư ơng pháp rút cạn

Exclusive-or operation (n): phép toán xor loại trừ

vết cạn trial (n): thử vết cạn vết

cạn (adj): kẽ vè vết cạn

tìm kiếm khóa vết cạn (n): phư ơng pháp tìm khóa vết cạn

factor (n): thừa số

factor (v): phân tích

ferrite ring (n): vòng phân tích

từ frequency analysis (n): phân tích tần số

freeware (n): phần mềm được cung cấp miễn phí

tư ờng lửa (n): tư ờng lửa

FOSS Phần mềm mã nguồn mở và miễn phí: phần mềm Nguồn mở và miễn phí

function (n): hàm

basic (adj): cơ bản

hacker (n): tin tặc

hàm bấm (n): hàm bấm máy tính

cá nhân hóa cầm tay (n): máy tính cầm tay cá nhân chữ ký viết tay (n):

chữ ký bằng tay Hieroglyphics (n): hệ thống chữ tự ợng hình

Host-based Intrusion Detection System (HIDS): hệ thống bảo vệ chống xâm nhập

dựa vào máy chủ

hybrid system (n): hệ thống ghép

nối ID (n): thiết bị nhận định dạng

mạo danh (v): giả mạo, mạo danh

implement (v): công cụ, phuơng tiện

implementation (n): sự thực thi, việc thực hiện không

thực tế (adj): không thực tế **index column** (n): cột

chỉ số row (n): hàng chỉ số **personal** (adj/n): thuộc

về cá nhân/ cá nhân

quán tính (n): quán

tính. infeasible (adj): không thể làm

được hứa hẹn dẫn (n): chỉ thị, chỉ dẫn **bảo hiểm** (n): bảo

hiểm tích hợp (v): hợp nhất, sát nhập

tư ờng lửa tích hợp (nph): tư ờng lửa tích hợp

liêm chính (n): sự toàn vẹn

intelligence (n): tình báo

integer factorization: phân tích nguyên số

nguyên factorization (n): phân tích nguyên số

Internet Protocol address (n): một địa chỉ giao thức Internet

cài đặt (v): cài đặt

đánh chặn (v): chặn

intranet (n): mạng nội bộ

Hệ thống ngăn chặn xâm nhập (IPS): hệ thống phòng chống xâm nhập

Internet Service Provider (ISP): nhà cung cấp dịch vụ Internet

graphics (n): đồ họa

Goal (n): Gadget

item (n): Đồ phụ tùng nhỏ

Hệ thống định vị toàn cầu (GPS): hệ thống định vị toàn cầu vấn đề

phân phối khóa (n): bài toán phân phối khóa

độ dài khóa: độ dài khóa

phư ơng trình tuyến tính (n): phư ơng trình

tuyến tính tuyến tính phản hồi bộ tạo (n): bộ sinh phản hồi tuyến

tính hàm toán học tuyến tính (n): hàm số toán học tuyến tính quan

hệ tuyến tính (n): mối quan hệ hệ tuyến tính lineartransform (n):

biến đổi tuyến tính linear cryptanalysis: phư ơng pháp thám mã tuyến

tính

logarit (n): logarit

maintain (v): duy trì

Viện Công nghệ Massachusetts (MIT): Viện Khoa học công nghệ

Massachusetts

matrix (adj/n): ma trận

malware (n): phần mềm độc hại

mã độc (n): mã độc

memory (n): bộ nhớ

mã xác thực thông báo (n): mã xác thực bản tin

tin nhắn trong ngày (MODT): tin nhắn trong ngày

mã xác thực thông báo (n): mã xác thực thông báo

microprocessor (n): bộ vi xử lý

minicomputer (n): máy tính mini

giám sát (v): giám sát

multi-task (n): đa nhiệm vụ.

phép nhân (n): phép nhân

thư ơng lượng (v): thư ơng lượng

Network Intrusion Detection System (NIDS): hệ thống bảo vệ chống xâm nhập

mạng

tư ờng lừa thé hệ tiếp theo (NGFW): tư ờng lừa thé hệ tiếp theo non-

repudiation (n): sự từ chối

Cơ quan an ninh quốc gia NSA: cơ quan an ninh quốc gia của Mỹ numeric

(adj): số học, thuộc về số học, xảy ra (v): xảy ra, xảy ra

login (v): đăng nhập

operation (n): thao tác

Operating system (n): hệ thống điều hành

Open System Interconnection (OSI): kết nối các gói hệ thống mở giao

diện outcomming của gói: cổng tin đi

giám sát (v): quan sát

Packet- Filtering Router: bộ định tuyến bộ lọc gói tin

Packet filtering (n): bộ lọc gói tin

thực hiện (v): thực hiện

hoán vị (n): phép hoán vị chu kỳ

của chuỗi (nph): chu kỳ của chuỗi

permute (v): hoán vị

pinpoint (v): chỉ ra một cách xác định chính xác, xác định chính xác

buồng điện thoại (n): trạm điện thoại

(n): mối đe dọa vật lý

bản rõ (n): bản rõ

polyalphabetic cipher (n): hệ mật mã đa biểu

polymath: nhà thông thái, học giả

đa hình (adj): đa dạng

power supply (n): bộ lưu điện

principle (n): nguyên tắc

priority (n): Sự ưu tiên.

process (v): xử lý

process (n): quá trình, tiến trình

product (n): tích

của hai số (n): tích của hai số Point-to-Point

Protocol (PPP): giao thức kết nối Internet 1-1 suất (n): hiệu suất.

protocol (n): Giao thức

tư ờng lửa dựa trên proxy: tư ờng lửa dựa trên proxy

máy chủ proxy (n): máy chủ nhiệm vụ port

(n): cổng prime factorization (n): phân

tích thừa số nguyên tố number (n): số nguyên tố

private key (n): khóa bí mật

khóa công khai: khóa công khai

quá trình vật lý (n): quá trình vật

lý số nguyên tố (n): số nguyên tố

trú ớc sự sắp xếp (n): sắp xếp thứ nhất

private key cryptography (n): mật mã khóa bí mật

pseudorandom (adj): thuộc về giả ngẫu nhiên

public key cryptography (n): mật mã khóa công khai public -

key hạ tầng cơ sở (PKI): cơ sở hạ tầng khóa công khai

public key (n): khóa công khai

xung (n): xung đột

random (adj): ngẫu nhiên

real-time (adj): thời gian thực

relative frequency (n): tần số quan hệ

tư ơng đối shift (n): dịch chuyển quan hệ

resource (n): nguồn

truy cập từ xa (n): truy cập từ xa

response (v): phản hồi

rotor machine (n): máy rôto

router (n): bộ định tuyến

security identification (n): nhận dạng cơ sở dữ

liệu mật khẩu an toàn (n): cơ sở dữ liệu mật khẩu bảo mật

secret (n): bí mật

Secure Sockets Layer (SSL): tầng socket bảo mật (một tiêu chuẩn của công nghệ

bảo mật)

chứng chỉ bảo mật (n): chứng thực bảo mật

security policy (n): chính sách bảo mật

security cable (n): khóa an toàn

máy chủ (n): máy chủ

SIM card (n): thẻ nhớ di động

signal (n): tín hiệu

đồng thời (adj): đồng thời

solution (n): giải pháp, lời giải

quyết (v): giải quyết

tư ờng lửa có trạng thái: tư ờng lửa có trạng

thái kiểm tra trạng thái tư ờng lửa: tư ờng lửa kiểm tra trạng thái

steganography (n): ngụy trang

stream cipher (n): mã dòng

Serial Direct Cable Connection (n): cáp nối trực tiếp nối tiếp sequence

(n): string scheme (n): sơ đồ

shift value (n): giá trị chuyển dịch

thuật toán ký thuật toán (n): thuật toán

kiểm tra chữ ký thuật toán xác minh chữ ký (n): thuật toán kiểm tra

chữ ký space (n): khoảng trống, khoảng trống

thuật toán cụ thể (n): thuật toán riêng biệt

spybot (n): chương trình chống phần mềm gián điệp miễn phí

storage (n): lưu trữ

store (v): lưu trữ

string (n): chuỗi

sub-cryptogram (n): đoạn mã thay thế

(n): sự thay thế

Phép trừ (n): phép trừ đúng

kẻ (adj): tính thực tế

enough (adj): đủ, có khả năng

tệp hoán đổi (n): chuyển

đổi tệp đệm (n/v): công tắc, chuyển

đổi khóa đối xứng (n): khóa đối xứng

terminal (n): điểm cuối, trạm máy

thuật ngữ (n): thuật ngữ

tam giác (n): đánh đổi hình

tam giác (adj: đánh đổi truyền

(v): truyền chuyển vị cipher

(n): mã chuyển vị

Transmission Control Protocol/Internet Protocol (TCP/IP)": bộ giao thức cho phép kết nối

các hệ thống mạng không đồng nhất với nhau

Transport Layer Security (TLS): Bảo mật tầng giao thông vận tải

trap door (n): cửa sổ

bẫy và dấu vết system (n): hệ thống kiểm tra và theo dõi xâm

phạm (n): sự xâm lấn thiên văn học thống kê: thiên văn học thống

khê

unbreakable (adj): không thể phá vỡ

union catalog (n): lục liên hợp.

lỗ hỏng: sự tổn hại dễ bị tổn

thương (adj): có thể bị tấn công

wipe (n): tiến trình xóa bỏ vĩnh viễn thông tin bảo mật

Tư ờng lửa ứng dụng web (WAF): Tư ờng lửa ứng dụng web

Ngữ ời giới thiệu

- [1]. A. Menezes, P. van Oorschot và S. Vastone, *Sổ tay Ứng dụng mật mã*, CRC Press Inc, 1997.
- [2]. Andress, J, *Khái niệm cơ bản về bảo mật thông tin: Hiểu các nguyên tắc cơ bản của InfoSec trong lý thuyết và thực hành*, Tổng hợp, 2014.
- [3]. Bergstra, J, *Lịch sử An ninh Thông tin: Toàn diện Sổ tay*. DeNardis, L. Nhà xuất bản Đại học Oxford, 2008.
- [4]. Fred Cohen, *Lịch sử ngắn về mật mã*, Fred Cohen – Tất cả các quyền Bảo lưu, 1990, 1995.
- [5]. Fred Piper và Sean Murphy, *Mật mã học: Phần giới thiệu rất ngắn*, Nhà xuất bản Đại học Oxford, 2002.
- [6]. Fred Piper, Simon Blake-Wilson và John Mitchell, *Chữ ký số: Kiểm toán và Kiểm soát Hệ thống Thông tin*, ISACA, 2000.
- [7]. ISO/IEC 27000, *Công nghệ thông tin - Kỹ thuật bảo mật - Hệ thống quản lý bảo mật thông tin*, 2009.
- [số 8]. Michael E Whitman, Herbert, J. Marttord, *Nguyên tắc bảo mật thông tin*, Phiên bản thứ tư, Công nghệ khóa học, Trung tâm 20 Channel, Boston, MA 02210, Hoa Kỳ, 2011.
- [9]. Newsome, B, *Giới thiệu Thực tế về An ninh và Quản lý Rủi ro*. Nhà xuất bản SAGE, 2013.
- [10]. Roland van Rijswijk và Martijn Oostdijk, *Ứng dụng hiện đại mật mã*, SURFnet BV, 2010.
- [11]. Serge Vaudenay, *Giới thiệu cổ điển về mật mã hiện đại*, Science and Business Media Inc, 2006.
- [12]. Vacca, John R, *Sổ tay bảo mật máy tính và thông tin*, SAGE Publications, 2009.

TIẾNG ANH THÔNG TIN

BẢO VỆ

Chịu trách nhiệm xuất bản

ĐBQH-TBT: NGUYỄN THỊ THU HÀ

Biên tập: Ngô Mỹ Hạnh
nguyễn long biên

Mã số: GD 44 Hm13

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG Trụ sở: Số 9, Ngõ 90, Phố Ngụy Như Kom Tum, Quận Thanh Xuân, TP. Hà Nội ĐT Biên tập: 04.35772143 E-mail: nxb.tttt@mic.gov.vn Website: www.nxbthongtintruyenthong.vn Phát hành: 04.35772138 Fax: 04.35772194, 04.35579858

Chi nhánh TP. Hồ Chí Minh: 8A đường D2, P25, Quận Bình Thạnh, TP. Hồ Chí Minh
Điện thoại: 08.35127750, 08.35127751 Fax: 08.35127751
E-mail: cnsg.nxbttt@mic.gov.vn

Chi nhánh TP. Đà Nẵng: 42 Trần Quốc Toản, Q. Hải Châu, TP. Đà Nẵng
Điện thoại: 0511.3897467 E-mail: cndn.nxbttt@mic.gov.vn Fax: 08.35127751

Khổ: 300 bản, khổ: 20x30 cm tại XN 951-Ban Cơ yếu Chính phủ

Số đăng ký kế hoạch xuất bản 1925-2013/CXB/43-776/TTTT

Số quyết định xuất bản: 387/QĐ-NXB TTTT ngày 28 tháng 1 năm 2019

In xong và cập nhật bản ghi Quý I năm 2020

